Developing a cybercrime framework for a developing country: A case of Eswatini

E.L. Howe



orcid.org/ 0000-0002-3142-9585

Thesis accepted in fulfilment of the requirements for the degree Doctor of Philosophy in Economic and Management with Business Administration at the North-West University

Promoter: Prof Anna-Marie Pelser

Graduation ceremony: May 2024

DECLARATION

I, Emmanuel Lungile Howe, declare "*A conceptualized cybercrime framework for a developing country: A case of the Kingdom of Eswatini"* is my work. All the sources used and quoted have been indicated and acknowledged using a complete list of references.

I further declare that I have not previously submitted this work, or part of it, for examination at the NWU for another qualification or at any other higher education institution.



_____ 24/11/2023

Signature Date

ABSTRACT

The Internet has become a routine activity in everyday life for people, industries and organisations, and it comes with a number of benefits which include abundant access to the Internet. These benefits have opened up opportunities for cybercriminals to exploit the Internet platform for criminal activities especially in the banking sector. Cybercrime involves criminal acts that usually involve electronic devices such as computers and networks. In the banking sector cybercrime increase is a result of many factors such as growth in Internet usage base, poor security awareness, lack of law enforcement training and limited cyberspace regulation. Due to high volume of cybercrime incidents such as phishing, viruses, hacking, there is a need to further explore and analyse the cybercrime scenario in the banking sector. The failure to control banking activities mostly occurring online provides opportunities for cybercriminals to take chances and conduct conventional crimes in *a new* way using the Internet as a tool. The main problem is the low technological literacy of users and the exposure of technical security system loops which are factors that contribute towards the rise of cybercrime. Therefore, this study sought to explore and analyse the cybercrime phenomenon and leading to provide measures that Eswatini banks can adopt to minimise their risk and exposure to cybercrime.

The routine activity theory, space transition theory and deterrence theory were used as theoretical lenses to formulate a conceptual framework that will aid towards a holistic understanding of cybercrime in the banking sector in Eswatini banks. Primary data was collected through interviews and questionnaires from participants that are mandated to address cybercrime issues and tasks within the organisation departments. This study is informed by the limited research in the field of cybercrime particularly in Eswatini banks and will attempt to bridge the existing cybercrime gap knowledge by analysing the cybercrime phenomenon from the perspective of Eswatini banks. In order to achieve this, the study adopted an interpretivism approach using a case study in Eswatini Banks.

The interpretation of findings suggests that to achieve a robust cybercrime response culture, financial institutions in Eswatini must ensure that cybercrime awareness interventions must be well established and aligned properly with the monitoring and reporting mechanisms. Management needs to strengthen their involvement in addressing cybercrime issues in the organisations. The original contribution of this thesis is developing a cybercrime framework that will help financial institutions to address and mitigate cybercrime threats and attacks.

Keywords: *Cybercrime, Eswatini Banks, Routine Activity Theory, Space Transition Theory, Deterrence Theory*

PEER-REVIEWED PUBLICATIONS FROM THE THESIS

Howe, EL and Prof Pelser Anna-Marie. 2022. Cybercrimes in the Eswatini banking sector: Implementing routine activity theory analysis. Ensovoort. Journal of Cultural Studies. Vol 43. No.07

Howe, EL and Prof Pelser Anna-Marie. 2020. Cybercrime in Eswatini: The deterrence theory approach. Ensovoort.Journal of Cultural Studies. Vol 41. No.11

Virtual Guest Lecturer Presentation at the New Horizon College of Engineering, Bengaluru, India. 06th May 2022 on the topic titled, **"Preventing Cybercrimes in Financial Institutions**

ACKNOWLEGEMENTS

This has been a long and demanding journey, still interesting and very gratifying at the end of it all.

First of all, I am grateful to the Almighty God, the creator, for giving me good health, a loving family, a blessed supervisor and above all the strength to finish this project.

Much appreciation goes to my supervisor, **Prof Anna-Marie Pelser** from whom I received unlimited guidance, encouragement, the highest level of patience and perseverance I have ever experienced in my life, to really shape the direction and final deliverable of this journey. During our journey, she transformed from being a supervisor to a loving and caring Mother, thank you I appreciate you. May the Almighty God reward you abundantly for all your efforts and sacrifice.

Special thanks to **Dr Hazvie Saurombe** and **Dr Andrew Mutsvangwa** who despite their busy schedule and my last minute request, assisted me to make this project unique.

Finally, I would like to thank and dedicate this thesis to my wife - **Matlotlo Adolphina Howe** and my children son - **Malibongwe Theo Howe** and daughter - **Sibanesethu Alma Howe** for their support and understanding throughout this journey.

DEDICATION

This study is dedicated to my late father, **Basil Eric Howe.**

ABBREVIATIONS AND ACRONYMS

AFRIPOL	African Union Mechanism for Police Cooperation
BIS	Bank for International Settlements
CERT	Computer Emergency Response Team
CSOC	Cybersecurity Operating Center
DoS	Denial of Service
DDoS	Distributed denial-of-service
GDP	Gross Domestic Product
ICMP	Internet Control Message Protocol
IOSCO	International Organization of Securities & Commissions.
IT	Information Technology
ISO	International Organization for Standardization
NIST	National Institute of Standards and Technology
PC	Personal Computer
SABRIC	South African Banking Risk information Centre (SABRIC)
SWIFT	Society for Worldwide Interbank Financial Telecommunications
SzCIRT	Eswatini Cyber Security Incident Response Team

TABLE OF CONTENTS

DECLARATION I

ABSTRACT II

PEER-REVIEWED PUBLICATIONS FROM THE THESIS III

ACKNOWLEGEMENTS IV

ABBREVIATIONS AND ACRONYMS VI

CHAPTER ONE 1

INTRODUCTION AND BACKGROUND 1

1.1 Introduction 1

1.2 Problem statement 3

1.3 Rationale and significance of the study 5

1.4 Aims and objectives of the study 6

1.4.1 Aim 6

1.4.2 Objectives 6

1.5 Research questions 6

1.5.1 Main research question: 6

1.5.2 Sub-questions 6

1.6 Preliminary Literature review 7

1.6.1 Cybercrime: Definition and conceptualisation 7

1.6.2 The role of the Internet and cybercrime activities 8

1.6.3 Cybercrime in the banking sector 9

1.6.4 The Eswatini Banking Sector 10
1.6.5 Types of cybercrime 10
1.6.6 A critique of related cybercrime 11
1.7 Definition of key concepts 12
1.7.1 Attacker 12
1.7.2 Cybercrime 13
1.7.3 Cybercriminal 13
1.7.4 Cybersecurity 13
1.7.5 Cyberspace 13
1.7.6 Insider Threat 13
1.7.7 Cyber Victim 13
1.7.8 Routine Activity Theory 14
1.7.9 Space Transition Theory 14
1.7.10 Threat 14
1.7.11 Deterrence Theory 14
1.8 Research paradigm, research methodology, research methods & research design 14
1.8.1 Research Paradigm 14
1.8.2 Research method 15
1.8.3 Research Design 16
1.8.4 Demarcation of the study 17
1.8.5 Study location and context 18

1.8.6 Conceptual framework and motivation for this study 18
1.8.7 Research processes 19
1.8.7.1 Population 19
1.8.7.2 Sampling 19
1.8.7.3 Data collection 20
1.8.7.4 Data coding and analysis 21
1.9 Ethical considerations 21
1.10 Summary of research questions 23
1.11 Outline of the dissertation 24
1.12 Summary of the chapter 25

CHAPTER TWO 26

LITERATURE REVIEW 26
2.1 Introduction 26
2.2 Cybercrime 26
2.2.1 Types of cybercrime 29
2.2.1.1 Identity theft 29
2.2.1.2 Denial of service (DoS) attack or distributed denial of service attacks 30
2.2.1.3 Malware 30
2.2.1.4 Pharming 30
2.2.1.5 Phishing 30

2.2.1.6 Ransomware 31
2.2.1.7 Hacking 32
2.2.1.8 Insider Threat 32
2.2.1.9 Card fraud 32
2.2.1.10 Cyber terrorism 33
2.2.1.11 Man in the middle attacks 33
2.3 Generation of cybercrime 33
2.3.1 First generation of cybercrime 33
2.3.2 Second generation of cybercrime 33
2.3.3 Third generation of cybercrime 34
2.4 The role of the Internet and cybercrime activities 34
2.5 Cybercriminals 35
2.6 Categories of cybercriminals 36
2.7 Cybercrime in a developing and developed countries 38
2.8 Current Global Cyberattacks in the Banking sector 39
2.9 Cybersecurity Frameworks 41
2.9.1 NIST Cybersecurity Framework 41
2.9.2 ISO/IEC 27001:2013 Standards on Information Security Management Systems 42
2.9.3 Center for Internet Security (CIS) 42
2.9.4 PCI-DSS 43

2.9.5 A framework for the Governance of Information Security in Banking system 43

2.10 Cyberspace and Cybercrime 43

2.11 Cybercrime in the banking sector 44

2.12 Eswatini and the Global view on Cybercrime 47

2.13 Cybercrime costs 48

2.14 Internet usage in Eswatini 48

2.15 Cybersecurity policy and strategy in Eswatini 48

2.16 Combating Cybercrime through existing frameworks 49

2.16.1.1 The Convention on Cyber Crime (Budapest Convention) 50

2.16.2.1 Global commission on the stability of cyberspace (GCSC) 50

2.16.2.2 Subcommittee on High -Tech crimes 50

2.16.3.1 The Paris Call for Trust and Security in Cyberspace 51

2.16.3.2 The Charter of Trust 51

2.16.3.3 Contract for the Web 51

2.17 Regional Initiatives to combat cybercrime in Africa 53

2.17.1 African Union Convention on Cyber security and Personal Data Protection – Malabo Convention 53

2.17.2 African Union Mechanism for Police Cooperation (AFRIPOL) 53

2.17.3 Interpol's regional Cybercrime strategy for Africa 54

CHAPTER THREE 56

THEORETICAL FRAMEWORKS **56**

3.1 Introduction **56**

3.2 Criminology **56**

3.3 Routine Activity Theory **56**

3.4 Deterrence Theory **60**

3.5 Space Transition Theory **63**

3.6 Theoretical framework similarities **65**

3.7 Theoretical frameworks differences **65**

3.8 Theories underpinning the study **65**

3.9 Conceptual Research Framework **66**

3.10 SUMMARY **67**

CHAPTER FOUR **68**

RESEARCH METHODOLOGY **68**

4.1 Introduction **68**

4.2 RESEARCH PHILOSOPHY **69**

4.2.1 Ontology **69**

4.2.2 Epistemology **70**

4.2.3 Axiology **70**

4.3 Research Approach **71**

4.4 Research Strategy **73**

4.5 Research Design **75**

4.5.1 Unit of analysis 75

4.5.2 Population 75

4.5.3 Sampling 76

4.5.4 Sampling method selected for this study 77

4.5.5 Participants 77

4.5.6 Data Collection Methods 77

4.5.7 Data analysis 79

4.5.8 Ethical consideration 80

4.6 SUMMARY OF THE CHAPTER 83

CHAPTER FIVE 84

DATA ANALYSIS AND DISCUSSION 84

5.1 Introduction 84

5.2 Analysis of the Qualitative data 85

5.2.1 The link between the themes and research objectives 86

5.3 INDUSTRY EXPERT'S FINDINGS 88

5.3.1 Demographics of the participants 88

5.3.2 Interview findings from industry experts 89

5.3.3 Emerging themes 89

5.3.4 Discussion of themes and sub-themes 90

5.3.4.1 Theme 1 – Competence in cybercrime awareness 92

5.3.4.1.1 Insufficient experience in cybercrime awareness 92

5.3.4.1.2 Cybercrime conviction 97

5.3.4.2 THEME 2 – Cybercrime Prevention 100

5.3.4.2.1 Internal threat control 100

5.3.4.2.2 Insufficient cybercriminal threat knowledge 103

5.3.4.2.3 Target attractiveness 110

5.3.4.3 THEME 3 – Cybercrime detection 116

5.3.4.3.1 Internal system control 116

5.3.4.3.2 Limited expertise in cybercrime investigation 120

5.3.4.3.3 Audit trail enforcement 125

5.3.4.4 THEME 4 - Cybercrime compliance 128

5.3.4.4.1 Change Management 128

5.4 Summary of findings 131

CHAPTER SIX 133

INTERPRETATION OF RESULTS AND FRAMEWORK 133

6.1 Introduction 133

6.3 Study Objectives 133

6.4 Interpretation of the study findings 134

6.4.1 Objective 1: To analyse the effectiveness of Space Transition in the combatting of cybercrime activities in the banking sector (Synonymous to Theme 1: Competence in cybercrime awareness) 134

6.4.2 Objective 2: To evaluate the effectiveness of Routine activity in the combatting of cybercrime activities in the banking sector (Synonymous with Theme 2) 137

6.4.3 Objective 3: To assess how deterrence theory of a financial institution can combat cybercrime (Synonymous with Theme 2 and 4) 142

6.4.4 Objective 4: To determine how banks in developing countries can minimize cybercrime activities in order to preserve their business (Synonymous with Theme 1, 2 and 3) 143

6.5 Conceptual Framework 144

6.5.1 The framework as recommendations 146

6.6 SUMMARY 151

CHAPTER SEVEN 152

EVALUATION OF THE RESEARCH, THESIS CONTRIBUTIONS, AND CONCLUSION 152

7.1 Introduction 152

7.2 The Research Problem 152

7.2.1 Study Goal 153

7.2.2. Primary Research Question 153

7.2.3 Sub research questions 153

7.3 Limitations of the study 155

7.4 Recommendations for future research 155

7.5 Thesis contributions 156

7.5.1 Theoretical 156

7.5.2 Practical 156

7.5.3 Methodological 157

7.5.4 Contextual 157

7.6 Conclusion 157

REFERENCES 158

ANNEXURE A: ETHICAL APPROVAL LETTER 202

ANNEXURE B: LANGUAGE EDITING CERTIFICATE 203

ANNEXURE C: INDUSTRY EXPERT INFORMATION AND CONSENT FORM 204

ANNEXURE D: INTERVIEW GUIDE 205

ANNEXURE E: VIRTUAL GUEST LECTURE POSTER 206

ANNEXURE F: LETTER OF APPRECIATION 207

ANNEXURE G: TURNITIN REPORT SUMMARY 208

LIST OF TABLES

Table 1.1: Eswatini bank fraud cases (Khumalo, 2019:3) 3

Table 1.2: Summary of research questions 23

Table 2.1: Global Projects addressing cybercrime 51

Table 3.1: Types of Guardianships 59

Table 3.2: Types of offenders (Sinca, 2015) 60

Table 3.3: Underpinning theories, concepts and approach 67

Table 4.1: Population and samples 77

Table 4.2: Summary of the research methodology 82

Table 5.1: Study objectives aligned with the theories 85

Table 5.2: Research objectives, themes and sub-themes 87

Table 5.3: Demographics of the industry experts 89

Table 5.4: Summary of Theme 1 – Cybercrime Awareness 91

Table 5.5: Summary of Theme 2 – Cybercrime prevention 99

Table 5.6: Summary of Theme 3 – Cybercrime detection 115

Table 5.7: Summary of Theme 4 – Cybercrime compliance 127

Table 6.1: Elements of the conceptualised framework 146

LIST OF FIGURES

Figure 1.1: The Kingdom of Eswatini Map 17

Figure 2.1: A circumplex model describing nine models of cybercrime, the skill level and motive (Rogers, 2010) 37

Figure 2.2: Cyberattacks in banks 46

Figure 3.1: Routine Activity Theory 57

Figure 3.2: Conceptual Research Framework 66

Figure 4.1: Sampling methods 76

Figure 5.1: Layout of Theme 1 with subthemes 92

Figure 5.2: Layout of theme 2 with subthemes 100

Figure 5.3: Layout of theme 3 with subthemes 116

Figure 5.4: Layout of theme 4 with subthemes 128

Figure 6.1: A cybercrime conceptual framework for Eswatini banks 145

Figure 6.2: Summary of the objectives, themes, theoretical lenses, findings and recommendations 150

CHAPTER ONE

INTRODUCTION AND BACKGROUND

1.1 Introduction

The number of people subscribed to the use of the internet, is a reflection of the many activities completed through this platform. The broadness of criminal activity on the Internet has been a result of all the elements of criminal activity migrating into cyberspace (Lewis, 2018:6). Sun, Shih & Hwang (2015:498) define cybercrime as a type of crime produced from the development of the internet and by utilising the Internet, cybercriminals use images, codes and any electronic communication in order to run malicious activities online (Arpana & Chauhan, 2012:4). This type of efficiency has also opened up other avenues for cybercriminals to exploit. Cybercrime has become one of those activities to conduct computer crime, hence it has transformed the way people interact with computers in their daily lives. Cybercrime in recent years has been referred to as crimes that occur over networks, particularly the Internet, however that term has gradually become a general synonym for computer crime (Alkaabi, 2010:1).

The banking sector in the mid-1990s was simple and reliable, however with the changes in technology, the banking sector experienced a paradigm shift (Jaleshgari, 1999:136). Latest technologies enabled banks to provide an enhanced customer experience allowing customers to have access to a wide variety of banking transactions ubiquitously (Vrancianu & Popa, 2010:389). However, such ease of access also gave rise to banking fraud allowing cybercriminals to exploit and use different ways to steal and manipulate customer and banking information (Choo, 2011:722). In 2018, the worldwide cost of cybercrime was approximately $600 billion (Muncaster, 2018:1), since cybercriminals are using different means to steal customers' bank information, money and bank sensitive information (Choo, 2011:725). In the African continent, the cost for cybercrime was estimated at $3.5 billion in 2017 (Dahir, 2018:1). The South African Banking Risk information Centre (SABRIC) states that South Africa loses approximately $157 million annually to cyberattacks (Kshetri, 2019:1).

Banks are defined as financial institutions that are licensed to receive payments, issue out loans, provide investment and currency exchange services to customers (Barone, 2021). The banking activities or functions are mandated by law (Keranen, 2022) and are supported and maintained by the Information Technology Departments or units (Bishnoi & Devi, 2017). For a number of years, the banking industry has gone through a severe transformation in order to improve service delivery capacity and the Information Technology departments or units have contributed in achieving that role (Harguem & Echatti, n.d). Erhabor (2008:37) describes cybercrime as one of the fastest growing criminal activities on the planet that covers a large range of illegal activities including financial scams to virus attacks. Ayofe and Oluwaseyifunnmitan (2009:154) define cybercrime as crime that is conducted in a virtual space where information about people, objects, facts, events phenomena or processes are represented in mathematical or as symbols and basically transferred through local and global networks. In the financial sector particularly the banks, these include unauthorised access to users' confidential data, Denial-of-service (DOS) attacks, virus dissemination, online frauds, system interruption, money laundering and hacking (Gordon, Loeb & Sohail, 2003:81 - 85).

Financial institutions worldwide face a problem in addressing cybercrime. In Pakistan, cybercrime incidents in the banking sector were a result of a lack of information security awareness application amongst banking employees (Malik & Islam, 2019:50). The Central Bank of Nigeria developed a risk-based cybersecurity framework for banks and financial institutions to identify the existing gaps within the cybercrime space (Kshetri, 2019:79). Bangladesh Central Bank was a victim of the largest bank heist in history, where hackers exploited a loophole in the SWIFT transfer system, as a result of a basic query spelling mistake (Borg, 2019:1). In the Southern African region, South Africa has the third highest prevalence of cybercrime in the world, following Russia and China (Sulfab, 2014:9), while Nigeria is ranked first in the African continent in the rate of cybercrime prevalence (Akuta, Ong'oa & Jones 2011:132). In the Kingdom of Eswatini, the Central Bank of Eswatini fell victim to cybercrime of data breach and fraud in 2013 and 2016, and it resulted in a loss amounting to E7.5 million, although the fraud attempt totalled E21 million (Thwala, 2019:15).

Eswatini banks also became victims of fraud between the years 2015 and 2017. In February 2015, Wesbank was defrauded of close to E3 million by a couple, in July 2015, a former Wesbank employee was arrested for E482 422, in July 2016 six (6) people were arrested for E20 million fraud at the Central Bank and in January 2017, E4.2M fraud was discovered at FNB (Khumalo, 2019:3).

Table 1.1: Eswatini bank fraud cases (Khumalo, 2019:3)

Year	Type of Crime	Name of Bank	Amount
February 2015	Fraud	Wesbank	E3 million
July 2015	Fraud	Wesbank	E482 422
July 2016	Fraud	Central Bank	E20 million
January 2017	Fraud	FNB	E 4.2 million

1.2 Problem statement

Cybercrime is a global problem that affects all industries, and it is progressing at a fast pace, with new criminal trends that are constantly emerging. Cybercriminals are demonstrating a growing knowledge of the banks' financial systems and the potential weaknesses that exist (KPMG, 2018:5). The increased adoption of technology by financial institutions especially banks has elevated countries' cyber-attacks risk, further exposing them to financial customer loss (Munda, 2019:1). The problems associated with cybercrime are normally research based, therefore, to address the cybercrime phenomenon in the Kingdom of Eswatini following a similar approach.

The main reason for following this kind of approach was to identify the research gap for this study. Various authors have conducted academic studies in cybercrime particularly in the financial sector. Lagazio, Sherif & Cushman (2014) investigated on the effects of cybercrimes on the financial sector, and findings revealed that inflated expenses on cybercrime defense and under reporting of cyber-crime incidents are the major behaviours of financial companies. Lubua (2014:47) concludes that the lack of

cyber laws in Tanzania has resulted in the violation of clients' rights in maintaining their information.

Cybercrime is a growing threat, since people and organisations rely more on the Internet on a daily basis, and because of its global nature it differs from other transnational crime problems compared to cybercrime (Bande, 2018:11). In financial institutions especially banks, customers are able to access different services without the need of visiting the physical bank premises. However, this convenience comes with the risk of cyber-attacks. With a high number of cybercrime incidents such as phishing, viruses, hacking, there is a need to explore and analyse the cybercrime scenario in the banking industry. Developing countries are normally a vulnerable target for cybercrime, due to structural and institutional imbalances (Antonescu & Birau, 2015:621). Cybercrime has become a tremendous threat in today's digital age and the estimation cost of cybercrime will grow from $3 trillion in 2015 to $6 trillion by the year 2025 (Morgan, 2017:1). Banking is the business activity of accepting and safeguarding money owned by other individuals and entities, and then lending out this money to earn a profit. However, this activity over time has been exploited by cyber criminals resulting in major disruptions including financial losses and trust issues in their operations.

While banking entities have initiated various means to address this issue with limited outcomes, the problem persists. Law enforcement agencies and bodies over the years have not been able to deal with cybercrime effectively, particularly in developing countries, due to the slow technology adaptation (Sussmann, 1999:465). Low technological literacy of users and the exposure of technical security system loops are other factors that contribute towards the rise of cybercrime (Lubua, 2014:39). This is because there is no known framework that may help address these issues for banking in the context of Eswatini. Cybercrime costs have quadrupled from the years 2013 to 2015 and there are predictions that from 2015 to 2019, there will be another quadrupling and the trend is that such activities end up undetected (Arcuri, Brogi & Gandolfi, 2017:175).

There is insufficient literature that addresses the cybercriminal activities particularly in the context of Eswatini Banks. A gap that has been identified is that there is limited

research conducted that relates to the cybercrime phenomenon specifically in Eswatini Banks, which makes this case study a unique one.

The main research problem is the lack of literature in addressing the cybercrime activities in Eswatini Banks. This study thus attempts to develop a conceptual framework from the perspective of Eswatini Banks using the space transition theory, deterrence theory and routine activity theory.

In order to address the gap in the body of knowledge, this study will explore and contextualise the cybercrime phenomenon from the perspective of Eswatini Banks using the space transition theory, deterrence theory and routine activity theory. This study therefore proposes to develop a conceptual framework that might address this issue. This study sought to explore and analyse the cybercrime phenomenon and leads to providing measures that the banks in Eswatini can adopt to minimise their risk and exposure to cybercrime.

1.3 Rationale and significance of the study

This study ought to bridge the gap in knowledge concerning the cybercrime phenomenon, through the use of the space transition theory, deterrence theory and routine activity theory to gain more understanding by applying these different theoretical lenses. The study led to the formulation of a cybercrime framework that will be useful in predicting new ways to understand and fight cybercrime activities in the context of the banking sector.

The rate at which cybercrime is growing as well as the slow progress in implementing counteractive solutions, has become a concern for individuals and organisations, therefore the findings will provide an insight and more options to combat the cybercrime epidemic. In addition, the findings provided a basis for future studies to enhance the understanding of cybercrime activities in the banking sector and how it affects the business banking processes. This included an attempt to explain individual and collective behaviors that influence the occurrence of cybercrime attacks.

This study focused on banks in the Kingdom of Eswatini. Furthermore, the study output provided a basis for future studies on the cybercrime phenomenon in other countries and organisations. Swaziland loses approximately E40M yearly through cybercrime (Nhlabatsi, 2017:3) and the Government of Eswatini has made attempts to address this issue by drafting the Computer and Cyber Crime Bill which is awaiting validation from stakeholders. Besides the draft bill, (COE, 2019) Eswatini does not have any other legislation which focuses on cybercrime.

1.4 Aims and objectives of the study

1.4.1 Aim

The study aimed to bridge the gap by providing an in depth and detailed understanding of cybercrime activities in Eswatini Banks, and to conceptualise a cybercrime framework

1.4.2 Objectives

- To analyse the effectiveness of Space Transition in the combatting of cybercrime activities in the banking sector.
- To evaluate the effectiveness of Routine activity in the combatting of cybercrime activities in the banking sector.
- To assess how deterrence theory of a financial institution can combat cybercrime.
- To determine how banks in Eswatini can minimise cybercrime activities in order to preserve their business.

1.5 Research questions

1.5.1 Main research question:

How should a cybercrime framework for Eswatini be conceptualised?

1.5.2 Sub-questions

- How effective is Space Transition in combatting cybercrime in the banking sector?

- How can Routine Activity be utilised in combatting cybercrime in the banking sector?
- How can the Deterrence theory assist in combatting cybercrime activities in banking?
- How can banks in Eswatini minimise cybercrime activities in order to preserve their business?

1.6 Preliminary Literature review

1.6.1 Cybercrime: Definition and conceptualisation

The definition of cybercrime is still not clear and has been a countless debate on what institutes cybercrime. Several nomenclatures have been used such as computer crime, computer-related crime, digital crime and information technology crime to accommodate the various forms of cybercrimes and motives (Maat, 2004:239). Cybercrime is different from other types of crimes, and the difference is that cybercrime is mostly associated with the usage of a computer. It is also defined as crime committed through the use of PCs and other IT devices (Gordon & Ford, 2006:14). Britz (2009:15) argues that cybercrime comes in the form of abusing and misusing computer systems connected to the Internet, which results indirect or indirect losses. Kranenbarg, Holt and van Gelder (2019:41) state that cybercrimes have a tendency to be committed in a different context compared to traditional crimes, leading to various risk factors for the offenders and victims. Cybercrime, also called digital crime was different and varied since 1960 to the present day. In the early era of information systems, computer crimes were committed by some employees, and also physical attacks on a computer system was common in the time between 1960 and 1980. In 1980 malicious software began to appear within personal computers. In the beginning of 1990s, the internet had been a significant factor of increasing digital crimes; criminals had access to poorly protected systems using unauthorised ways normally for financial gain and credit-fraud. By the end of the 20th century and beginning of the 21st, credit card fraud evolved into a broader category called identity theft, whereby criminals were stealing identities of other people to conduct illegal activities. Choo (2011:720) posits that cybercrime is not a victimless crime and its impact falls under two categories which are:

Short term impacts: These types of impacts consist of daily activities of individual users which include ATM usage and viewing of recent financial information.

Long term impact: These include day-to-day activities of businesses and government.

Africa as a developing continent, faces a challenge to control and prevent cybercrime when compared to the rest of the world (Mugari, Gona, Maunga & Chiyambiro, 2016:135), and the contributory factors include the growth in Internet usage, poor security awareness, lack of law enforcement training and limited regulation (Olowu,2009:4-5).

The banking sector during the mid-1990s was simple and reliable, however with the arrival of technology, there was a paradigm shift (Jaleshgari,1999:136). Banks experienced competition from other industry players and in order to maintain and enhance their customer base, they had to introduce several platforms whereby transactions could be performed more easily (Vrancianu & Popa, 2010:390).

These platforms enabled customers to access their finances during daylight and at night, throughout the year irrespective of location. This poses a risk to the stability to the whole banking and financial sector due to the increasing cyberattacks in scope, numbers and sophistication making it difficult to predict the overall impact (Boer & Vazquez, 2017:1).

1.6.2 The role of the Internet and cybercrime activities

The internet over the years has changed the way human beings interact and view life, and the impact it has on our daily lives is impacted by the cyberspace that surrounds us. Cybercrime and traditional crimes are similar, but cybercriminals are more involved in cybercrime because of the availability of the Internet. The Internet was never designed with security in mind and that opens up opportunities for hackers and cybercriminals to take advantage (Van Ommeren, Borrett & Kuivenhoven, 2014:36). A contributing factor is that cybercriminals have become versatile and specialised in executing crimes in the cyberspace. (Kirgel, 2012:470). The role of the Internet has

enabled the transformation of cybercrime activities in generational stages. The first generation of cybercrime occurred within discrete computing systems and was characterised by exploitation activities. It paved the way for departure from conventional criminal activity. The second generation of cybercrime occurred across networks, and involved acts such as hacking and cracking. The third generation is characterised by its dispensed and automated nature of computer systems interaction (Wall, 2007:44-47).

1.6.3 Cybercrime in the banking sector

An increase and adoption of digitalisation by organizations results in an increase in cybercrime, due to the reliance and adoption of digital systems and networks for their business operations (Staal, 2015:11). The concentration of financial wealth in banks is one driver of cybercrime, providing a fertile ground for crime, and high potential for targeting by cybercriminals (Herlseman & Warren, 2004:260). The high volume of sensitive customer information processed through settlement and payment systems is also a major factor in the rise of cybercrime (Khan, 2018). Less developed countries are often exploited by cybercriminals due to their weak security controls, and these exploitations are then used to target more developed countries to gain access to their systems (Lakshmanan, 2019:1). The banking sector's involvement with the digital world has left it more vulnerable to cybercrime. Banks provide many services to customers in order to keep up with the digitisation era. Financial institutions now operating across various jurisdictions, are at risk as online banking, frequent international transactions, innovative payment methods such as PayPal, and existence of databases in banks provides easy targets and high profits (Oliveria & Stickings, 2016:17). It has become necessary to protect financial institutions from the antics of cybercriminals, due to the pivotal roles of banks in the growth and economic development of any nation (Ikechi & Okay, 2013:254), since banks remain the favourite target of skilled cybercriminals (Lewis, 2018:9).

The impact of cybercrimes in banks often leads to the failure to complete business and financial contracts created to deliver goods and services as well as intellectual property rights abuse. Banks are the most targeted due to the cybercriminal's intention to damage the reputation of such firms (Onchomba, 2018:3). One of the main factors

contributing to the rise of cybercrime is the low level of digital literacy of bank customers in utilising banking products (Kovalova & Kovalova, 2021). Crimes committed in the financial sector are considered to be among the most dangerous economic crimes, since the negative impact is often reflected not only to the financial institution system but also to other economic entities (Kovalova & Kovalov, 2021).

1.6.4 The Eswatini Banking Sector

The Eswatini banking sector is a highly regulated environment, and it complies with numerous pieces of legislation and regulations. To address such crimes, the Kingdom of Eswatini has instituted some legislative measures which include the Financial Institutions Act No.6 of 2005, The Money Laundering and Financing of Terrorism (Prevention) Act of 2011, Prevention of Organized Crime Bill and Draft Computer Crime and Cybercrime Bill, 2013 and the Electronic Communications and Transactions Bill of 2017 (Government of Eswatini, 2019:1). These provisions or instruments also need to be aligned to both regional (within SADC) and international norms (including the Budapest convention), criminalise malicious cyber activities in Eswatini, and improve the investigation and prosecution of cybercrimes (Eswatini National Cybersecurity Strategy, 2020).

1.6.5 Types of cybercrime

Cyberattacks can be conducted in many forms and methods and the level of complexity ranges from simple to a very high level of sophistication, which normally requires programming skills. There are many types of cybercrimes and according to Aggarwal, Arora, Neha and Ponam (2014:48-49) they are defined as follows:

- Hacking: the illegal access or entry into a computer system through the usage of a variety of softwares.
- Cyber stalking: this is an online harassment where the victim is exposed to a bombardment of messages and electronic mail.
- Virus Dissemination: this software maliciously attaches itself to other computer softwares. Such viruses include worms, Trojan horse, time bomb and logic bomb.

- Denial of Service attack: this is whereby the cybercriminal fills the victim's e-mail with spam messages with the intention of depriving the user access to computer and network services.
- Software piracy: this is the illegal copying for original programs and thereafter distributing them.

Different studies reviewed in the literature in the previous sections, all conclude that cybercrime is an ever growing and evolving phenomenon, and organisations are facing ~~a~~ difficulty in keeping up. Moreover, there are various factors identified that are contributing factors to the spreading of cybercrime which are mostly focused in more developed countries. Africa has limited research done on cybercrime and Quarshie and Odoom (2012:98) further state that a lot of cybercrime emanates from the African continent accompanied by threats that are easily spread due to poorly protected computer systems, hence there is a need to address this problem. The literature identified a trend that most of the studies especially in the African context, applied only a few criminology theories in their research in order to obtain an in depth understanding of cybercrime activities in varied sectors.

1.6.6 A critique of related cybercrime

Various studies on cybercrimes in the financial and banking sector have been conducted in order to analyse challenges across Europe, Asia and Africa. A study done by Mugari, Gona, Maunga and Chiyambiro (2016:135) in Zimbabwe revealed that hacking, phishing, identify theft and malware were the most common types of cybercrime that affected banks. The same study further revealed that the cyber security systems installed by financial institutions were not sufficient to address cybercrime incidents, as they lacked in meeting the technological advancement pace.

Siddique and Rehman (2011:159-164) conducted research that focused on establishing the impact of cybercrime within the banking sector in India. The aim of the study was to determine how online criminal activities affect the banking sector with the aim to eliminate cybercrime. The findings from the study showed that banks incurred enormous costs to criminal activities which affected customer confidence towards banks.

Sawaneh (2018:23-27) conducted a study focusing on the effects and challenges of cybercrime in Sierra Leone. The study showed that the country had weak laws regarding cybercrime and cybersecurity, and most of the citizens in the working environment had limited knowledge on how to address cybercrime issues. The study proposed that stronger regulations, policies and laws should be enforced. Matthew (2016) examined the sociological and technological factors of cybercrime in Nigeria by using theoretical and investigative points of views. The findings from the study define cybercrime as a threat to a nation's economy, therefore there is a need for a holistic approach to combat crime.

Olowu (2009:3) posits that the reliance on obsolete cybercrime laws by most African nations affects the way cybercrime is understood and eventually addressed. He further states that African states should learn from others and prepare themselves for the everchanging cybercrime phenomenon.

The cybercrime concept has attracted a lot of discussions among academia and industry due to the evolving and unpredictability of cybercrime cases especially in the banking sector. Various studies that have been conducted worldwide have outlined various reasons of why and how cybercrime occurs and the impact that it has. A majority of these studies are international, while a few are particularly African focused. Based on these theoretical and contextual gaps, this study further seeks to create a conceptual framework to address cybercrime in the financial sector in Eswatini Banks through the theoretical lenses of the social activity theory, space transition theory and deterrence theory.

1.7 Definition of key concepts

1.7.1 Attacker

An attacker is the individual or organization who performs the malicious activities to destroy, expose, alter, disable, steal or gain unauthorized access to or make unauthorized use of an asset (Javapoint, 2024)

1.7.2 Cybercrime

Cybercrimes are criminal activities that are accomplished through the utilisation of cyberspace as a medium of communication (Dalla & Geeta, 2013:997). Quarshie and Odoom (2012:98) define cybercrime as an activity that involves both the computer and the person, and both are classified as victims, while Hassan, Lass & Makinde, (2012:626) simply define cybercrime as crimes carried out with the assistance of a computer system. For the purpose of this study, cybercrime is defined as a crime facilitated through the use of a computer.

1.7.3 Cybercriminal

A cybercriminal is a person that seeks financial profit by stealing and selling information using different methods (Sabillon *et al.,* 2019)

1.7.4 Cybersecurity

Cybersecurity defined as the specifications of security requirements to prevent unauthorized intrusions access to an individuals' computer or server (Jang-Jaccard & Nepal, 2014).

1.7.5 Cyberspace

Cyberspace is a global domain within the information environment consisting of a network of information technology infrastructures, including the Internet, telecommunication networks, computer systems, and embedded processors and controllers (Lippert & Cloutier, 2021).

1.7.6 Insider Threat

This is a malicious threat that happens inside the organization, whereby the employee misuses the systems through authorized access (Devi & Mohankumar, 2019).

1.7.7 Cyber Victim

This refers to any person who has been defrauded financially through the Internet (Ennin, 2015:9).

1.7.8 Routine Activity Theory

The convergence of motivated offenders and suitable targets within unguarded or unprotected systems of networks that creates an opportunity favourable to victimization (Reyns, 2013:221).

1.7.9 Space Transition Theory

The space transition theory explains the nature of the behaviour of the persons who bring out their conforming and non-conforming behaviour in the physical and cyberspace. This involves the movement of persons from one space to another physical space to cyberspace and vice versa (Jaishankar, 2008:292-296).

1.7.10 Threat

Threat is a circumstance or event that has or indicates the potential to exploit vulnerabilities and negatively impact organizational operations, organizational assets, individuals, other organizations, or society (Lechner, 2017).

1.7.11 Deterrence Theory

A concept that focuses on the use or the threat of punishment with the intention of people to evade breaking the law that oversees the coexistence of a society (Schneider, 2019:1).

1.8 Research paradigm, research methodology, research methods & research design

1.8.1 Research Paradigm

Kivunja & Kuyini (2017:26) define research paradigm as a conceptual lens through which a researcher scrutinises and observes the various methodological aspects of that particular research project in order to determine the applicable research methods that will be used and how the analysis of data will be done. For research purposes, there are more than two research paradigms and the most prominent ones are interpretivism and positivism research paradigms. In positivist paradigm, the research

is conducted in order to observe, measure and predict the empirical phenomena as well as to build tangible, material knowledge (Tracy, 2013:39).

The researcher remains detached, neutral and objective as he or she examines the evidence and replicates the research of others (Neuman, 2014:102). In interpretivist paradigm the intention is to obtain an understanding of the world of human experience (Cohen & Manion, 1994:36).

Mackenzie and Knipe (2006) support the interpretivist research paradigm as one that is suitable for a case study method to observe trends in data as patterns of meaning. Below is the justification for selecting the interpretivist research paradigm ~~is~~:

- The concept of cybercrime is a well-known phenomenon, however very little empirical research is available, therefore the qualitative research method to be used in this study will provide a deep understanding of the factors that lead to cybercrime activities from a viewpoint of Eswatini banks using the three theories.
- The study will adopt the interpretivism research paradigm and it is suitable because it is context specific and focuses on the banking sector in the Kingdom of Eswatini.
- The primary data will be collected from participants who are involved in cybercrime issues and have extensive knowledge of this phenomenon.
- The case study will be on Eswatini Banks and the primary data collection tool will be interviews and observations.
- The objective of this study is to explore and evaluate the effectiveness of the cybercrime phenomenon through the lens of the routine activity, space transition and deterrence theories.

1.8.2 Research method

There are three common research approaches namely; quantitative, qualitative and mixed method. A qualitative approach is useful in exploring and understanding individuals or social groups or human problems (Creswell, 2009:183) while quantitative approach is used when researchers want to test objective theories by

examining the relationship among variables. In this study, the qualitative approach was used. Kothari (2007:5) emphasises that the qualitative approach focuses on the subjective assessment of attitude and behaviour. The justification for selecting the qualitative method is that it will help to provide a profound understanding of the factors that lead to cybercrime activities from a perspective of banks in Eswatini using the three theories.

This study is also context specific and focuses on the banking sector where the data obtained will be of high quality. The objective of this study is to analyse the effectiveness of the routine activity, space transition and deterrence theories in combatting cybercrime activities in the banking sector, and since cybercrime is a unique specific and evolving phenomenon, the selected qualitative approached is suitable.

1.8.3 Research Design

Research design is defined as the overall plan for addressing a research question and it normally includes specifications that enhance the integrity of the study (Polit & Beck, 2012:741). A case study is an empirical research strategy used to intensely study a phenomenon over a given period in its natural setting in one or more sites (Yin, 2003:47-49). The objective of this study is to conceptualise a cybercrime framework for Eswatini banks and according to Yin (2013:47-50), a single case may be considered when the case is unique, revelatory or longitudinal, which is the current case with cybercrime.

Due to the nature of this study, the case study strategy has been selected as it is more suitable for complex social phenomena, which normally are not easily explained using methods such as quantitative, and the aim is to answer questions such as “how” or “why”. Bhattacherjee (2012:93) also views the use of a case study as the most suitable for the characteristics of this kind of study in the sense that a case study will supply answers to the “how” and “why” questions. In terms of context, a case study is suitable when certain variables within the study are not previously known (Eisenhart & Graeber, 2007:28). The researcher will have no control over the phenomenon under investigation and also the opportunity to control the participants of the study on how

they perceive the cybercrime perception in Eswatini Banks. The researcher will take the place of a viewer or outsider to the phenomenon therefore this makes the case study suitable.

1.8.4 Demarcation of the study

The location of this study will be in the Kingdom of Eswatini which is landlocked, bordered by South Africa to the North, South and West and Mozambique to the East. The surface area is 17,363 square kilometres. The country has four regions, Hhohho, Manzini, Shiselweni and Lubombo. There are five (5) main banks and a Building society in the Kingdom of Eswatini, namely FNB, Nedbank, Standard Bank, Swaziland Building Society and SwaziBank. The building society is called Status Capital Building Society. It is worth mentioning that Swaziland Building Society is in the process of converting from a society to a bank. The banks and the building society have branches all over the country. Hhohho region is where the headquarters of all the banks are situated. The capital city being Mbabane, has approximately a population of 68,000.

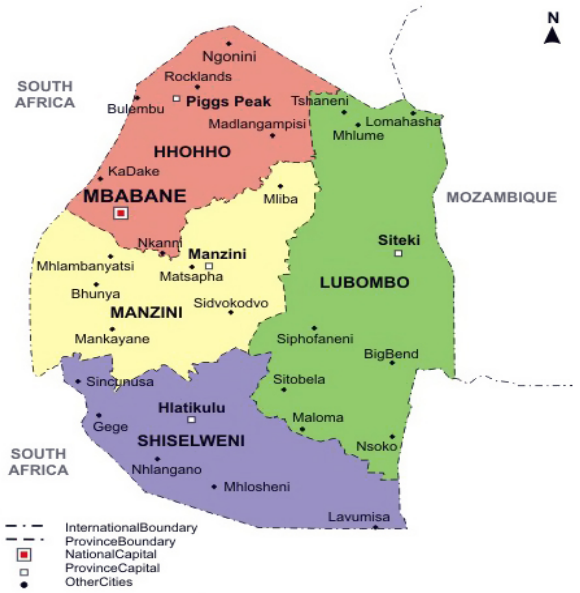


Figure 1.1: The Kingdom of Eswatini Map

The Kingdom of Eswatini has a population of about 1.1 million, with 36.6% of the population under the age of 15 years. Seventy-seven (77%) percent of the country's population resides in rural areas and 23% in urban settlements. The country is classified as a lower-middle-income country with a gross domestic product of $3,03 per capital. The economic activity in the country, measured by real GDP is projected to decline by 0.4% in 2018. The World Economic Forum's Global Competitiveness report (2012 to 2013) ranks Eswatini in a solid 46th position out of 144 countries in terms of soundness of banks. The 2011 World Bank's ease of doing business index shows Eswatini as 13th out of 46 sub-Saharan African nations in overall ease of doing business. Eswatini has already developed the Draft Computer Crime and Cybercrime Bill of 2017, Data Protection Bill of 2017 and the Electronic Communications and Transactions Bill of 2017.

1.8.5 Study location and context

The context of the study is cybercrime in the banking financial sector. The study location is the Kingdom of Eswatini.

1.8.6 Conceptual framework and motivation for this study

A conceptual framework is a network of a plan of interconnected concepts that offer an understanding of a particular phenomenon (Jabareen, 2009:51). It shows the relationship between concepts and their impact on the particular phenomenon that is being investigated (Ngulube, Mathipa & Gumbo, 2015:47). Therefore, in the Kingdom of Eswatini, the banking sector is one segment in the economy space that has a huge gap to fill by addressing the cybercrime issue through the theoretical lens of the three theories. The conceptual framework for this study will be based on the Routine Activity Theory, Deterrence theory and Space Transition Theory, and these theories will be used to analyse cybercrime in the banking sector, from the perspective of Eswatini country.

The routine activity theory attempts to explain human behaviour when an interaction takes place between the subject and its world. The assumption is that a constant supply of motivated offenders affects the behaviors, activities and situational contexts that create a possible target for victims (Pratt, Holtfreter & Reisig 2010: 273). The space transition theory explains the nature of the behaviour of the persons who bring out their conforming and non-conforming behaviour in the physical and cyberspace. This involves the movement of persons from one space to another physical space to cyberspace and vice versa (Jaishankar, 2008:292-294).

1.8.7 Research processes

1.8.7.1 Population

Population is defined as the abstract idea of a large group of many cases from which a researcher is able to draw a sample for which the results are to be generalized (Neuman 2014:247). Hanlon and Larget (2011:7) further describe a population as that which consists of all the individuals or units of interest relevant to the study, and the study sample refers to a subset of the individuals in a population. Kothari (2007:152) defines sampling as the process of obtaining information about an entire population by examining only a part of it for the purpose of the study. Babbie (2010:188) defines sampling as the process of selecting observations. Purposive sampling was adopted for this study, since it will be addressing the cybercrime phenomenon in the banking sector.

1.8.7.2 Sampling

The key participants in this study will be specialist employees from departments in the banks, stakeholders that are mandated to address cybercrime issues and tasks. These participants are the ones who are solely responsible and have a vested interest and knowledge in curbing cybercrime in the best interest of the banks. The participants were purposively selected based on their experience, familiarity and knowledge of the banking sector, particularly in the cybersecurity and cybercrime space.

The researcher targeted five (5) industry experts from different financial institutions to give credibility to the study and also to solicit their expertise and suggestions on how a cybercrime framework for Eswatini Banks could be created. The criteria for the expert's selection was based on their knowledge on cybercrime awareness, detection, prevention and compliance.

Purposive sampling is mostly used to select members of a difficult-to-reach and specialised population (Neuman 2014:274) and in this study, the specific participants were selected from the banking sector in Eswatini based on the nature of their jobs and the activities that are aligned with cybercrime activities. The participants also need to satisfy the characteristics of the phenomenon under investigation. The justification of using purposive sampling was to ensure that the experiences and views of the participants really address the cybercrime objective of the study, once the data saturation was reached. Fusch and Ness, (2015:1408) claim that "failure to reach saturation has an impact on the quality of the research conducted". Given (2016:135) considers saturation as the point at which "additional data do not lead to any new emergent themes". When the researcher during interviews begins to hear the same comments repeatedly, data saturation is reached (Grady, 1998:26).

The response rate was 100% and it was accomplished through self- administration of the interview guide, constant notification of the participants and a positive interest of the participants in the research.

1.8.7.3 Data collection

Data was collected through face-to-face in-depth interviews. The researcher conducted the interviews himself. The researcher had a list of questions and utilized an interview schedule to obtain answers from the identified participants. The participants were contacted telephonically to set appointments on dates, time and location most suitable for them. Data was collected after the process of collection and terms of agreement was explained.

The participants were contacted telephonically to set appointments on the date and location most suitable to them. Data collection was collected once permission had been granted from the relevant stakeholders. Consent was sought from the study participants prior to data collection. Each interview was tailored to suit the interviewee and researcher, depending on their job detail and work-related cybercrime experience. A one-on-one interaction approach was adopted to ensure that the data is captured as much as possible.

1.8.7.4 Data coding and analysis

Data analysis means to systematically organize, integrate and examine the patterns and relationships in the data in order to connect the particular data to concepts, generalisations and themes (Neuman, 2014:477). The raw data was captured, organized and prepared for analysis. The data were then coded to categorise similar responses and ideas to form themes. To aid the researcher in the development of theme clusters, the researcher will read the transcripts several times in order to identify recurring statements and themes from the data collected. Linneberg and Korsgaard (2019: 259-260) reiterates that coding involves providing each unit of data within a data item a code that summaries the extract's meaning. The overall aim is to make data of interest to be accessible for further analysis (Saunders *et al.,* 2016:581)

1.9 Ethical considerations

Cybercrime is a sensitive topic and ethics need to be highly considered in this study, as there is always a concern about breach of company and individual confidentiality. Therefore, the following measures will be taken in this study to address the issue, and the researcher will conduct this study in a responsible and respectful manner.

- Informed Consent

The researcher informed the participants of their rights, the nature of the study and benefits of participating. The researcher made sure that the participants were informed that participation was voluntary and withdrawal from the study process will be allowed. Prior to participating in the study, the participants were made aware of the consent forms.

- Confidentiality, Privacy and anonymity

The researcher and participants must have clear understanding regarding the data, results and findings of the study (Maree, 2010:301). The researcher will see to it that all the participants' information is not shared and is kept private, the principle of anonymity shall be applied. Regarding privacy, the responses from the participants was used for this study.

- Respect and trust

The researcher should strive to gain support through trust and respect by conveying to the participants the objective of the study explicitly (Creswell, 2013:174) The researcher will see to it that time is respected and that participants are appreciated by ensuring that the interview conversation space is friendly, and the participants must be able to feel at ease. This is to ensure that full cooperation and a high level of professionalism is expected from the researcher in order to gain trust and respect from the participants. The researcher held preliminary discussions with the participants before the commencement of the actual data collection exercises. This is to ensure that the participants do not feel as if they are being victimised or forced into taking part in the study. In addition, the participants were given the opportunity to fully scrutinise the intention, purpose and impact of the study that they are requested to be part of. During the data collection process, the researcher ensured that questions are asked in a clear and proper manner and solely focused on the subject being investigated. To further ensure trust, the researcher will not surprise the participant with questions or any content that is not relevant to the study.

- Researcher's role

The researcher coordinated all the activities of the study. The role of the researcher in the study is to create a partnership with the participants during the collection and analysis phases of the study (Maree, 2010:41).

The researcher will see to it that preparation and collection of data, interaction with participants during interviews, appointment scheduling and data analysis are all managed and controlled by the researcher at a high level of integrity, professionalism and ethical application.

- The researcher will present an ethical certificate from the university to relevant authorities seeking permission to conduct research among identified banking employees and stakeholders,
- Names of participants will not to be revealed to anyone, the use of pseudo names will be applied,
- Participants will be informed that their commitment to participate in the study can be reversed that is, they can withdraw from the study at any point.
- Assurance will be given to the participants on the confidentiality of the data collected,
- An agreement of informed consent that details the ethical protocols will be observed and signed by the participants prior to issuing or utilisation of the data collection tools.

1.10 Summary of research questions

The table below summarises the research problem, questions, sub-questions, methods and objectives.

Table 1.2: Summary of research questions

Research Question	**How should a cybercrime framework for Eswatini be conceptualised?**	
Research sub questions	**Method**	**Objectives**
How effective is Space Transition in combatting cybercrime in the banking sector?	Interview	To analyse the effectiveness of Space Transition in the combatting of cybercrime activities in the banking sector.
How can Routine Activity be utilised in combatting cybercrime in the banking sector?	Interview	To evaluate the effectiveness of Routine activity in the combatting of cybercrime activities in the banking sector
How can the Deterrence theory assist in combatting cybercrime activities in banking?	Interview	To assess how deterrence theory of a financial institution can combat cybercrime.
How can banks in developing countries minimise cybercrime activities in order to preserve their business?	Interview, Literature study	To determine how banks in developing countries can minimise cybercrime activities in order to preserve their business

1.11 Outline of the dissertation

This study sought to explore and analyse the cybercrime phenomenon, leading to providing measures that banks in Eswatini can adopt to minimise their risk and exposure to cybercrime. The theoretical lenses for this study are the Routine Activity theory, deterrence theory and space transition theory. The chapter introduced the research background to the field of study in the cybercrime space. The next chapters are structured as follows:

Chapter Two – Literature review
This chapter will contain the introduction, problem statement and significance of the study. The key concepts of cybercrime will be discussed and conceptualised with reference to existing literature.

Chapter Three – Theoretical frameworks
This chapter discusses and describes the theories which underpin the study, two of them being criminological theories and the other a social theory. A discussion on the routine activity theory, space transition theory and deterrence theory, and how they interlink and complement one another as theoretical lens for cybercrime will follow. The different parts of each of the theories will be used to explain the aspects of the topic in this study.

Chapter Four - Methodology
This chapter will contain the methodology used in the study. It will also provide an outline and explanation of the research approach, research questions and data collection methods.

Chapter Five– Empirical results and discussion of data collected
This chapter will deal with the conclusions to the study and recommendations to the various role players in the cybercrime space and for research for further studies. The qualitative data that will be collected will describe the experiences and themes of the participants and entities interviewed. In this chapter the findings will be linked with the conceptual framework and literature review. Ethical considerations will be followed throughout the data analysis process.

Chapter Six – Interpretation of results and development of the framework
This chapter serves to conclude and give a summary of the study. The findings and recommendations will be included to provide a well-defined understanding of how the objectives were gathered in order to achieve the aims of the study.

Chapter Seven – Evaluation of the research
This chapter will discuss the contribution of the study, intended goals and objectives. Recommendation will be offered on the basis of what will be revealed from the findings.

1.12 Summary of the chapter

This chapter introduced the thesis and gave background to the research problem. The problem statement was also specified, followed by the purpose of the study and significance. The research's main goal and objectives are clearly stated as well as the main and sub-research questions. A preliminary literature review was provided to connect the study's main phenomenon to the current and past research information. The study concepts were also defined, followed by the research paradigm, method, study demarcation, sampling and data collection method. The chapter was finalised with a discussion of ethical issues. The next chapter reviews the literature.

CHAPTER TWO

LITERATURE REVIEW

2.1 Introduction

The preceding chapter introduced and gave the background to the study. This chapter analytically appraises literature published by researchers and scholars regarding cybercrime in the financial environment. The purpose of this section of the study is to assist the reader in understanding how cybercrime has evolved and the impact it has made in society.

2.2 Cybercrime

The cybercrime phenomenon has become a global topic of high interest that has become borderless (Urbas, 2012:7) and has developed into a business that attackers utilise internationally (Arief *et al.,* 2015). It is currently the biggest threat in the banking industry, and it has led to massive losses in monetary value. Cybercrime comprises not only malicious acts but also includes the misuse of the functionality that information technology systems initially designed (Shalaginov, Johnsen & Franke, 2017). Cybercrime focuses on targeting people, organisations and countries. The high-level of sophistication of cybercriminals is one of the main reasons for the high volume of cybercrime incidents globally (Standard Bank, 2017; Kundu *et al.,* 2018).

The definition of cybercrime is still not clear and there has been an endless debate on what constitutes cybercrime. Cybercrime is explained by totally different people, for instance, national security authorities, policemen, criminologists, technical consultants and unprofessional persons (Brown, 2015). Furthermore, the complexity of cybercrime affects many other fields which are computer science, psychology, sociology, economics, political science, geography, law and criminology (Payne, 2020).

The term cybercrime was adopted at the Convention of Cybercrime of the Council of Europe, ETS No. 185 (Mercer, 2016). Several nomenclatures have been used such as computer crime, computer-related crime, digital crime and information technology crime to accommodate the various forms of cybercrimes and motives (Maat, 2004:239). Paoli, Visschers & Verstraete (2018) list five types of cybercrime affecting

businesses which are cyber espionage, data or system interference, illegal access to IT systems and Internet fraud. It is also defined as crime committed through the use of PCs and other IT devices (Gordon & Ford, 2006:14).

Britz (2009:15) argues that cybercrime comes in the form of abusing and misusing computer systems connected to the Internet, which results in direct or indirect losses. Kranenbarg, Holt and van Gelder (2019:41) state that cybercrimes have a tendency to be committed in a different context compared to traditional crimes, leading to various risk factors for the offenders and victims. Naturally cybercrime is the extension of the conventional criminal activity, and these differences depend on the target. The factors that define the differences are:

i. Remoteness of the cyber-attacker: A typical criminal is aware of the victim and the damage experienced while a cyberattack normally occurs over great distances.
ii. Cyber-attacks power influence: A cybercriminal has access to a wide variety of online tools that they use together with other criminals to launch simultaneous attacks with the advantage of the anonymity of the Internet.
iii. Cybercriminal law ambiguity: The infancy of implementation and adoption of cyber law as well as the low levels of enforcement are a major difference when compared to the typical crime approaches (Mandelcorn, 2013).

Cybercrime, also called digital crime were different and varied since 1960 to the present day. In the early era of information systems, computer crimes were committed by some employees, and also physical attacks on computer systems were common in the time between 1960 and 1980. In 1980 malicious software began to appear in personal computers. In the beginning of the 1990s, the internet became a significant factor in increasing digital crimes; criminals had access to poorly protected systems using unauthorised ways normally for financial gain and credit-fraud. By the end of the 20th century, credit card fraud was involved in a broader category called identity theft, whereby criminals were stealing identities of other people to conduct illegal activities. Choo (2011:720) posits that cybercrime exists in conjunction with other types of crime and its impact falls under two categories which are:

- Short term impacts: These types of impacts consist of daily activities of individual users which include ATM usage and viewing of recent financial information.
- Long term impact: These include day-to-day activities of businesses and government.

The various intricacies regarding cybercrime are supplemented by the skill of the individual to disguise their online identity (Turkle, 2011). The transnational nature of cybercrimes enables the perpetrator to be pinpointed in one country whilst the victimised individual, data or computer system is located in another geographic location (Orji, 2015). These crimes are committed with ease and the perpetrators escape punishment, since they are not physically present when committing the crime (Aransiola & Asindemade (2011). This is an important and distinctive feature of cybercrime that entails the diversity and wide dynamics of potential development of crime (Gillespie, 2015).

In Africa over 90% of businesses are operating without cybersecurity protocols in place, which increases the vulnerability to cyberthreats like hacking, phishing and malware attacks (Jackson, 2023). The low levels of cyber maturity, limited offensice and defensice cyber capabilities are contributing factors to the rise in cybercrime (Allen & van der Waag-Cowling, 2021).

The banking sector during the mid-1990s was simple and reliable, however with the arrival of technology, there was a paradigm shift (Jaleshgari,1999:136). Banks experienced competition from other industry players and in order to maintain and enhance their customer base, they had to introduce several platforms whereby transactions could be performed much easier (Vrancianu & Popa, 2010:390). These platforms enabled customers to access their finances during daylight and at night, throughout the year irrespective of location. This poses a risk to the stability of the whole banking and financial sector due to the increasing cyberattacks in scope, numbers and sophistication making it difficult to predict the overall impact (Boer & Vazquez, 2017:1).

Kirwan (2017:38) states that the perception of cybercrime plays an important role in the likelihood of individuals participating in illegal activities online. Cyberattacks can be conducted in many forms and methods and the level of complexity ranges from

simple to a very high level of sophistication, which normally requires programming skills. Council of Europe (2018) further contends that many organisations and individuals are unaware of possible targets from hackers, cyber thieves and extortionists until it is late to respond or recover from the intended incident. Therefore, cybercrime is defined as an intentional attack on organisations, people and entities in order to obtain or extract valuable data and information.

2.2.1 Types of cybercrime

Thangiah, Basri & Sulaiman (2012) classify cybercrime into content based and technology-based crime. Content based crime is hosted by organizations that focus on threatening, defaming, and demoralising countries' images. Technology based crime focuses on hacking, acts of espionage and injecting malicious codes.

Muncie, Talbot and Walters (2010) further categorise cybercrime into three sections:

(a) Traditional cybercrimes: These are common crimes and include stalking, bullying, pornography and hateful material dissemination.

(b) Hybrid cybercrimes: These are similar to traditional cybercrimes, and they require the existence of the Internet to conduct cybercrimes such as identity fraud, phishing and unauthorised distribution of patent material.

(c) True cybercrime: These types of crimes are fully immersed in cyberspace and include hacking and financial fraud.

These forms of cybercrimes have also been seen in the banking sector and are listed as follows.:

2.2.1.1 Identity theft

Identity theft happens when one individual uses another's identity features and traits without their permission (Dzomira, 2014; Minniti, 2016). Sarannia and Padma (2014) defined may you kindly fix this spaceidentity theft as the stealing of sensitive information for illegal use without the owner's acknowledgement. Vasylenko (2012) emphasises that identify theft is the most prominent form of cybercrime since it involves criminals using the Internet to steal information. Identity theft is a growing problem because of the increasing migration and adoption of online activities.

2.2.1.2 Denial of service (DoS) attack or distributed denial of service attacks

A denial-of-service (DOS) attack operates by flooding a computer or organisation website with data which causes an overload of the bandwidth of a network or computer system and forces it to enter a hung stage that makes the IT environment to fail to function (Dicks, 2012). This attack floods a computer server with thousands or even millions of page requests that originate from a group of configured computers under the control of the attacker (Cevidalli and Austen, 2016). Another type of DOS assault is a distributed denial-of-service (DDoS) attack, in which the attacker has access to several channels in a network and each victim acts as an agent to attack another computer system, often referred to a zombie (Douligeris & Serpanos, 2007).

2.2.1.3 Malware

Rama (2016) defines malware as a combination of the words 'malicious' and 'software' and it is a malicious virus that can be built to gather the victim's data and information via the unhindered entrance of social media (Wani, 2017). According to Sloan and Warner (2014), malware is often downloaded to a user's computer and activated when an unsuspecting victim inadvertently executes an infected electronic mail attachment or clicks on a suspicious web link imbedded in an electronic mail. Furthermore, malware can also be used to steal sensitive or classified information, usernames, passwords, or other information, that is then forwarded to a cyber syndicate to commit cybercrime.

2.2.1.4 Pharming

This kind of fraud involves redirecting the victim's internet connection to a bogus website operated by the cybercriminal (Vrincianu & Popa, 2010). It involves a two-step process that begins with an attacker installing malicious code into the computer, whereby that code directs the victim to a spoofed website (Fortinet, 2022).

2.2.1.5 Phishing

Liao *et al.,* (2017) define phishing as "the act of sending fake messages to the victim often in the disguise of bank notifications or emails promising monetary gains and romantic relationships, luring the victim into handing over sensitive information such as account number and password, or install malware on the victim's system". Banking websites are most prone to this type of attack since customers have to enter their

credentials to access banking services. Chawki (2006) further describes other techniques of phishing;

- Dragnet method: This involves the use of spammed emails, bearing falsified corporate identification such as logos, corporate names, and addressed to large group of people in concentrated areas such as a bank, with the intention to trigger immediate response.
- Lobsterpot Method: This technique involves creation of similar websites to the legitimate corporate one.
- Rod and Reel method: This technique targets prospective victims with whom there was initial contact or prior engagement, with the intention to prompt their disclosure of personal and financial data.
- Gillnet phishing: With this technique the cybercriminal introduces a malicious code into emails and websites. When the victim opens the email or browses through the website, the malicious code changes the user settings, installs codes that record user's keystrokes which is then transmitted to the cyber criminals for illegal access to the victim's bank accounts.

2.2.1.6 Ransomware

Ransomware is a type of malware used by cybercriminals to freeze computer devices with the intention to steal data and demand a ransom normally in monetary terms (Aba, 2022). Ransomware is installed on a computer connected network and then encrypts sensitive or critical information by means of public-key encryption, which is different from most cyber hacking tools, like malicious software and this encryption key remains on the hacker's computer (Symantec, 2016). The victims of ransomware are then blackmailed to pay large sums of money, in some cases through cryptocurrency in order to receive a private key to decrypt their software. Ransomware is becoming increasingly popular amongst cybercriminals and according to Symantec (2016), it has been observed that an increase of 500% month-on-month in Ransomware incidents have been reported. Research from Kaspersky shows that in the year 2020, there were more than 1.5 million ransomware detections in Africa (Interpol, 2021).

2.2.1.7 Hacking

Liao *et al.,* (2017) define hacking as the illegal act of breaking into a computer system by deliberately passing through security measures with the intention of stealing information normally stored in computers and network systems. Bawane and Stelke (2014) mention denial of services, spoofing, sniffing, viruses, key loggers as some of the hacking techniques used by cybercriminals. When hackers successfully invade a computer system, the victim company or individual suffers a great loss that includes confidential information and credentials. Hackers apply tactics to get in touch with the target through email, telephone means or social media platform in order to build trust and further manipulate the victim's behaviour (Gaumer, Mortier & Moutaib, 2016). In Southern Africa, hacking recorded a rise during the 1990s due to the popularity and adoption of the Internet (Dlamini & Mbambo, 2019).

2.2.1.8 Insider Threat

Insider threat is defined as the threat caused by a person, mostly employees, contractors or business partners who have authorised access privileges and knowledge of the computer information systems of an organisation and inspired to influence the organisation processes (Brackney & Anderson, 2004).

The attacking of Personally Identifiable Information (PII) of clients is the prominent target in banking systems (Cummings, Lewellen, McIntire *et al.,*2012). Financial institutions are most vulnerable to insider threats due to the extremely sensitive information maintained and the strong reliance on information technologies (Yaseen, 2016). This threat is even greater in the form of intentional leaks of sensitive and strategic information shared with competitors or even worse with a cybercrime organisation (Gaumer, Mortier and Moutaib, 2016).

2.2.1.9 Card fraud

Sharma and Nanda (2006) define card fraud as a type of crime involving the illegal use of unauthorised account or personal information so as to misrepresent the account information. Sonepat and Sonepat (2014) agree with Sharon & Nanda by defining credit card fraud as the use of an unauthorised personal account for operations not intended. KPMG (2012) went further to reveal that credit card fraud can only be administered after stealing the cards and the relevant information needed for the transaction to take place. There are two kinds of card fraud which are online and offline

card fraud (Sonepat & Sonepat 2014). Offline card fraud, also known as card-no-present (CNP) involves stealing information through the internet and phone.

2.2.1.10 Cyber terrorism

Cyber terrorism is an unlawful action that involves violence against people and properties, and it often has links to political, racial and ideological reasons. This type of cybercrime normally spreads fear, anxiety and violence amongst people and affects the integrity and accessibility of information (Al-Khater, Al-Maadeed, Ahmed, Sadig & Khan, 2020). In Africa, the main cyberthreats are online scams, digital extortion, business email compromise, ransomware and botnets (Interpol, 2021).

2.2.1.11 Man in the middle attacks

Man in the middle attacks attempt to intercept communication between two people's data and modifying them to be delivered to the intended person. O'Hanley (2013) mentions eavesdropping and manipulation attacks as the two types of man in the middle attacks.

2.3 Generation of cybercrime

To address the argument of cybercrime, Wall (2007) recognised three kinds of generations of cybercrime, each kind of generation is unique, and the intangible differences between them can express the current differences in the possibility of the criminal occasion.

2.3.1 First generation of cybercrime

The first generation of cybercrime encompasses traditional crime, whereby computers are purely a tool, and this is referred to as low-end cybercrime. This type of cybercrime generation can be observed as a combination of computer technology, even networked technologies. Conversely, this technology plays a great role in assisting traditional criminal acts and this process is continued by different means if the machinery were unconcerned.

2.3.2 Second generation of cybercrime

The second generation of cybercrime is the crime which is committed over the network, and it is referred to as hybrid cybercrime because the internet has given new

possibilities for traditional methods of criminal happenings to include global networks. This global nature needs transjuridictional processes that look complicated to achieve.

2.3.3 Third generation of cybercrime

The third generation of cybercrime is known as true cybercrimes because it is exclusively produced by technology. This generation of cybercrime cannot occur when the internet is down, for example ransomware and phishing (Wall, 2015). Since they are the result of the internet, this cybercrime expresses each of its transformative features. Especially, through the gap that exists between physical and online criminal activities. A cybercriminal is the main actor in conducting criminal activities due to the freedom of using the Internet anonymously resulting in unlimited cyber threat attacks to users. As a result, online activities become vulnerable to cybercriminals immediately and unexpectedly outside the normal obstacle of physical gab (Yar, 2013).

2.4 The role of the Internet and cybercrime activities

Over time, the Internet changed the way human beings interact and view life, and the impact it has on our daily lives is impacted by the cyberspace we live in. Although cybercrime and traditional crimes are similar, the availability of the Internet has led to an increase in the number of cybercriminals. The Internet was never designed with security in mind and that opens up opportunities for hackers and cybercriminals to take advantage (Van Ommeren, Borrett & Kuivenhoven, 2014:36). A contributing factor is that cybercriminals have become more adept and specialised in executing crimes in cyberspace (Kirgel, 2012:470).

The Internet's function has made it possible for cybercrime activities to change across generations. The first generation of cybercrime occurred within discrete computing systems and was characterised by exploitation activities. It paved the way for departure from conventional criminal activity. The second generation of cybercrime occurred across networks, and involved acts such as hacking and cracking. The third generation is characterised by its dispensed and automated nature of computer systems interaction (Wall, 2007:44-47).

The increasing cyberattacks in Africa can be attributed to the vulnerability of organisational systems and negligence towards implementation and usage of cybersecurity practices (Kshetri, 2019). Africa is particularly vulnerable to cybercrime

threats largely due to the vast increased bandwidth that has been designed to bridge the digital gap for economic and social developments (Chetty, 2007).

2.5 Cybercriminals

Georgia State University (2022) defines cybercriminals as individuals and organisations who use computers to attack other people's systems, networks, IoT devices and data. Cybercriminals are increasingly agile, focused and organised in exploiting new technologies, altering and modifying their attacks and cooperating in ways to execute the attacks (Interpol, 2022). The attention of cybercriminals has shifted from targeting individuals to focusing more on organisations such as financial institutions due to the higher value of data targeted (Gaumer, Mortier & Moutaib ,2016). Arbak (2005) clarifies that cybercriminals are often concerned about their social status in the physical world and pay less attention about the cyberspace status because there is the policing factor involved. Rogers (2010) mentions personality traits and socio-demographics as characteristics that contribute to a cybercriminal committing a crime. Furthermore, Kranenbarg, (2021) considers characteristics of self-control, self-motivation, proficiency in IT, and routine activities as factors that contribute to engagement in crime.

Cybercriminals are motivated by many aspects to commit crime which includes peer recognition, the experience of power, curiosity urge, addiction feeling, boredom tendencies and political acts (Long, 2012). In addition, cybercriminals constantly upgrade their technical skills to further invent new ways of committing crime (Trozze *et al.,* 2022). Cybercriminals are normally located internationally, which makes it difficult to locate and extradite them. Furthermore, to construct one profile for a cybercriminal is often difficult since it involves the physiology, psychology and motivation of each cybercrime committed (Adams & Makramalla, 2015).

The use of the same old tricks when it comes to stealing bank customers' credentials and bank accounts is often used by cybercriminals (Thomson Reuters, 2014). In recent times, cybercriminals are imitating business models from legitimate corporations to structure their operations (Tropina, 2012). Cybercriminals tend to calculate the risk factor against the benefits that will accrue if they commit fraudulent activities (Plessis, 2021).

Moon (2019) states that the increase of cyberattacks in financial institutions is linked to nation states, resulting not only in theft but in destructive and disruptive damages. This type of cyberattack is referred called state sponsored cyberattacks. Mondragon (2021) defines state sponsored cyberattacks as hackers employed by countries through their militaries and government agencies to attack another country, organisation or industry. Allen & van der Waag-Cowling (2021) mention that African governments and regional organisations have been targeted by high profile state sponsored attacks including Chinese espionage at the African Union and North Korea's 2017 Wannarcy Ransonmware attack. To reduce the impact of state sponsored cyberattacks, there should be cooperation between a country's national security agency, the financial institutions and diplomatic communities (Maurer & Nelson, 2021).

2.6 Categories of cybercriminals

Cyber criminals are categorised into nine models:

- Script Kiddies (SK) or Novice (NV) – these have limited programming and computer skills, and they conduct attacks using toolkits.
- Cyber-Punks (CP) – they possess advanced technical skills including coding and programming skills to develop software.
- Hactivist (H) or Political Activists (PA) – these are individuals or groups that justify their behaviour on moral grounds, and it is often aligned to political issues.
- Petty Thieves (PT) – these are opportunistic people that take advantage of an organisation's poor internal security setup.
- Internals (IN) – consists of disgruntled ex-employees or current employees within an organization.
- Old Guard Hackers (OG) – have no interest and intention to commit a crime, however they do possess the skills.
- Professional Group (P) or Professional Criminals (PC) – they are specific and thorough in their activities, through access of state-of-the-art equipment. In

most cases these cyber attackers carry out these instructions on behalf of competitors to penetrate systems for financial gain (Dogaru, 2012).

- Cyber-Terrorist (CT) or Information Warriors (IW) – these are funded to participate in cyber-attacks that may be politically motivated (Rogers, Siegfried & Tidke, 2006).
- Virus Writers (VW) – these are coders that write script and also utilise automated tools.

The most dangerous group of cybercriminals are the professional criminals and cyberterrorists as they are well trained, financially motivated and knowledgeable with their attack approaches. Cybercriminals are generally motivated by four aspects, (1) revenge, (2) financial, (3) notoriety and (4) curiosity. Old Guard hackers (OG), Political Activists (PA), Professional Criminals (PC) and Information Warriors (IW) have the highest skill levels, Virus Writers (VW) and Internals (IN) are enthused by revenge, Cyber Punks (CP) and Political Activists (PA) are motivated by notoriety, Information Warriors (IW), Petty Thieves (PT) and Professional Criminals (PC) are motivated by financial motives and Novice (NV) and Old Guard Hackers (OG) are motivated by curiosity (Rogers, 2010). Figure 2.1 summarises the skill level and motivation factor of cybercriminals.

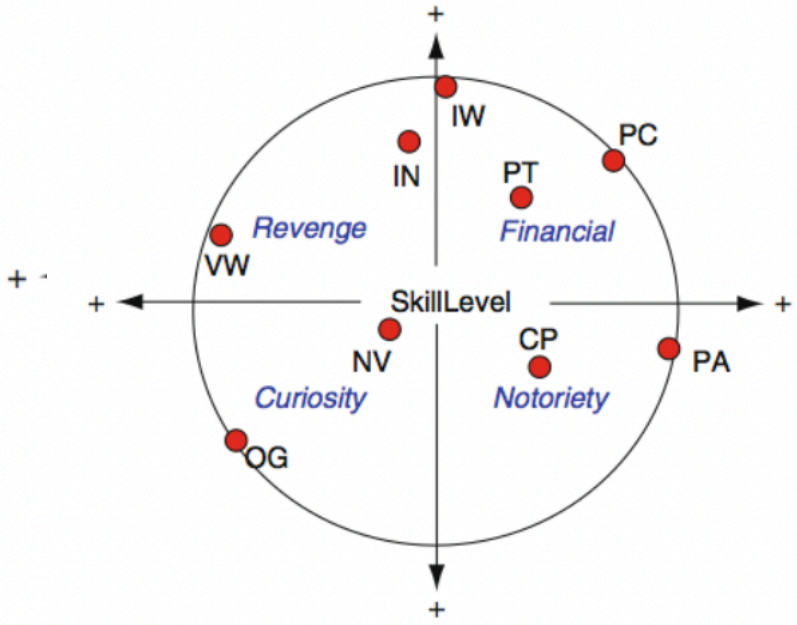


Figure 2.1: A circumplex model describing nine models of cybercrime, the skill level and motive (Rogers, 2010)

This model is crucial for comprehending the types of cyber incidents affecting an organisation. Furthermore, profiling a cybercriminal using this model assists law enforcement to categorise the types of cybercriminals that commit specific types of cybercrimes (Shinder, 2010).

2.7 Cybercrime in a developing and developed countries

Cybercrime affects developed and developing countries in different ways and it has become a global issue. This has prompted many countries, especially developing countries, to deliberately develop plans, goals and initiatives to counteract such cybercrimes. A developing country is a country with a relatively low standard of living and restricted barriers to sustainable development (United Nations, 2022). These countries often lag behind in terms of technology implementation and overall government and stakeholder support. Generally, they also lack the resources to establish institutions to address cybercrime (Kshetri, 2010) and the citizens experience challenges that impact on the basic cyber awareness issues (Veiga, Loock & Renaud, 2021). Cybercrime is more inclined to affect developing countries than developed countries due to the ability of the developed country to mitigate the cybercrime effects (Wint, 2003). Structural factors strongly influence a developing country's cybercrime position, particularly in the preliminary stages of digitisation processes (Kshetri, 2010; Swiatkowska, 2020).

There are several reasons why developing countries are vulnerable to cybercrime:

- *Bandwidth-intensive applications*

  In developing countries, the Internet connectivity is not smooth most of the time and therefore cyber criminals use this opportunity as a gap to launch their attacks. This low level of consistency thus makes it easier for cybercriminals to launch attacks at an aggressive pace (Goel, 2020).

- *Growing demand for Personal Computers*

  The demand for personal computers is high due to the rapid industrialisation and globalisation of access and computer usage (Shenoy, 2019).

- *Technology problems*

Technology related problems is another reason for the rise in cybercrime which is flourishing due to the limited governance interventions such as enforcing the necessary security standards, poorly secured, outdated, unlicensed and poorly managed information assets (Swatkowska, 2020).

- *Hardware and software procurement*

  ICT products sourced for developing countries undergo changes to meet the conditions of the respective local market. Most of these products targeted for developing countries are low-cost versions, since sophisticated versions of the same product are unaffordable for most citizens (Goel, 2020).

- Anonymity factor

  Potential offenders no longer need to possess specialised skills or knowledge to commit crimes, as they can easily acquire or buy tools and material online (Swiatkowska, 2020).

- Cybercrime complexity

  Law enforcement agencies lacking the understanding of newer and evolving types of cybercrimes lead to an unceasing rise in illegal criminal acts (McQuade, 2009).

Developed countries have adopted methods in the direction of maintaining diverse cybersecurity strategies, while developing countries are still at the infancy stage of digital transformation (Cacaho, 2021). Mongolia, Cambodia, Bolivia, Algeria, Zimbabwe and Honduras are some of the countries that offer the least of protection against cybercrime. These countries have very weak cybercrime legislation; hence they carry a huge risk for all users when engaging in transactional activities of personal information (Varga, 2022). Developing countries can improve their status by entering the information society without exposing themselves to excessive risk, through gaining experience from developed countries (ITU, 2007).

2.8 Current Global Cyberattacks in the Banking sector

Financial institutions fall victim to cyberattacks more than most industries. This is a result of the connectivity to the Internet and the existence in cyberspace. These attacks are constantly growing in both frequency and sophistication, and some of the cybersecurity threats are:

Lack of regulatory enforcement

Industry regulations are applicable to all organisations and the financial sector is no exception. The regulatory aspect alone might not be enough to cover all the elements required to ensure that an organization is protected from all cybersecurity risks (Duncan & Whittington, 2014). These regulations outline various requirements that financial institutions must enforce in order to prevent and protect confidential data (Filipkowski, 2021). The lack of regulatory enforcement in cyberspace provides cybercriminals with an endless supply of targets to carry out their crimes (Peters & Jordan, 2020).

Ransomware

Financial institutions are attractive targets for ransomware criminals because of their valuable customer information. During a ransomware attack, the malware deployed by the cybercriminals encrypts the bank's computers and the action is reversed once payment is made (Kost, 2022).

Insider Threats

The 2020 Verizon Data Breach Investigation Report found that 30% of all breaches were a result of the activities of an insider threat. These breaches tend to lead to incidents such as fraud, financial losses and data leaks. Insider threats are a major issue in financial institutions because not only do they target data and financial credentials, but they also affect the goodwill of the institution (Chavali, 2020).

Supply chain attacks

A supply chain attack arises when an individual infiltrates an organization system through an external partner or partner provider to gain access to the organization system and data (Korolov, 2021).

Credential stuffing

This is an attack in which user credentials obtained from a data breach from one service are used to attempt to log in to another unrelated service (Cloudfare, 2024).

IoT exploitation

IoT exploitation is a cyber-attack that gains access to users' sensitive data with the help of another IoT device (Educative, 2024).

Ransomware

This is a form of malware that blackmails its victims through malicious e-mail attachments, infected software apps, infected external storage devices or compromised websites (Hull, John & Arief, 2019).

Advanced Persistent Threats (APT)

An advanced persistent threat is a sophisticated sustained cyberattack in which an intruder established an undetected presence in a network in order to steal sensitive data over a planned and prolonged period of time (Lenaerts-Bergmans, 2023)

2.9 Cybersecurity Frameworks

Cybersecurity frameworks provide a common language and a set of standards for the understanding of various security postures, in order to define processes and procedures that an organisation should follow to address cybersecurity risk (Cisternelli, 2020). In tackling cybercrime, one of the challenges faced worldwide exists in the failure to fully understand the relationship between cybercrime stakeholder relationship and the sociology impact of criminology towards cybercrime (Singh, Frank & Wan Zainon, 2021). Grobler, Van Vuuren & Zuurman (2013) mention lack of collaboration between industries, state departments, regions and the legal fraternity as some of the challenges that countries face in combating cybercrime. Reducing an organisation's exposure to cyberattacks and identifying areas most vulnerable to data breaches and activities compromised by cybercriminals are the two main objectives of a cybersecurity framework (Reciprocity, 2021). The most common cybersecurity frameworks are:

2.9.1 NIST Cybersecurity Framework

This framework was created to assist organisations of all sizes and types to manage and coordinate cybersecurity and business (National Institute of Standards and Technology, 2018). It is relevant to the financial sector due to the complex, regulatory environment as well as local, regional and international compliance requirements. In

the context of cybercrime, the NIST Cybersecurity framework allows for an easier approach to assess the progress with stakeholders. Furthermore, it complements existing cybercrime initiatives in order to minimize disruptions and allowing organisations to strengthen their cybersecurity measures (Szentgyorgyi-Siklosi, 2023).

2.9.2 ISO/IEC 27001:2013 Standards on Information Security Management Systems

This is an expert committee founded to develop international management systems standards for information security to protect organisations' information assets (Iec, 2013). This standard consists of risk management, security management, governance and compliance which assists organisations in placing essential people, procedures, and technologies to achieve a proactive approach to security and risk management (ISO, 2013). According to Amarachi and Ajaegbu (2013), ISO 27001 is a standard used to examine information security frameworks and ensure that suggested solutions are practical and applicable.

This standard addresses the unique security challenges within the banking sector through its risk-based approach, and the key component is the emphasis on continuous improvement and regular audits, ensuring that banks remain vigilant in the cybersecurity enforcement area (ISMS, 2024). Ewuga, Egieya, Omotosho & Adegbite (2023) state that the ISO 27001 assists banks to achieve compliance with other standards or frameworks, such as NIST, in order to build trust and reputation with customers and stakeholders.

2.9.3 Center for Internet Security (CIS)

This is an in-depth defence security best practices created by IT experts from an extensive range of sectors to mitigate cyberattacks against systems and networks (Center for Internet Security, 2018). The CIS develops recommendations for cybersecurity practices and procedures which are validated through a consensus-driven decision-making process (Choi, 2020). These practices form a framework of critical security controls that are effective in protecting financial institutions against common attacks. The cyberattacks in banks are minimized through controls that are put in place to manage identified risks, such as physical barriers (*e.g.* locks, electronic

barriers (*e.g.* firewalls, antivirus), policies, procedures and user training initiatives (Liebl, 2022).

2.9.4 PCI-DSS

PCI-DSS was developed by an information security council and is concerned with bank financial services like VISA International Inc. and MasterCard to ensure consistency of data security measures on a global level (Solomons, 2019). This standard was adopted to assist banks to process card systems, and at the same time prevent fraud by increasing the control of the data to prevent too much exposure (Solomons, 2019).

2.9.5 A framework for the Governance of Information Security in Banking system

The Information security governance (ISG) framework is an integration of several governance frameworks such as the Federal Financial Institutions Examination Council (FFIEC), Control Objectives for Information and Related Technology (COBIT), the International Organisation for Standardisation (ISO) 27002 and PCI-DSS, the Corporate Governance Task Force (CGTF), Information Systems Security Association (ISSA) and the Corporate Information Security Working Group (CISWG) Ula *et al.,* (2011).

These cybersecurity frameworks can act as a starting point for banks in governing the information against cyberthreats and risks, by implementing the available standards. Implementation of these frameworks varies from country to country. In the case of Eswatini, positive steps have been taken such as the approval of the national cybersecurity strategy as well as the launching of the Eswatini Cyber Security Incident Response Team (SzCIRT).

2.10 Cyberspace and Cybercrime

Cyberspace is perceived as a conceptual environment where communication occurs using computer networks (Pawar, Mente, Bapu & Chendage, 2021). Cyberspace is a communication medium that can provide global access to resources through a wide range of formats created to meet user requirements (Venables, 2021). As a virtual environment, cyberspace has become militarised by cybercriminals as a result of the ease of access and the availability of hacking tools (Venables, 2021). According to the

European Commission (2013), cyberspace is the global, virtual, and computer-based networked environment that is made up of the open-air gapped Internet and connects systems and other infrastructure that is required to meet societal needs.

Bajrami, Dika, Shabani & Selimi, (2020) mention easy access to information and data, and communication opportunities as advantages of cyberspace while a rise in cybercrime activities and reduction of personal and information privacy as its disadvantages. Cyberspace is already a tool for facilitating all types of criminal activities (Tropina, 2013) by providing anonymity in communication, advertisement possibilities and money laundering (Goodman, 2010). In cyberspace, it is very difficult to apprehend a criminal due to the ease of hiding their identity as compared to the physical world. The increase in cybercrime activities in cyberspace is a result of the loopholes, lack of awareness from cyber defenders and gaps that cybercriminals exploit. The main characteristic that is shared between cyberspace and cybercrime is the harsh and unethical practices that have evolved over the years (Uma & Padmavathi, 2013).

2.11 Cybercrime in the banking sector

Due to the reliance and adoption of digital systems and networks for their business operations, organisations' increased digitalisation leads to an increase in cybercrime (Staal, 2015:11). Financial wealth that is often concentrated in banks is one driver of cybercrime empowering a fertile ground for crime, and enormous potential focus for cybercriminals (Herlseman & Warren, 2004:260). Less developed countries are often exploited by cybercriminals due to their weak security controls, and these exploitations are then used to target more developed countries to gain access to their systems (Lakshmanan, 2019:1).

The banking sector’s involvement with the digital world has left it more vulnerable to cybercrime. To remain competitive in the age of digitisation, banks offer a wide range of services to their clientele. Financial institutions, which are currently active in many different jurisdictions, are vulnerable because of the ease with which they can target and profit from online banking, frequent international transactions, the existence of databases within banks, and innovative payment methods like PayPal (Oliveria & Stickings, 2016:17). It has become necessary to protect financial institutions from the antics of cybercriminals, due to the pivotal roles of banks in the growth and economic

development of any nation (Ikechi & Okay, 2013:254), since banks remain the favourite target of skilled cybercriminals (Lewis, 2018:9).

The consequences of cybercrimes in banks frequently result in the violation of intellectual property rights and the inability to fulfil financial and business agreements made in order to provide goods and services. Because cybercriminals want to harm these companies' reputations, banks are the ones that they target the most (Onchomba, 2018:3).

The banking sector is one of the most important foundations for a country and it is important that coordination between all stakeholders in the financial sector collaborate to mitigate the impact of cybercrime.

Figure 2.2 below outlines the various types of cyberattacks that occurred in banks worldwide. The type of tactic used, the estimated costs and the name of the bank are displayed, highlighting the devastating effects of cybercrime.

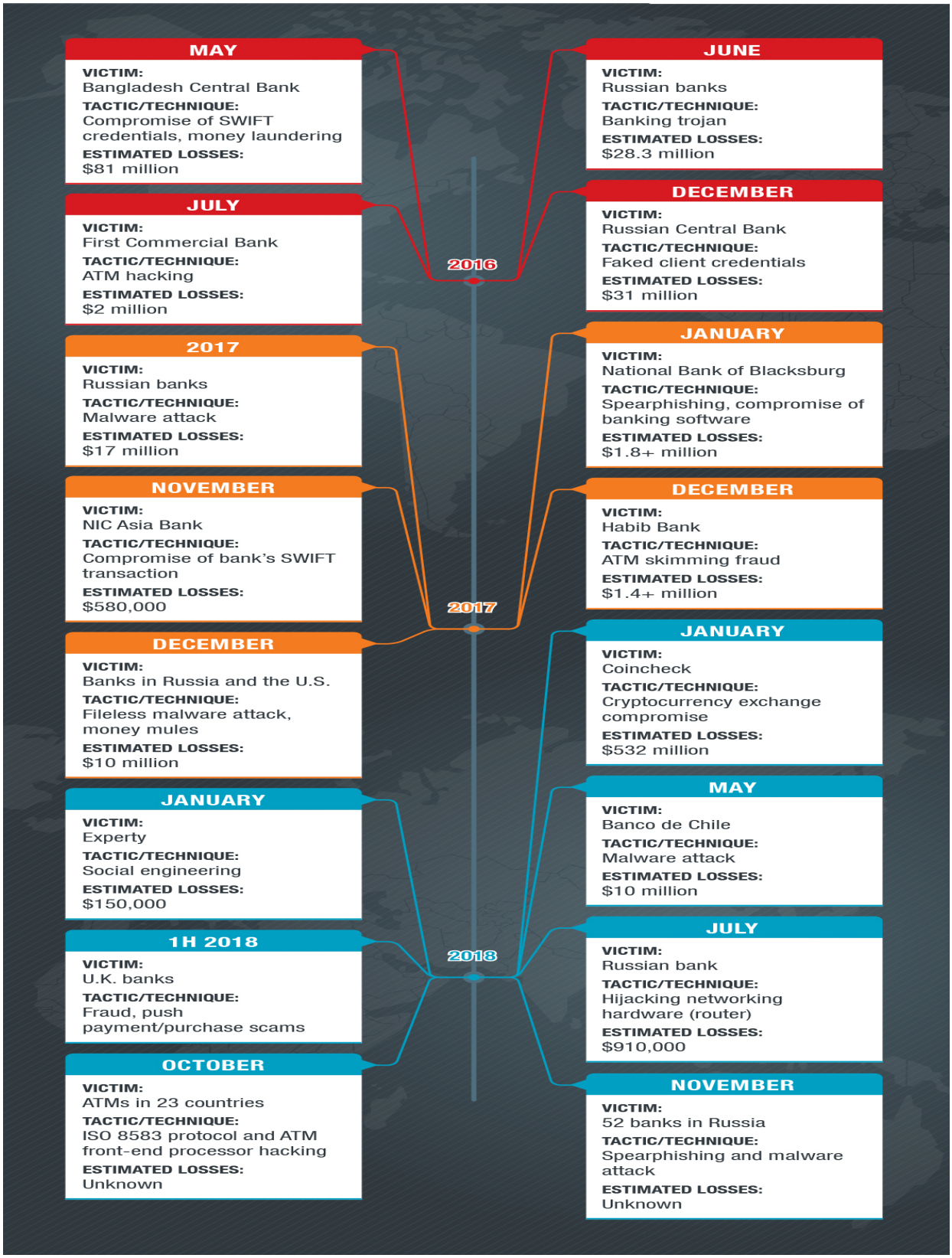


Figure 2.2: Cyberattacks in banks

2.12 Eswatini and the Global view on Cybercrime

The global nature of cybercrime has affected the way individuals and organisations detect, prosecute and execute cybercrime incidents. Tendulkar, (2013) affirms that the jurisdictional conflict and uncertainty about cybercrime often heightens the probability for regulatory arbitrage and confusion regarding the necessary legal channels to be used. An attempt to resolve this matter was through the establishment of a committee that will develop cyber legislation for commonwealth states. This committee, called The Cybercrime Legislation of Commonwealth States, used Budapest Convention and Commonwealth model law that consisted of three areas of cooperation:

Cooperation area 1: The participants are expected to work together to provide extensive cooperation to each other and to reduce obstructions so that a smooth and rapid flow of information is achieved.

Cooperation area 2: There should be an extension of assistance to all criminal offences related to computer systems as well as the collected electronic evidence.

Cooperation area 3: This should be conducted both “in accordance with the provisions of this chapter” and “through application of relevant international agreements on cooperation in criminal matters and agreed on the basis of uniform or reciprocal legislation.

Africa Cyber Security Report (2016) states that most African organisations are not fully equipped to respond to information security threats. In the year 2022, most African countries experience a significantly large number of cyberattacks (Carter, 2023).The banking world has advanced with online banking through technology, becoming a more convenient way of conducting banking activities. Banks in Eswatini rely on technology provided by various third-party systems to conduct local and global transactions.

The Eswatini banking sector is a highly regulated environment, and it complies with numerous pieces of legislation and regulations. To address such crimes, the Kingdom of Eswatini has instituted some legislative measures which include the Financial Institutions Act No.6 of 2005, The Money Laundering and Financing of Terrorism (Prevention) Act of 2011, Prevention of Organized Crime Bill and Draft Computer

Crime and Cybercrime Bill, 2013 and the Electronic Communications and Transactions Bill of 2017 (Government of Eswatini, 2019:1).

Moreover, there are various factors identified that are a contributing factor to the spreading of cybercrime which mostly concern more developed countries. Africa has limited research carried out on cybercrime and Quarshie and Odoom (2012:98) further state that a lot of cybercrime emanates from the African continent accompanied by threats that are easily spread due to poorly protected computer systems, hence there is a need to address this problem. This is further hindered by the lack of cybercrime knowledge (Akuta, Ong'oa & Jones, 2011:219). The literature identified a trend whereby most of the studies especially in the African context, applied only a few criminology theories in their research in order to obtain an in depth understanding of cybercrime activities in varied sectors.

2.13 Cybercrime costs

Cybercrime costs are one of the biggest issues faced by financial organisations worldwide. Ponemon Institute (2016) categorises cybercrime costs into three groups:

(1) Direct costs which are the main expenses spent to accomplish the task.
(2) Indirect costs which consist of time, effort and organisation resources.
(3) Opportunity costs which consist of negative reputation and missed opportunities.

In Eswatini, cybercrime costs consist of online trading, change of beneficiary details, cryptocurrency, forex trading, Ponzi and pyramid schemes (Howe and Pelser, 2022).

2.14 Internet usage in Eswatini

According to the Internet World Statistics report (2022), Eswatini had a total estimated number of 665, 245 Internet users by 2022, whereas the Internet growth from 2000 to 2021 was 6,552 users, a 23% growth from 12 236 to 15 015, exceeding fixed wired connections which declined by 2.5 % from the previous year (ESCOOM, 2022).

2.15 Cybersecurity policy and strategy in Eswatini

In November 2022, the Ministry of ICT launched the Eswatini National Cybersecurity Strategy 2022 – 2025. This strategy outlines important elements necessary for ensuring a good cybersecurity posture of Eswatini and includes the current context of

cybersecurity in terms of current and emerging cyberthreats relevant to Eswatini. In addition, the Eswatini Communications Commission (ESCOOM) in collaboration with local industry stakeholders developed a website for the National Computer Incident Response Team (nCIRT) - https://ncsirt.org.sz/- that will allow the public to share important alerts and information on cybersecurity incidents in the country (ESCOOM, 2022).

The Central Bank of Eswatini in 2021 introduced the Cybersecurity Guidelines for Financial institutions to manage cyber risks affecting ICT systems in the banking sector (Central Bank of Eswatini, 2024). Additionally, the Eswatini Bankers Association (EBA) which is made up of the banks in Eswatini, is an organization that focuses on promoting strength, growth and sustainability in Eswatini's economy by encouraging efforts to minimize fraud (EBA, 2024).

2.16 Combating Cybercrime through existing frameworks

The financial sector in developing and developed countries has recognised the escalating risks of cybercrime and as a result, standards and guidelines to assist financial institutions have been developed (Baur-Yazbeck, Frickenstein & Medine, 2019). The complexity of cybercrime is a challenge for law enforcement agencies and countries when it involves controlling cybercrime. Countries have taken the route of collaborating with existing cybercrime fighting organisations. Okonigene (2010) emphasises that one of the contributing factors is that cybercrime is difficult to prove since it lacks the traditional and structured paper trail.

It is crucial for organisations to adopt known international cybersecurity standards to oversee or guide banks in combating cybercrime. It is a key element to improve cooperation between countries and law enforcement agencies in harmonising cybercrime laws (Chang, 2020). These include (i) The Convention on cybercrime, (ii) Global Commission on the stability of cyberspace, (iii) The Paris Call for Trust and Security in Cyberspace, (iv) The Charter of Trust, (v) Contract of the Web and (vi) Subcommittee on High -Tech crimes. Cassim (2011) emphasises the importance of following a suitable framework in order to manage cybercrime in banks.

2.16.1 Treaties

A treaty is a formally signed and ratified agreement between two or more countries (LII, 2021). Treaties bind those countries that have explicitly accepted them or have ratified an international agreement containing set rules (Nesovic & Jerotijevic, 2018).

2.16.1.1 The Convention on Cyber Crime (Budapest Convention)

This is the first international legislation against criminal behaviour in the cyberspace, since it adopts a simple definition of cybercrime, and addresses a majority of malicious activities on the Internet (Hui, Kim & Wang, 2017). The goal of this convention was to establish a global approach to cybercrime that would involve harmonizing national law, strengthen investigative abilities and enabling international cooperation (Ohanian, 2022).

2.16.2 Commission

A commission is a multiheaded body formed to perform a particular function, whether it is administrative, judicial or legislative (Britannica, 2023).

2.16.2.1 Global commission on the stability of cyberspace (GCSC)

A multi-stakeholder group committed to the formation of diplomatic norms focusing on governmental offensive action in cyberspace, which operated between 2017 to 2019 (Ciglic & Hering, 2021). The Global Commission on the Stability of Cyberspace (GCSC) engages the full range of stakeholders to develop proposals for norms and polices to enhance international security, stability and to guide responsible state and non-state behavior in cyberspace (EastWest Institute, 2020).

2.16.2.2 Subcommittee on High -Tech crimes

The Group of Eight (G8) established a Subcommittee on High-Tech Crimes in 1997, that dealt with the fight against cybercrime (Marco, 2012). This committee adopted ten principles and a ten-action plan to fight against cybercrime and obliterate ways of committing crime. There are many efforts employed by the banking sector to overcome cybercrime and the multi-stakeholder approach is one method that can be 50mphasiz (Boateng *et al.*, 2010). This approach involves governments, private sectors, legal institutions and cybercrime practitioners. Aligning international standards with existing comprehensive state cybercrime laws contributes positively to preventing cybercrime. Buono (2014) emphasizes the need for the establishment of dialogue sessions at both

vertical and horizontal levels, where prosecutors, judges, public awareness groups and industry stakeholders address cybercrime issues.

2.16.3 Declarations and commitments

2.16.3.1 The Paris Call for Trust and Security in Cyberspace

An international commitment to cybersecurity principles by the French government in 2018, focusing on preventing conflict in the digital domain (Rose, 2018). It is based on nine (9) principles that promote and ensure the security of cyberspace and the safer use of information and communications technologies (CyberPeace Institute, 2021)

2.16.3.2 The Charter of Trust

The Charter of Trust is an industry compact spearheaded by Siemens that addresses escalating risks associated with the ubiquitous connectivity in the digital space (Charter of Trust, 2021a).

2.16.3.3 Contract for the Web

This multi-stakeholder initiative launched in 2021 is meant to promote a better online world and is designed around distinct responsibilities across three stakeholder groups mainly governments, organisations and citizens (Ciglic & Hering, 2021).

Table 2.1 below shows examples of collaborative projects from around the world that address cybercrime.

Table 2.1: Global Projects addressing cybercrime

	Partnership name	Purpose	Country of origin
1.	The German Competence Centre against Cyber Crime e.V (G4C)	This was formed by three (3) commercial banks in 2013 with the purpose of collaborating on identifying and eliminating security risks at inception stage. It also cooperates with Germany's Federal Criminal Police Office and Federal Office for Information Security	Germany
2.	Suricate Solutions	This is a cybersecurity support centre for microfinance institutions that offers a range of	Senegal

		services and solutions such as technical advisory services, systems monitoring, incident response, technical audits and assessments.	
3.	South African Banking Risk Information Centre (SABRIC)	This is a non-profit company that was set up by four major South African banks to coordinate interbank activities aimed at addressing organised bank related financial crime, violent crime and cybercrime.	South Africa
4.	Thailand Banking Sector CERT (TB-CERT)	This was setup in 2017 by the Thai Bankers Association and the Thai Government. It focuses on sharing threat information and best practices among its members, provides training, capacity building and facilitates dialogue between the industry and regulator.	Thailand
5.	The United States Financial Services Information Sharing and Analysis Centre (FI-ISAC)	This was setup in 1999 by a consortium of US - based FSPs in response to a Presidential Decision Directive that mandated the public and private sectors to share information about physical and cyber security threats and vulnerabilities via information sharing and analysis centres (ISACs)	United States of America
6.	Swift Information Sharing and Analysis Centre	Originally established in 1973 by banks to address the transfer of financial information across the globe. Recently the Swift Information Sharing and Analysis centre was launched to facilitate access to cybercrime threat intelligence within the financial environment	Belgium

Financial institutions and private companies collaborate to share threat information that leads to combatting cybercrime. Eswatini Communications Commission (ESCCOM) launched the Computer Incident Response Team (SzCIRT) which acts as a focal point in coordinating cybersecurity incidents for Government Departments, Internet Service Providers and other relevant entities in Eswatini (ESCCOM, 2024).

Furthermore, since 2019, ESCCOM has been hosting National Cybersecurity awareness months to promote awareness on cybersecurity in all sectors of the country (ESCOOM, 2024)

2.17 Regional Initiatives to combat cybercrime in Africa

Cybersecurity has become a major concern across the world and is accelerated by the growing cyberattacks on vulnerable targets. The aspect of international collaboration has resulted in the call for drafting of standards, legislation, regulations and guidelines in a unified and harmonised manner, with the ultimate goal to fight cybercrime. In Africa, delegates from twenty-eight (28) countries committed to the Lome Declaration on Cybersecurity and the fight against cybercriminality. This commitment was established to push through the signature and ratification of the African Union (Malabo) Convention on Cyber Security and Personal Data Protection, with the objective of enabling a safe African cyberspace (Atabong, 2022). In order to keep pace with the evolving nature of cybercrime, African countries are highly recommended to continue to review existing cybercrime legislation and latest technological progress (Interpol, 2023).

2.17.1 African Union Convention on Cyber security and Personal Data Protection – Malabo Convention

The Malabo Convention was drafted in 2011 and only adopted in June 2014 and the purpose was to create a framework that will consolidate, promote and address cybersecurity, combating cybercrime, and protection of personal transactions and data. As of May 2022, only 13 countries (Angola, Cape Verde, Ghana, Guinea, Mauritius, Mozambique, Namibia, Niger, Republic of the Congo, Rwanda, Senegal, Togo and Zambia) out of 55 African Union member states signed up (Mitchell, 2022).

2.17.2 African Union Mechanism for Police Cooperation (AFRIPOL)

The AFRIPOL is an institution that exists under the African Union and its status was adopted by the African Union conference in January 2017. The mandate is to strengthen cooperation between the police agencies of AU member states in the prevention and fight against organised transnational crime, cybercrime and terrorism (Afripol, 2023). AFRIPOL's cybercrime strategy of 2020 – 2024 is based on three pillars; firstly, raising awareness in a country's population, secondly, reinforcement of policy, treaty and collective legislation towards the fight against cybercrime and thirdly, the establishment of technologies at country level to reinforce cyber defences (Mitchell, 2022).

2.17.3 Interpol's regional Cybercrime strategy for Africa

This is a regional cybersecurity strategy for Africa provided through INTERPOL (International Police) which underpins the operational framework of the African Cybercrime Operations Desk. The African Cybercrime Operations Desk under the AFJOC project will address cybercrime in support of the African region through the following strategic pillars;

Strategic objective 1: Enhancing cybercrime intelligence for effective responses to cybercrime

INTERPOL will collaborate with private organisations to share up-to-date information related to cybercrime threats, trends and risks in the African region.

*Strategic Objective 2: Strengthening cooperation for joint operatio*ns against cybercrime

INTERPOL will have close cooperation with member countries, private partners and national Computer Emergency Response Team (CERT) communities through the African Cybercrime Operations Desk.

Strategic Objective 3: Developing regional capacity and capabilities to combat cybercrime

INTERPOL will plan, develop and deliver cyber capability and capacity building projects and programmes to enhance member countries' ability to tackle cybercrime in Africa. As part of this effort, it will maximise the use of tools and platforms including the Cybercrime Knowledge Exchange, Cybercrime Collaborative Platform – Operations and Cyber Fusion Platform.

Strategic 4: Promoting good cyber hygiene for a safer cyberspace

INTERPOL will run a global awareness campaign with the aim of raising public awareness of the key cyberthreats and promoting good hygiene for individuals and businesses in Africa.

The campaign will also support regional law enforcement mitigation and prevention efforts targeting the top cyberthreats, for better operational outcomes (INTERPOL, 2021).

There are many views on the severity of cyberattacks in the financial sector. Many experts and influential figures in the cybersecurity space highlight the increasing scale of the risks modeled by cybercrime activities in the financial sector. The US House Intelligence Committee implied that a large scale and properly orchestrated attack on financial organisations could cause a ‘cyber-crisis’ that would have a devasting impact (Tendulkar, 2013).

CHAPTER THREE

THEORETICAL FRAMEWORKS

3.1 Introduction

This section discusses three theories that underpin the present study. A theoretical framework within a study is very important, since it assists and guides in understanding the research problem and related concepts underpinning the study. McQuade (2006) defines theory as “an interrelated and testable set of propositions that explains a phenomenon”. Theories can provide an in-depth understanding in developing appropriate crime prevention and enforcement strategies for protecting information systems and infrastructure (Bello, 2018). The theories underpinning the study are the Routine Activity Theory, Space Transition and Deterrence theory which are part of criminology.

3.2 Criminology

Criminology is defined as the scientific approach that focuses on the social phenomenon of crime to counteract and address it (Sutherland & Cressey ,1960). The emphasis is that crime is not an act that exists in a vacuum, but it contains elements that fulfill it (Anshori, 2021). There has been an increase in the number of criminological studies in cybercrime in the last twenty years, mainly due to the increase in cybercrime incidents (Wu, Peng & Lemke, 2023). Criminology in cyberspace is mostly understood as the social spaces that stimulate opportunities for criminal activities to arise (Yar, 2005).

3.3 Routine Activity Theory

The routine activity theory attempts to explain human behaviour when an interaction takes place between the subject and its world. This theory advocates that when suitable targets and motivated offenders convene in the absence of capable guardians, a crime activity will probably happen (Miller, 2013). The patterns of crime will be affected if changes in routine activities influence the convergence of space and

time of motivated offenders, suitable targets and the absence of capable guardians (Cohen & Felson, 1979:589). This theory proposes that three situations facilitating the occurrence of crime must happen at the same time and in the same space.

The assessment of the situation determines whether or not a crime takes place. Crime is a product of the intersection of time and space of the potential criminal, suitable targets and the absence of capable guardians (Kodellas, Fisher & Wilcox, 2015:322). The routine activity theory is relevant to this study in the sense that it provides significant understanding as to why people engage in cybercrime activities in cyberspace. Furthermore, Kigerl (2012) emphasises that the routine activity theory can be used in analysing emerging threats in cybercrime. In the context of the banking sector, the routine activity theory is an environmental theory, a time and place-based interpretation of crime, where the connection of individuals and behavioral patterns of a place and time influence where and when cybercrime activity occurs (Williams, 2015). In cyberspace, the routine activities are online based including shopping, communication, business transactions and websites visited (Smith & Stamatakis, 2020).

The suitability of the routine activity theory is supported by many researchers through the combination of length and the type of exposure to the Internet as a proxy for the routine activities criteria (Holt & Bossier, 2008).



Figure 3.1: Routine Activity Theory

3.3.1 Suitable targets

A suitable target refers to an individual's availability as a victim, including attributes of attractiveness to the offender (Cohen & Felson, 1979*).* Holtfreter *et al.,* (2010) argue that the theory assumes that a constant supply of motivated offenders focuses on the behaviours, activities and situational contexts that place potential targets at risk of victimisation. The Routine activity theory was introduced by Cohen and Felson (1979), before the existence of the Internet. The assumption is that most offences would occur between a motivated offender and suitable target physically, therefore the applicability of this theory in a virtual space is not applicable. However, Reyns (2013) argues that with the advancement of technologies and access to the Internet, the increase in Internet based routine activities has made it appropriate to adopt the theory to crimes that occur in cyberspace.

3.3.2 Capable Guardians (Guardianships)

A capable guardian can be any person who is present in a situation or place that a cybercriminal would have taken an advantage or opportunity to conduct the intended or planned criminal activity. Capable guardians include end-users, technical staff (network administrators) as well as automated protections such as firewalls, virtual private networks, anti-virus and anti-intrusion software, and ID authentication and access management systems (Leukfeldt & Yar, 2016). Parents are also capable guardians that monitor their children's Internet usage. In the context of the banking environment, a capable guardian is not only a general security guard or police officer but anyone whose presence acts as a protector of the space or area in cyberspace.

Law enforcement agencies, account holders, banks, Computer Emergency Response Teams (CERTS) or individuals possess a capability of discouraging the offenders, thus qualifying to be called capable guardians (Yar, 2005). Social- informal guardians, which includes firewalls, Intrusion Detection Systems, Virus Scanning Software, In-house IT Network administrators also form part of the capable guardians' definition (Denning, 2000).

Guardianship in cyberspace is categorized as technical guardianship, social guardianship, behavioral guardianship and personal guardianship (Ahmad & Thurasamy, 2022). The most important aspect of the capable guardian is availability and providing supervising actions that deter the criminal to commit or continue with the cybercrime act.

Table 3.1: Types of Guardianships

Guardianship type	Description
Technical Guardianship	Refers to the use of protective software which are Anti-virus software, filtering software and firewalls (Fleming, Greentree, Cocotti-Muller, Elias & Morrison, 2006)
Social Guardianship	Refers to the social circles or persons that can assist in discouraging cybercriminal acts (Reyns, Henson & Fisher, 2016)
Behavioural Guardianship	Refers to the use of protective means such as password changing and modification (Ahmad & Thurasamy, 2022).
Personal Guardianship	Refers to means that a person uses to protect oneself from cyber victimisation (Ahmad & Thurasamy, 2022).

3.3.3 Likely offenders

Likely offender refers to persons who are willing to commit a crime when an opportunity presents itself through the presence or absence of a capable guardian and target (Marcum, Higgins & Ricketts, 2010). An offender will take the opportunity and commit a crime if the presence of a guarding is either lacking or absent. Argun and Daglar (2016) insist that a crime will occur when a motivated offender or cybercriminal meets the opportunity.

Aligning these definitions to this theory, the suitable targets are the bank customers accessing bank services either physically or online, the capable guardians referring to security measures such as authentication methods and the likely offenders referring to threat actors taking advantage of any opportunity to exploit. The routine activity

theory looks at crime from the offender's point of view. In that way the crime will only be committed if the likely offender thinks that a target is suitable, and a capable guardian is absent. In the current situation where banking services are mostly available online and online presence is ubiquitous, this theory is therefore even more relevant. Furthermore, (Mustaine and Tewskbury,2000) emphasise that the routine activity theory can be successfully applied not only to criminal victimisation, but to offending criminal activities. The process of adopting the Routine Activity Theory to cybercrime requires that the cyberspace's place, distance and temporal order be identifiable and definable as existing in the physical world (Smith & Stamatakis, 2020).

The migration of crime from the physical space to cyberspace has created a variety of offender types, as shown in Table 3.2.

Table 3.2: Types of offenders

Type of offender	Description
Aggressive offender	Causes damage through remote access tools by obtaining unauthorised access
Acquisition offender	Crime is committed against property, cash and belongings
Professional offender	Crime is committed in a systematic and well-planned manner
Occasional offender	Crime is committed under the influence of temptations, that can include professional or external environment factors
Ideological offender	Crime is committed based on political, scientific, religious beliefs and ideas

3.4 Deterrence Theory

Taddeo (2018:341) defines deterrence as a coercive strategy that is based on conditional threats with the overall goal of persuading the opponent into behaving in a desirable way. Pratt, Cullen, Blevins, Daigle and Madensen (2006:367) further state that it is based on an underlying model that criminals act upon rational choices, and that particular interventions for consequences can turn criminals away from conducting such acts.

Deterrence is originally a cold war doctrine used in the military realm to prevent the proliferation of nuclear arms between countries (Baram, 2008). In cyberspace, the setup is different due to the number of actors and platforms available in conducting and engaging in cybercrime related activities. Deterrence is characterised by actions and events directed at preventing and stopping planned crime activity, through means to make it unattractive (Ibor, 2016). The deterrence theory is exemplified in the rational choice theory where the emphasis is on the individual, merely placing the individual as the main agent in decision making (Luce & Raiffa, 1957).

The deterrence theory specifies that stricter penalties and tougher fines deter individuals from committing crime in the first place or dampen their efforts from committing further crimes. McQuade (2016) states that a key component of deterrence is publication of potential and actual punishment. Brantly (2018:38) emphasises that it requires substantial relevant costs and the development of mechanisms to be established, and that additional costs are allocated to provide clarity for an adversary. The basis of the deterrence theory suggests that certainty, severity and celerity of punishment have a deterrence effect on offenders and would be offenders. The certainty element means how certain the possibility of sanctions to be enforced or how likely will the offender be punished, the severity element relates to how firm the punishment for the offender and the celerity element addresses the speed at which the punishment is enforced (Burns, Posey, Courtney, Roberts & Nanayakkara, 2017).

The deterrence theory has received considerable approval from scholars, militaries and policy makers in mitigating cyber risks and fostering stability of cyberspace (UN Institute for Disarmament Research, 2014). There are two basic types of deterrence: specific and general. Specific deterrence: prescribed punishment is designed to deter only the individual offender from carrying out the crime in the near future (Taylor *et al., 2017*). General Deterrence: punishment is designed to deter the general population from engaging in crime. Overall, the deterrence effect is often publicized to make potential offenders aware of the futility of participating in crime (Nagin, 1998:4042). The main aim of deterrence is to offer disincentives for potential computer fraudsters (Whitman, 2004).

Deterrence theory suggests that individuals can be dissuaded from committing antisocial activities through the use of countermeasures, ranging from strong disincentives to sanctions that are relative to the activity (Straub & Welke,1998:441). It is normally accomplished through the creation of fear and consequences of perpetration with the aim to discourage potential criminals from attempting fraudulent activities (Kimani, 2013). The objective is to proactively discourage potential violators from implementing a threat by warning them about logging policies and of remedial actions.

Deterrence is considered by functions, actions, operations and activities intended to prevent cybercriminal activities before they happen, more especially to discourage the attempt at committing fraud. Examples of deterrence include laws, regulations and policy implementation, card activation, bank verification methods, data and fraud management programmes (Deloitte, 2015). A major challenge in deterring a cybercrime activity is determining which online behaviour to focus on. In order for deterrence to work (Morgan,1985) emphasises that there should be a credible threat from a willing attacker and the willingness of the probable victim to react against the attacker. Other factors mention that a potential attacker must be satisfactorily concerned that their identity would not be exposed and the retaliation to be followed is the misuse of the obtained information (Hsiang Wei, 2015).

Howe & Pelser (2020) emphasise that financial institutions should understand the punishment level linked to each type of cybercrime incident or activity in order for the cybercrime activity to be dealt with. Furthermore, the punishment for the cybercrime should be transparent in order to achieve the desired deterrent effect on the cybercriminals (Tan, 2018).

3.5 Space Transition Theory

The space transition theory addresses the cybercriminal behaviour as it argues that people behave differently when they move from one space to another (Jaishankar, 2008:292-294). This theory also highlights that persons who repress criminal behaviour in the physical space have a propensity to commit a crime in cyberspace, which if they were in the physical space, they would not have committed due to their status and position (Wada, & Odulaja, 2012:79). Jaishankar (2008) stipulates that the space transition theory clarifies the nature of individuals who display their conforming and non-conforming behaviours in the cyberspace and physical space. This transition between the physical and cyberspace environments enables the individuals or cybercriminals to also migrate with their social values and alignments (Abayomi, 2020).

The postulates of the theory are:

- Persons, with repressed criminal behaviour (in the physical space) have a propensity to commit crime in cyberspace, which otherwise they would not commit in physical space, due to their status and position.
- Identity flexibility, dissociative anonymity and lack of deterrence factor in cyberspace provides the offenders the choice to commit cybercrime.
- Criminal behaviour of offenders in cyberspace is likely to be imported to physical space which, in physical space may be exported to cyberspace as well.
- Intermittent ventures of offenders into the cyberspace and the dynamic spatial-temporal nature of cyberspace provide the chance to escape.
- Strangers are likely to unite together in cyberspace to commit crime in the physical space. Associates of physical space are likely to unite to commit crime in cyberspace.
- Persons from closed societies are more likely to commit crimes in cyberspace than persons from open society.
- The conflict of norms and values of physical space with the norms and values of cyberspace may lead to cybercrimes.

The space transition theory concludes that informal online engagement, identity flexibility, lack of deterrence and dissociative anonymity attracts physical space criminals to the cyber space.
Ndubueve (2016) affirms that the theory provides a plausible insight into the nature of transition between the physical and virtual spaces and the implications for order in society. In cyberspace, everyone is connected to one another, therefore the chances that cybercriminals meet with other potential cybercriminals is high.

The main aim of this study is to conceptualise a cybercrime framework for Eswatini and to address the cybercrime gap that exists in Eswatini banks. The three theories applied in this study are applicable and relevant to this study for the following reasons:

The routine activity theory provides a deeper understanding of how the presence of its three components (suitable target, capable guardian and motivated offender) facilitate crime.

The space transition theory does not explain physical crime but cybercrime and how people move and behave from one space to the next. This theory is found to be more applicable in cyber-trespassing, cyber deception and theft and cyber pornography than cyber-violence (Kethineni, Cao & Dodge, 2017:7), which are all components of cybercrime. Moreover, cybercrime growth is escalating and there will be a thin line between physical and cyberspace offenders, resulting in a rise in cyberspace offender population (Karuppannan & Chandra, 2017). Therefore, the space transition theory is ever more appropriate and relevant to address this issue in the current situation.

The deterrence theory enables an examination of the countermeasures and effects on online fraud also known as cybercrime. The deterrence activities also assist in facilitation of preventative activities through the establishment of necessary awareness for the operators of that particular system (Alanezi & Brooks, 2014:3).

Jaishankar (2008) emphasised that one of the main catalysts of cybercrime in the context of cyberspace is a result of the nature and characteristic of criminal activities that conform to the changes in time coupled with identity flexibility, anonymity and lack of deterrence.

3.6 Theoretical framework similarities

The deterrence theory and routine activity theory view likely cybercriminals as rational actors that would consider engaging in a crime by deciding whether the benefits are worth it. Tillyer (2011) concludes that the deterrence theory and routine activity theory are complementary in predicting crime occurrence. The deterrence theory emphasises that punishment can demotivate potential cybercriminals, while the routine activity theory highlights that the presence of a capable guardian can discourage potential criminals (Hui, Kim and Wang, 2017).

3.7 Theoretical frameworks differences

The routine activities theory focuses on criminal events and disregards the criminal motivations of behaviour (Grohe, 2006; Williams, 2015). The space transition theory aims to explain and appreciate the causation of crime, the behaviors in the area of conforming and non-conforming behaviour in the physical and virtual space (Ahmed, 2019). Although the routine activites theory has limitations in addressing cybercrime in the virtual space (Ghazi-Tehrani, 2021), however the space transition theory complements it through a plausible insight into the nature of physical and virtual transition (Ndubueze,2016).

3.8 Theories underpinning the study

The theories underpinning the study are the space transition theory, deterrence theory and routine activity theory. There is need to understand how the routine activity theory explains the occurrence of a crime through the convergence of the three elements, offender, target and guardian.

The understanding of these elements will provide more knowledge on how to prevent a crime from occurring. The space transition theory will offer an explanation on how a cybercriminal behaves as they transition from the physical to a virtual space. The deterrence theory will provide an explanation on how a crime can be deterred to lessen the impact and eventually prevent it. The conceptual research framework is derived from the triangulation of these three theories.

3.9 Conceptual Research Framework

A conceptual research framework is used to give the research study a foundation to test the empirical data and to observe a phenomenon by aligning to existing and tested theories applicable to the study. The conceptual framework statements are used to stipulate a primary philosophy of what the study is about and the reasons why the phenomenon is occurring (Bickman & Rog, 2008).

The conceptual research framework below is meant to guide the study in addressing the gap identified in the introductory chapter. The theories underpinning the study are used to conceptualise a research framework for the study.

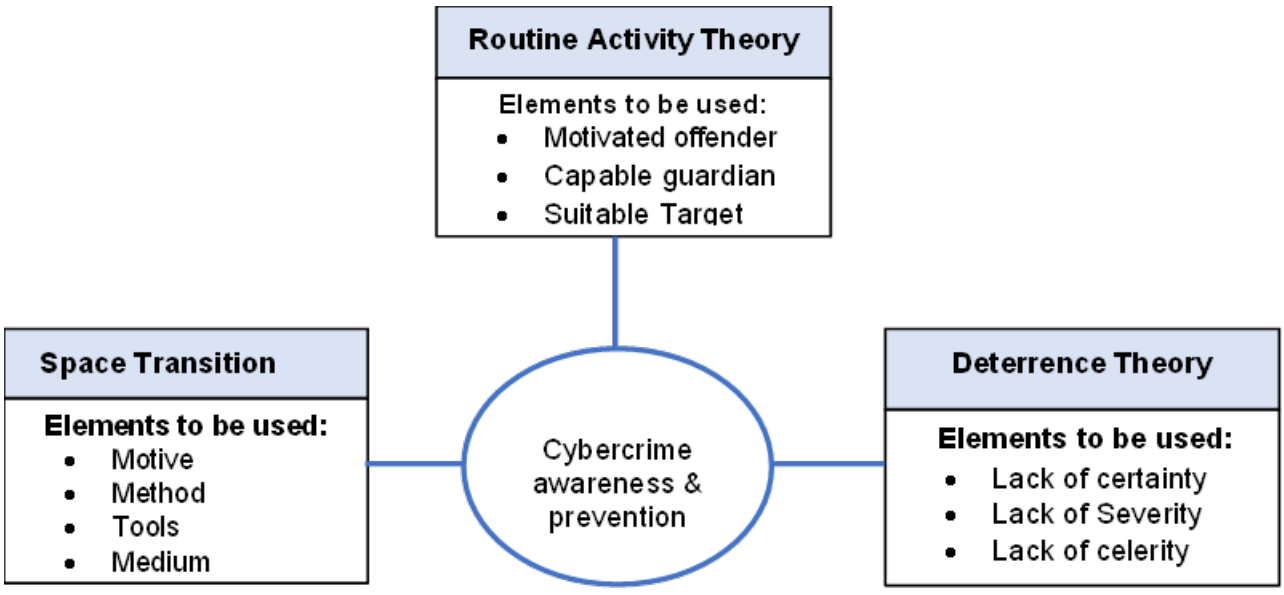


Figure 3.2: Conceptual Research Framework

The theories are triangulated as each of them brings an important aspect of addressing cybercrime in the financial environment for Eswatini Banks. Table 7 below describes the theoretical concepts and the alignment to cybercrime.

Table 3.3: Underpinning theories, concepts and approach

Theory	Criminology concepts	Cybercrime Approach
Routine Activity Theory	Crime occurs when the three elements meet, the motivated offender, a suitable target and the absence of a capable guardian (Cohen & Felson, 1979)	An offender will most likely engage in a criminal activity when the target is easy to access and when the presence of the guardian is low
Space Transition Theory	Provides an explanation for the criminal behavior in the cyberspace (Olayemi, 2014)	If the behavior of the cybercriminal in physical space can be performed in cyberspace, the crime is most likely to happen. In addition to the anonymity of the Internet, these elements lead to cybercrime
Deterrence Theory	Depends on an offender or potential offender's perception of the sanction threats or punishment as well as the likelihood to be caught or arrested (Tomlinson, 2016).	Deterrence is described by the actions, and methods aimed to prevent a likely offender from committing a crime.

3.10 SUMMARY

This chapter discussed the theories underpinning the study. The routine activity theory, deterrence theory and space transition theory are the theories informing and guiding the present study. The theories underpinning the study will be used to explain and extend the current understanding of cybercrime in the financial environment and incorporation into the body of knowledge. The next chapter discusses the research methodology followed in order to achieve the objectives of the study.

CHAPTER FOUR

RESEARCH METHODOLOGY

4.1 Introduction

This chapter outlines the research design approach which incorporates the philosophical paradigm in which the study is conducted. This chapter provides insights into how the study was conducted and the rationale for using the research methods engaged. It also explains the population, sampling strategy, research instrument design and data collection procedures. Yin (2009) verifies that research methodology is a strategy that enables a study to systematically achieve the set goal and tackle the research questions by applying the right research methods and techniques.

The study drew on the routine activity theory, deterrence theory and space transition theory as lenses underpinning the study. These theories served as lenses to understand how financial banks can minimise cybercrime activities. This chapter defines the importance of qualitative research in the field of research.

The main aim of this study was:

To develop a conceptual framework in perspective of Eswatini Banks using the space transition theory, deterrence theory and routine activity theory

The objectives to this study were:

- To analyse the effectiveness of Space Transition in the combatting of cybercrime activities in the banking sector.
- To evaluate the effectiveness of Routine activity in the combatting of cybercrime activities in the banking sector
- To assess how deterrence theory of a financial institution can combat cybercrime.
- To determine how banks in developing countries can minimize cybercrime activities in order to preserve their business.

4.2 RESEARCH PHILOSOPHY

Research philosophy is known to be the foundation of any research, the core position controlling the researcher in making the right and sustainable decisions on the data collection procedures and in answering the research questions (Bridges & Smith, 2007). It relates to knowledge management and the nature of knowledge in social sciences, and it includes assumptions about how researchers view the social world (Bahari, 2010). Easterby-Smith (2008) describes three critical reasons why philosophical understanding of research is important. Firstly, it guides the researcher in clarifying the research design, which includes the type of data or evidence required, the collection method and analysis. Secondly, having knowledge of philosophy further aids the researcher to choose the best option regarding the research design. Thirdly, it guides the researcher in avoiding wasting time while guessing which approach to adopt. Fourthly, it helps the researcher recognise and conceptualised designs that are not part of the previous research experience. In research philosophy, the different assumptions are made at every research stage and include epistemological, ontological and axiological assumptions (Saunders *et al.,* 2016).

4.2.1 Ontology

Ontology is the study of nature of reality, existence or being (Winit-Watjana, 2016). Realism is based on the premise that reality is predetermined by nature and is independent of consciousness and human cognition. Idealism is a philosophical tactic that has the fundamental idea that belief is merely factual reality, the single element worth knowing. Concisely, ontological assumptions concerning the nature of the phenomenon being investigated and different ontologies make different assumptions (Bahari, 2010). Ontology is also concerned with the nature of reality, how it exists to the assumptions individuals have about the world, the entities within the world and how they operate (Saunders, Lewis & Thornhill, 2009). For this study the ontological position adopted is relativism. This is because the researcher acknowledges that multiple realities exist which are shaped by the context. The context in this study is cybercrime in financial institutions. With relativism the reality is created by the human mind and categorises that as a result an observer may have opposing views about reality (Ade Bilau *et al.,* 2018). The overall understanding is that the researcher considers that the context changes and therefore there is a need to investigate more into the phenomenon.

4.2.2 Epistemology

Epistemology refers to the characteristics of scientific knowledge and the development of cognitive or views of scientific knowledge, which is a personal scientific philosophical belief (Elder, 2012). Epistemology relates to what is conceived as satisfactory and reliable knowledge (Allmark & Machaczek, 2018). Epistemology can either be objective or subjective and is mainly concerned with approaching research to produce valid and acceptable knowledge in a field of study (Ade Bilau *et al.,* 2018). Epistemology is the relationship between the researcher and what is known, while ontology indicates the nature of reality and the researcher's expectations about its nature (Smith & McGannon, 2017).

The best way to study and research about the cybercrime phenomenon in financial institutions is subjectively. The epistemological position adopted by this study is subjective because the researcher believes that knowledge should be discovered through subjective measures. Additionally, the researcher believes the interaction is important to maintain relevance and to be part of the research.

4.2.3 Axiology

Axiology focuses on the value judgement of the researcher (Bryman, 2012), personal values such as aesthetics, ethics and their association with knowledge, while the research reasoning is revealed by the logic of inquiry (Winit-Watjana, 2016). Axiology takes up two positions, namely from positivism which is value-neutral and interpretivism which is value-laden. The value laden position maintains that researchers should not eliminate their values, but rather, they should acknowledge, pronounce and group them (Ponterotto, 2005:131). The axiological position chosen for this study is relating to interpretivism because the researcher considers his values part of the research process and therefore cannot be excluded. Additionally, since this study deals with framework formulation, it is proper that an in-depth study is conducted to obtain a clear understanding of the phenomenon. Therefore, a close engagement between the researcher and the participants is necessary.

4.3 Research Approach

A typical research approach incorporates the paradigm, conceptual and theoretical frameworks including methods and techniques for designing, collecting, analysing and interpreting the data (O'Leary, 2007). This section describes the appropriate research paradigm for this information systems research.

4.3.1 Qualitative Research

Qualitative research involves the use of qualitative data using interviews, participant observation and documentation in order to understand and explain social phenomena (Myers, 1997). It is concerned with subjective assessment of attitudes, opinions and behaviour (Kothari, 2004). Qualitative research makes two major assumptions that reality is socially created and that the variables in a situation are intertwined, extremely intricate and challenging to measure (Szyjka, 2012). Bansal and Corley (2011) maintain that while qualitative research is known by its methodological variants, it still remains vital irrespective of the method used to demonstrate methodological rigour and theoretical contribution. For the purpose of this research, the qualitative approach will be followed, because it aims to provide depth of understanding rather than a statistical analysis of the event or phenomenon (Ary *et al.,*2010). The result of this approach is not driven by statistics, but it is supported by small samples of which the sample size can be a review of a single case (Creswell, 2013).

4.3.2 Positivist Research

In positivist research, the researcher is not part of the research and primarily relies on observations as a means of data collection (Livesey, 2006). Positivist research is normally characterised by repeatability (the ability to re-perform an observation and obtain the same results), refutation (the ability to challenge the research outcomes), replicability (the ability to independently replicate the observation) and falsifiability (the ability to disprove a particular phenomenon) and parsimony (the ability to explain complex phenomenon using the simplest logical explanation (Bhattacherjee, 2012).

The positivist paradigm concludes that human experience dictates knowledge, and this ontological view gives rise to the belief that the world consists of discrete and observable elements that interact with itself in a manner that permits a researcher the ability to observe and make conclusions in a consistent manner (Collins, 2010). Positivism is based on the idea that the social world exists externally, and that its properties should be measured through objective methods, instead of being inferred subjectively through sensation, reflection or intuition (Easterby-Smith *et al.,* 2002). Positivists are convinced that the researcher is disconnected from the subject studied (Ade Bilau *et al.,* 2018:600)

4.3.3 Interpretive Research

Hassan (2011) emphasises that the main focus should be on what people, whether individually and collectively, are thinking and feeling, and the attentions should be focused on the ways they communicate with one another, whether verbally or non-verbally. The main aim of interpretive research is to analyse human interaction, and the interpretation of such interactions employs the use of methods that are not common in the positivist paradigm (Weber, 2004). Similarly, Trauth and Jessup (2000) further mention that by choosing this approach, the researcher is admitting that access to the people being studied, comes through social constructions such as language, shared meanings and consciousness. The interpretive approach features efforts to acknowledge and recognise social phenomenon by generating meaning from experiences of the participants or contributors (Fadayo, 2018). In an interpretive research approach, the contributor or interviewee is active in the process and can influence the meaning of the findings. It takes into account the differences between circumstances and cultures while attempting to provide richness from insights received (Alharahsheh & Pius, 2020). It is known that the interpretive approach regards the research procedure as a collaboration activity between the participants and the researcher. Creswell (2008) mentions that interpretivists design and understand research by means of using terms, which are: themes and concepts that emerge from collected data or participants' lived experiences, processes and relations between chosen concepts, research questions, and observed in processes, experiences, views, perceptions, feelings of participants' lived experience in an unobtrusive and non-manipulated way within that context, context-based or context-

limited studies. The interpretivist approach permits interviewees to state their views and experiences on cybercrime in banks, permitting their interpretations and opinions to take precedence over those of the researcher. In this study, the interpretive research approach will be used as it permits for the emergence of unanticipated results (Klein & Myers, 1999).

4.3.4 Justification for Interpretive Research Approach

The study aims to bridge the gap by providing an in depth and detailed understanding of cybercrime activities in Eswatini Banks using the space transition theory, deterrence theory and routine activity theory. A gap that has been identified is that there is limited research conducted that relates to the cybercrime phenomenon specifically in Eswatini Banks, which makes this case study a unique one. The interpretive approach is significant in this research since unexpected data gathered will be interpreted from the interview interactions.

4.4 Research Strategy

Research strategy provides a clear direction of the research pathway as it assists the researcher to conduct research systematically (Kilani & Kobziev, 2016). It is also a methodological process through which research objectives can be questioned (Emhemed & Pandey, 2017). Bhattacherjee (2012) mentions a number of research design approaches such as case studies, experiments, surveys, ethnography and action research. These types are normally underpinned by the philosophical viewpoint and the nature of the research questions.

4.4.1 Case Study

Yin (2003) defines a case study as an empirical research strategy used to intensely study a phenomenon over a given period in its natural setting in one or more sites. It is viewed as a rigorous depiction and exploration of a social unit or a phenomenon such as an individual, group, community or institution (Merriam, 2002). Oliver (2009) states that, case studies use techniques including structured or unstructured interviews as well as direct observations which include direct measurements, participant observation and group discussion to gather information.

4.4.2 Justification for case study selection

Simons (2009) describes a case study as an in-depth exploration from multiple perspectives of the complexity and uniqueness of a particular project, policy, institution, program or system in a real life. The case study research strategy adopted:

Context – The nature of the study involves a phenomenon, which makes a case study approach most appropriate since it provides an intensive, holistic description and analysis of a single, bounded unit in a specific context (Poneli, 2015).

Control and Flexibility – The researcher will take the place of a viewer or outsider to the study the phenomenon, therefore the case study approach makes it suitable, since one of its strengths is that of being flexible and adaptable.

Theoretical Base – the study is based on the routine activity theory, deterrence theory and the space transition theory as theoretical base to delimit the study.

4.5 Research Design

Bless and Hidson-Smith (1995) define research design as the planning of any scientific research from the first to the last step. A case study is an empirical research strategy used to intensely study a phenomenon over a given period in its natural setting in one or more sites (Yin, 2003:47-49). The objective of this study is to conceptualise a cybercrime framework for Eswatini and according to Yin, (2013:47-50), a single case may be considered when the case is unique, revelatory or longitudinal, which is the current case with cybercrime. Due to the nature of this study a case study is more suited for complex social phenomena, which normally are not easily explained using methods such as quantitative, and the aim is to answer questions such as “how” or “why”.

4.5.1 Unit of analysis

The unity of analysis is defined as the variety of objects of a study (Graneheim and Lundham, 2004). Kumar (2018) further describes a unit of analysis as a thing, a person, a group of people, an organisation and the individuals within an area such as a country, a technology or an object that is the subject of the study in which the researcher is collecting data. In this study, the unit of analysis was identified as the cybercriminal activities under investigation and will be used to guide the data collection instruments. The unit of observation are the specific entities that the data was sourced from and for this study participants that address cybercrime issues in their respective jobs and activities were the unit of observation. The study was about cybercrime in local banking institutions and therefore the unit of analysis were local banking institutions.

4.5.2 Population

The location of this study will be in the Kingdom of Eswatini which is landlocked, bordered by South Africa to the North, South and West and Mozambique to the East. The surface area is 17,363 square kilometres. The country has four regions, Hhohho, Manzini, Shiselweni and Lubombo. There are five (5) main banks in the Kingdom of Eswatini, namely FNB, Nedbank, Standard Bank, Swaziland Building Society and SwaziBank, and they have branches in all the regions. Hhohho region is where the headquarters of all the banks are situated. The capital city being Mbabane has approximately a population of 68,000. In the last five years, the local banking sector,

including the Central Bank of Eswatini and subsidiary banks has experienced a rise in cybercrime activities. The case study will focus on the local banks using the qualitative research method, in understanding the phenomenon. Purposive sampling will be utilised in this research, since it will be addressing the cybercrime phenomenon in the banking sector. Neuman & Nueman (2000) further assure that purposive sampling is more adoptable in situations where the researcher chooses cases or elements that are predominantly informative. This means that purposive sampling is employed when there is a need to gather information from a specific group that has most of the information.

4.5.3 Sampling

A sample is a subset of a larger population, employing the proper sampling procedures to support the researcher in reducing costs, increase research efficiency, greater accuracy and access to information needed for the research (Latham, 2007). A sample is very important in a research project for efficiency and ethical reasons since one cannot study a whole population (Marshall, 1996). Sampling techniques are categorised into two, probability and non-probability sampling (Lohr, 2009). Figure 4.1 below shows the probability and non-probability sampling methods.

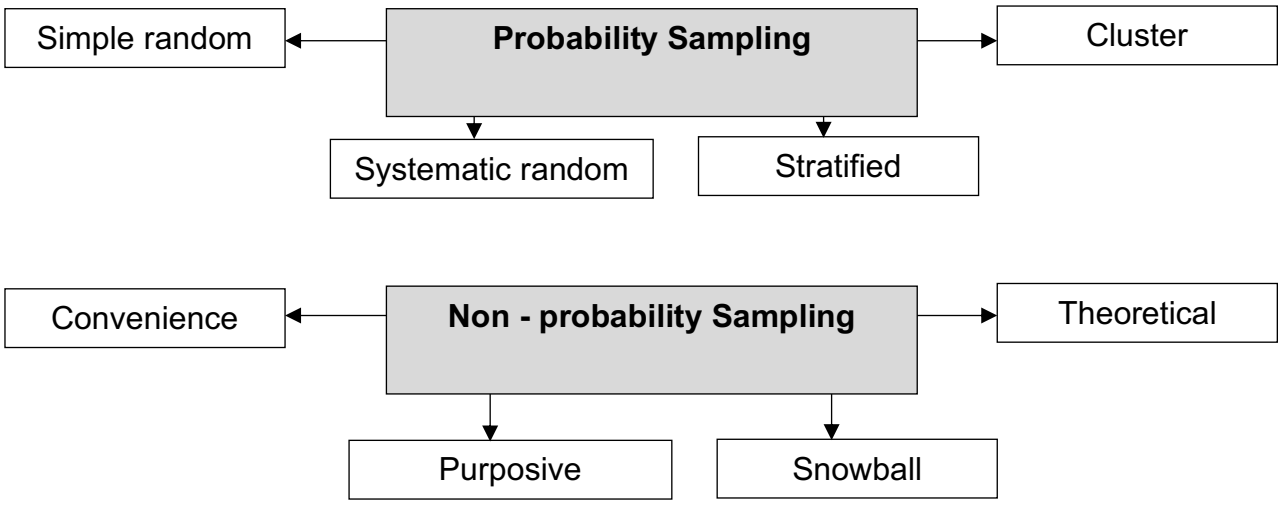


Figure 4.1: Sampling methods

Probability sampling focuses on selecting a representative of the population in order to simplify the entire population, while non-probability sampling is about choosing a sample that will aid the researcher in addressing research questions under

investigation (Devers & Frankel, 2000). The aim of non-probability sampling is to identify particular groups of individuals who are part of the phenomenon under investigation (Mays & Pope, 1995). For this study the non-probability sampling is applicable because the researcher selects the most suitable participants related to the phenomena, mainly focusing on the investigation's objectives.

4.5.4 Sampling method selected for this study

The study used a purposive sampling technique. The study sampled the local banks in Eswatini to provide information and knowledge towards conceptualising a cybercrime framework for the banking sector. This method was selected based on the researcher's knowledge of the population and the objectives of the study. The decision was based on the researcher's judgment and the investigation's objectives which are aligned with the chosen sampling technique to provide the answers to the research questions.

4.5.5 Participants

The key participants in this study were specialist employees from departments in the banks, stakeholders that are mandated to address on cybercrime issues and tasks. These participants are the ones who are solely responsible and have a vested interest and knowledge in curbing cybercrime in the best interest of the banks. The total number of participants were five (5) and they were contacted individually for participation in this study. The participants were from local Eswatini licenced banks.

Table 4.1: Population and samples

Population	Sample
Number of selected banks	4
Total number of selected staff	5
Total sample size	5

4.5.6 Data Collection Methods

A data collection method is a process whereby the research collects or gathers data that is required to answer the research problem (Patton, 1990:66). A one-on-one interactive approach will be adopted to ensure that the data is captured as much as possible, a recorder will also be used to ensure capturing of quality data.

For ethical reasons, consent will be obtained from the participants. Normally a disadvantage of interviews is that they tend to be time consuming, therefore, to minimise that effect, thematic analysis and data triangulation will be used. Therefore, since this is a case study, there are several strategies that can be used to collect data which includes interviews, direct observation, participant observation and archived records.

These sources of data do not have a relative advantage over one another, but should be utilized to complement each other (Yin,2013:47-50). Multiple methods of data collection should be used as inferences about the phenomenon of interest since they tend to be detailed and contextualised (Bhattacherjee, 2012:93). An advantage of using a case study is that one is able to perform research by engaging diverse forms of evidence including reviewing of documents, interviews, artefacts, observation and archival records (Yin, 2003:47-50).

4.5.6.1 Justification for selecting interviews as a data collection method

For the purpose of this study, an interview was considered appropriate, because one of the key strengths of interviews is that they provide perceived casual inferences (Gillham, 2000). The interview method made it easier to understand the problem from the viewpoint of the participants. When investigating cybercrime in banks, it is important to select suitable participants in the organisation being investigated in order to avoid a situation of getting a low response rate (Krambia-Kapardis, 2002). Qualitative research stresses the importance of context in data analysis (Denzin & Lincoln, 2005). This is important for the participants to choose and decide on the venue or location most comfortable for them to conduct the interviews.

4.5.6.2 Interview language

The interviews were conducted by the researcher using English as the preferred language. Eswatini has two official languages, and fortunately the participants had no problem in using English as the main interview language, therefore translation from the native language was not necessary.

4.5.6.3 Challenges faced during data collection

The majority of the participants responsible for cybercrime issues in the financial institutions were welcoming and participated with high levels of interest, but however, those who were not part of the interviews declined due to uncertainty on the information that they were going to share. One of the participants even said that he is afraid and worried that if he shares information, his superiors might enforce disciplinary hearing. The major problem is the issue of information leakage and the reputational risk that is being perceived by top level management.

4.5.7 Data analysis

Data analysis means to systematically organise, integrate and examine the patterns and relationships in the data in order to connect the particular data to concepts, generalisations and themes (Neuman, 2014:477). The study acknowledges the different types of qualitative data analysis in research which are thematic analysis, content analysis, narrative analysis, grounded theory and framework analysis. In analysing the collected data, the thematic analysis method was used. Thematic analysis is a qualitative data analysis approach that involves searching through data collection to find, analyse and report on recurrent patterns (Braun & Clarke, 2006).
The overall objective is to uncover themes that are related to a particular phenomenon (Archer, 2018). According to Joffe (2012:212) textual data collected from face-to-face interviews are most appropriate for thematic analysis. Since the data was collected from the industry experts personally, the data was analysed using thematic analysis and was considered most appropriate.

Data coding is considered as the transformation of data into a state that computers and accompanying application programs can understand and translate. The data analysis steps followed by the researcher were:

- Reviewing the transcribed one-on-one interviews
- Consolidating the codes into categories
- Analysing the sampled documents
- Comparing the data from documents and interviews with data from the literature review as proposed by Creswell (2013:160).

To aid the researcher in the development of theme clusters, the researcher will read the transcripts several times while using the tape recorder in order to identify recurring statements and themes from the data collected.

4.5.8 Ethical consideration

Cybercrime is a sensitive topic and ethics need to be highly considered in this study, as there is always a concern about breach of company and individual confidentiality. Therefore, the following measures will be taken in this study to address the issue, and the researcher will conduct this study in a responsible and respectful manner.

Informed Consent

Informed consent is the ethical norm that consists of voluntary participation and assurance of no harm to the participants during participation in a study or research project (Babbie, 2010:66). The researcher made sure that the participants are made aware in detail, of the nature of the study and its impact. The researcher ensured that the participants were informed that participation in the study is voluntary and withdrawal from the study process will be allowed. Prior to participating in the study, the participants were made aware of the consent form that forms part of the study.

Confidentiality, Privacy and anonymity

The researcher and participants must have clear understanding regarding the data, results and findings of the study (Maree, 2010:301). The researcher informed the participants that their information will not be shared and will be kept private. In addition, the principle of anonymity shall be applied. Regarding privacy, the responses from the participants will only be used for this study. This level of transparency encouraged the participants to freely share their views, opinions, and experience.

Respect and trust

The researcher should strive to gain support through trust and respect by convey to the participants the objective of the study explicitly (Creswell, 2013:174). The researcher will see to it that time and appreciation of the participants is respected by ensuring that the interview conversation space is friendly, and the participants must be able to feel at ease. This is to ensure that full cooperation and a high level of professionalism are obtained from the researcher in order to gain trust and respect from the participants. The researcher will hold preliminary discussions with the participants before the commencement of the actual data collection exercises. This is to ensure that the participants do not feel they are being victimised or forced into taking part in the study. In addition, this will also give the participants the opportunity to fully scrutinise the intention, purpose and impact of the study that they are requested to be part of. During the data collection process, the researcher will ensure that questions are asked in a clear and proper manner and solely focused on the subject being investigated. To further ensure trust, the researcher will not surprise the participants with questions or content that is not relevant to the study. In summary, the participants were instructed before the interview commenced not to answer any questions where they feel it might compromise the organisation's confidential data.

Researcher's role

It is crucial that the researcher coordinates all the activities of the study. The role of the researcher in the study is to create a partnership with the participants during the collection and analysis phases of the study (Maree, 2010:41). The researcher will see to it that preparation and collection of data, interaction with participants during interviews, appointment scheduling and data analysis, are all managed and controlled by the researcher at a high level of integrity, professionalism and ethical application.

- The researcher will present an ethical certificate from the university to relevant authorities seeking permission to conduct research among identified banking employees and stakeholders.
- Names of participants will not to be revealed to anyone, pseudo names will be used.

- Participants will be informed that their commitment to participate in the study can be reversed, that is, they can withdraw from the study at any point.
- Assurance will be given to the participants on the confidentiality of the data collected,
- An agreement of informed consent that details the ethical protocols will be observed and signed by the participants prior to issuing or utilisation of the data collection tools.

Interviews reflection

On completion of the interviews, the interviewer and the participants assessed the overall interview process and the outcome. The main purpose of this engagement was to obtain feedback from the participants on areas that might have been overlooked or missed out. Overall, the participants expressed appreciation to be given an opportunity to partake in this study. The participants were openly sharing their experiences and showed great enthusiasm during the engagement sessions. The end goal for this interview reflection phase is that the findings would add value to the financial institutions' cybercrime prevention initiatives.

Table 4.2 shows a summarised view of this chapter.

Table 4.2: Summary of the research methodology

Research Paradigm	Interpretivism
Research Design	Case study
Participants	Specialist employees focusing on cybercrime issues in the respective banks
Theoretical Framework	Routine Activity Theory, Deterrence Theory and Space Transition Theory

Research design • Unit of analysis • Population • Data Collection • Data Analysis	 Cybercrime activities Individuals Interviews (face-to-face) Thematic Analysis
Ethical Consideration	Every participant will be given a brief outline of the purpose of the study and what it involves. Once the researcher receives confirmation that the participant would like to take part in the study, the participants will be handed a participant information sheet as well as an informed consent form for signing before commencement of data collection.

.

4.6 SUMMARY OF THE CHAPTER

This chapter dealt with the aspects regarding the data analysis, interpretation and presentation. The study adopted the interpretivism research paradigm and case study approach was used to gather data for analysis and synthesis. Data collection was conducted using face-to-face interviews, reports and research articles. Participants were banking specialist employees focusing on cybercrime issues in the respective banks. The next chapter analyses data collected and discusses the study findings.

CHAPTER FIVE

DATA ANALYSIS AND DISCUSSION

5.1 Introduction

The previous chapter provided an explanation of the research methodology used. This chapter provides an analysis of the data gathered during the data collection phase. Thematic analysis was used to analyse the transcribed semi-structured interviews. Four distinct themes emerged from the research data. Semi-structured interviews were conducted with five (5) industry experts from the banking sector. Additionally, the preceding chapter discussed how data were gathered using interviews. Data collected from the banks were from the following industry experts.

- Industry Expert 1 = IT Manager
- Industry Expert 2 = Chief Information Officer (CIO)
- Industry Expert 3 = Technology Risk & IT Security Manager
- Industry Expert 4 = Senior Cybercrime Detective
- Industry Expert 5 = Information Security Practitioner

Thematic analysis is used to analyse the interview data and the themes were aligned to the study objectives. Below is a summary of the objectives and theories used:

Study Objectives

- To analyse the effectiveness of Space Transition in the combatting of cybercrime activities in the banking sector.
- To evaluate the effectiveness of Routine activity in the combatting of cybercrime activities in the banking sector
- To assess how Deterrence theory of a financial institution can combat cybercrime.
- To determine how banks in Eswatini can minimise cybercrime activities in order to preserve their business.

Theories used:

Routine Activity Theory
Deterrence Theory
Space Transition Theory

The following table lists the study objectives together with the theories as lenses.

Table 5.1: Study objectives aligned with the theories

Study objectives	Theories
To analyse the effectiveness of Space Transition in the combatting of cybercrime activities in the banking sector	Space Transition Theory
To evaluate the effectiveness of Routine activity in the combatting of cybercrime activities in the banking sector	Routine Activity Theory
To assess how Deterrence theory of a financial institution can combat cybercrime.	Deterrence Theory
To determine how banks in developing countries can minimise cybercrime activities in order to preserve their business.	Space Transition, Routine Activity and Deterrence theories

5.2 Analysis of the Qualitative data

This section analyses data and discusses findings from industry experts from three banks, Bank A, Bank B and Bank C. Bank A is the newest establishment amongst all the interviewed banks in the country, while Bank B and C have a long history of existence in the country. The themes identified in the data analysis are linked to the reasons why cybercrime transpires and how Eswatini banks can minimise exposure to cybercrime activities. The analysis was made by linking the themes to the study objectives:

- Theme 1 identifies and describes the awareness of cybercrime activities in the banking sector.
- Theme 2 analyses the effectiveness of combatting cybercrime activity through the lenses of the space transition, routine activity and deterrence theories.
- Theme 3 analyses the methods that financial institutions detect and manage cybercrime incidents.
- Theme 4 analyses and highlights the importance of compliance as an approach to minimize cyberthreats.

5.2.1 The link between the themes and research objectives

The main aim of this study is to conceptualise a cybercrime framework for Eswatini, whereby the four research objectives were derived from the main objective. The data collected fulfilled the requirements of the main research question and the objectives. Table 5.2 shows the connection between the themes that emerged from the data analysis.

Table 5.2: Research objectives, themes and sub-themes

Theme	Sub-theme	Research Objectives
Theme 1: Competence in cybercrime awareness	1. Insufficient experience in cybercrime awareness 2. Cybercrime Conviction	Objective 1: To analyse the effectiveness of Space Transition in the combatting of cybercrime activities in the banking sector. Objective 4 To determine how banks in developing countries can minimise cybercrime activities in order to preserve their business.
Theme 2: Cybercrime Prevention	1. Internal threat control 2. Insufficient cybercriminal threat knowledge 3. Target attractiveness	Objective 1: To analyse the effectiveness of Space Transition in the combatting of cybercrime activities in the banking sector. Objective 2: To evaluate the effectiveness of Routine activity in the combatting of cybercrime activities in the banking sector Objective 3 To assess how Deterrence theory of a financial institution can combat cybercrime Objective 4 To determine how banks in developing countries can minimise cybercrime activities in order to preserve their business.
Theme 3: Cybercrime Detection	1. Internal System Control 2. Limited expertise in cybercrime investigation 3. Audit trail enforcement	Objective 4 To determine how banks in developing countries can minimise cybercrime activities in order to preserve their business.
Theme 4: Cybercrime Compliance	1. Change Management	Objective 3 To assess how Deterrence theory of a financial institution can combat cybercrime

5.3 INDUSTRY EXPERT'S FINDINGS

5.3.1 Demographics of the participants

The qualitative study interviewed five (5) industry specialists from the banking sector. Their job descriptions included focus on cybercrime issues. The participants have worked for their organisations in their respective roles for more than 8 years and that reflects adequate possession of information and knowledge in the cybersecurity and cybercrime environment. The diverse composition of the participants allowed the collection of data from difference perspectives, therefore enriching the data. The financial industry consists of local and international organisations and the participant representation accommodated for both. The participants were from local and international /franchised financial institutions, and they are described below:

Industry Expert 1: This participant has experience in the IT banking industry, working in various departments within the information technology space. The participant was very comfortable with the questions asked and had no problem in sharing additional information. Although the company he was working for was fairly new in the country, the information he shared was sufficient and relevant for the study.

Industry Expert 2: This participant is a Chief Information Officer, possessing a lot of experience in the banking sector.

Industry Expert 3: This participant is a Technology Risk & IT Security Manager who was very cooperative and prompt in responding to the interview. The responses from this participant were informative and the interest shown was appropriate for the study.

Industry Expert 4: This participant was one of them most important ones because he works with cybercrime cases in the police force. He has been a cybercrime detective for the past 18 years. He was very supportive in sharing information and even guided the researcher in obtaining clearance from the Headquarters of the Police department.

Industry Expert 5: This participant is a former Information Security officer from one of the local banks. Currently she works for a communications regulator under the cyber and information security department.

Table 5.3: Demographics of the industry experts

PARTICIPANT	BANK TYPE	POSITION	EXPERIENCE
Industry Expert 1	International/Franchise	IT Manager	8 years
Industry Expert 2	Local	Chief Information Officer (CFO)	10 years
Industry Expert 3	International/Franchise	Technology Risk & IT Security Manager	10 years
Industry Expert 4	Government (Royal Eswatini Police Fraud department)	Senior Cybercrime Detective	20 years
Industry Expert 5	Former Information Security Officer	Information Security Practitioner	10 years

5.3.2 Interview findings from industry experts

This qualitative study interviewed five (5) industry experts from the banking and law enforcement sectors, to furnish information and knowledge towards conceptualising a cybercrime framework for the banking sector. The conclusion of these interviews were used to formulate the cybercrime framework.

5.3.3 Emerging themes

The process of developing themes involves the transformation of the findings into an interpreted format. Patton (2002) clarifies that it involves separating the data that is not applicable, classifying the data into logical themes and consolidating the data. The researcher allowed the participants to express themselves as they engaged with the interview question. In this way, the researcher encouraged the participants to use words and expressions so that the true meaning of the phenomenon is obtained.

The researcher sought to explore and analyse the cybercrime phenomenon in financial institutions in Eswatini. Furthermore, the researcher embarked on this study in order to gain an understanding on how to provide measures that the banks in

Eswatini can adopt to minimise their risk and exposure to cybercrime. The gap in knowledge concerning the cybercrime phenomenon was determined through the use of the space transition theory, deterrence theory and routine activity theory. The study will lead to the formulation of a cybercrime framework that will be useful in predicting new ways to understand and fight cybercrime activities in the context of the banking sector.

During the data collection phase, the researcher used the participants' response and feedback to generate and analye the data to develop the themes. Generation of themes that originated from the interview data was converted into data that made sense (De Vos *et al.,* 2011). The qualitative approach enabled the researcher to generate as many themes as possible from the participants. The generation of the themes also resulted in inappropriate or repeated information, whereby that information was discarded as a result of theoretical saturation. The researcher during interviews reached a stage where comments and phrases were repeatedly mentioned.

5.3.4 Discussion of themes and sub-themes

The themes, subthemes and categories that emerged from the study are discussed in the following section and presented in Table 5.4.

Table 5.4: Summary of Theme 1 – Cybercrime Awareness

Theme 1: Competence in cybercrime awareness (cf. 5.6.1)	
Subtheme 1.1 (c.f. 5.6.1.1) Insufficient experience in cybercrime awareness	Subtheme 1.2 (c.f. 5.6.1.2) Cybercrime Conviction
Categories	
• Banking services • Vulnerability to cybercrime • Qualifications • Guidelines	• Conviction rates

Source: Author's own

5.3.4.1 Theme 1 – Competence in cybercrime awareness

Competence in cybercrime awareness is a very sensitive issue that most organisations and cybersecurity experts encounter on a constant basis. The aspect of awareness helps organisations especially the staff, customers and management to learn about the various malicious methods that cybercriminals use. A number of factors regarding the importance of cybercrime awareness have been highlighted in literature. In theme 1, two subthemes emerged that describe the gap that exists in cybercrime awareness. Participants were asked about the lack of cybercrime awareness in the banking industry. Figure 9 shows the identified subthemes.

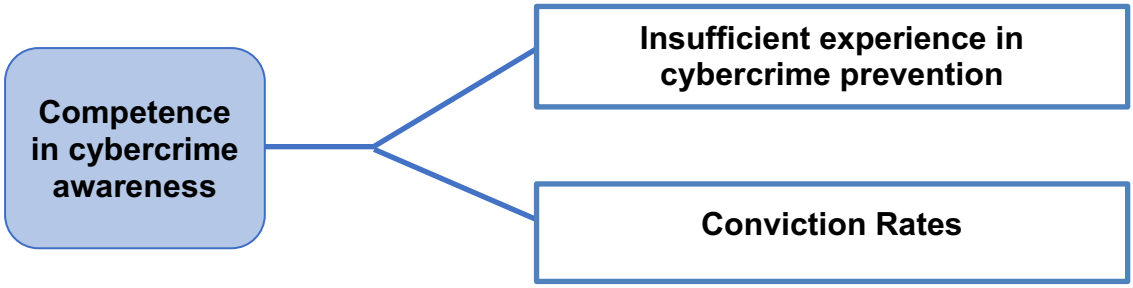


Figure 5.1: Layout of Theme 1 with subthemes

5.3.4.1.1 Insufficient experience in cybercrime awareness

Cybercrime awareness requires extensive experience and dedication to identify and address cyber incidents. It is crucial that the right content, tactic and knowledge is applied to address each cyberthreat or incident for proper assessment. Basically, in addressing cybercrime there is a need to be prepared and constantly be updated to meet the changes associated with cybercrime. Malby *et al.,* (2013) mention that the receipt of information about cybercrime did not necessarily translate into "feeling informed" about cybercrime.

Banking services

Cybercriminals use various techniques and methods to gain access to client information. The responses from the participants outline the banking services provided by the banks as potential entry points to be exploited by cybercriminals. In the banking environment, the banking services are the link between customers and the bank and therefore they become the gateway for cybercriminals to exploit. The participants were

asked about their knowledge of the banking services provided and the level of access by the participants.

Industry expert 3 responded by saying:

> *"As a Bank we offer Walk-in services which includes registration, cash withdrawals and checking statements. These are all internal services available inside our branches. Our outside services channel are ATM and Mobile banking"*

Also, industry expert 1 noted that:

> *"Since we are a newly established bank with a focus on providing online services, we have adopted a centralised approach of providing services through our Headquarters based in Johannesburg."*

Industry Expert 2 stated that:

> *"Cellphone Banking; Physical channels (ATMs and Cash Deposit Machines; Walk-ins, eBanking Application; Internet Banking and personalised relationship banking are the major banking services mostly accessed by our clients)"*

In concurrence Industry Expert 5 said:

> *"Internet banking, Enterprise and Business online are the most recent services that our customers are using"*

Banks offer diverse services that assist customers with their business and financial transactions. All the banks offer similar services to their customers which are part of the cyberspace, further increasing the chances of cyberattacks across the banking sector. These service channels also act as entry points for cybercriminals to exploit and they should be protected and monitored constantly for potential cyberattack incidents and threats. Banks constantly make means to defend against cyberattacks, but however, it is proving to be a difficult task to keep pace due to cybercriminals constantly implementing new ways to access banking services. Strom, *et al.,* (2017) state that even if organisations enforce software upgrading and patching programmes, a cybercriminal often finds ways such as zero days or social engineering tactics to penetrate the organisation network.

Vulnerability to cybercrime

The vulnerability of banks to cybercrime is due to the attractive target, which is money, that is kept by banks. The participants were asked about their awareness and knowledge regarding the banking services that are most vulnerable to cybercrime.

Industry Expert 2 mentions that:

"In our case as a bank it has been the ATMs and the Mobile Banking channels"

Also, Industry Expert 3 noted that:

" For our bank the cellphone banking is the most vulnerable target for us"

While Industry Expert 1 had a different response:

"At the moment since we are a newly established bank, we have not yet established the vulnerability level of our services. For our local Eswatini branch we have not started to map out the services"

Industry Expert 5 responded by saying:

"Internet Banking was the most vulnerable because most of our customers were familiar with the new technology"

The responses from the industry experts conclude that banking services are vulnerable to cyberattacks. These vulnerabilities are due to the value of the data and money that banks host (Packetlabs, 2021) and the banking services are the first point of contact between the customers and the banks. Furthermore, as customers use various devices and methods to conduct their banking transactions, it increases the opportunity for cybercriminals to take advantage of the entry points.

Qualifications

In the cybersecurity environment, the type of qualifications plays an important role in executing cybersecurity activities. In today's cyberspace environment, qualifications are contextually designed to address issues specific for each type of Information

technology field. The participants were asked about their positions and the type of qualifications they hold towards addressing cybercrime issues in their organisation.

Industry Expert 1 commented:

> "*Unfortunately, I have been in this position for less than a year and I have a Masters in IT and a Certificate in Ethical Hacking"*

Whereas Industry Expert 2 said:

> *"I have been holding this position for 2 years now and I have a degree in Computer science and a Master's in Business Administration"*

It was a similar case with Industry Expert 3 who mentioned that:

> *"I have been in this position for two and a half years and I hold a B.Sc in Computer Science and Mathematics. In addition to that I also possess professional qualifications in CISSP, CISM, CISA and CGEIT"*

According to the responses above, all the industry experts have a respectable educational foundation to handle cybercrime issues within their organisations. The participants were further asked if they are confident to deal with cybercrime issues looking at the strong foundation of qualifications they possess.

Industry Expert 3 concurred by saying:

> *"For cybersecurity yes I am very confident because my focus is based on cybersecurity, however for cybercrime I am not equipped enough.*"

In support Industry Expert 2 said:

> *"I am definitely confident because of my CISSP certification."*

The same views were also shared by Industry Expert 1 who said:

> *"For cyber security I am equipped enough to handle, however for cybercrime I still need more assistance and guidance.*"

The participants admitted that there they are not confident to handle cybercrime issues as a result of the speed of change and adaptation. One of the factors to this issue is the speed in which cybercrime incidents occur and the lack of response from the relevant stakeholders. Acquiring the right qualification further increases the knowledge

base in cybercrime awareness as well as increasing the cybersecurity practitioner's confidence. More importantly, vetting and verification of their qualifications and references should be checked prior to employment (Mwai, 2015).

Guidelines

Guidelines play a vital role in providing assurance that the right steps and processes are followed. In terms of the availability and usage of guidelines in addressing cybercrime, the participants were asked:

Industry expert 1 responded by saying:

> *"Unfortunately, we do not even have an IT structure that shows how the information technology processes and related departments should work together, however this is in the plan of action from our Headquarters."*

Industry Expert 2 concurred by saying:

> *"At the moment we are guided by the IT Security Policy which I feel it needs to be improved looking at how cybercrime is evolving."*

This was backed by Industry Expert 3, who said:

> *"Yes, we do have policies and guidelines."*

With the banks, the existence of policies and guidelines is a good method that greatly assists in addressing cybercrime incidents. The industry experts were probed about the existence of a cybersecurity strategy, and the status of its existence and implementation. Industry Expert 3 said;

> *"Yes, we do have a cybersecurity strategy and it defines programs and controls that align to the strategy and implement it incrementally."*

In agreement, Industry Expert 2 said:

> *"Yes, a cybersecurity strategy exists, and the Board is aware of it"*

In support, Industry Expert 1 stated that:

> "*Yes. We define programs and controls that align to the strategy and implement it incrementally*."

Furthermore, Industry Expert 5 confirmed:

> *"Yes, a cybersecurity strategy is mandatory, and it is implemented within the headquarters and cascaded to the country branches."*

The level of awareness from the participants shows that there is a good starting point to map out current and potential cybercrime incidents within an organisation. In most organisations, cybercrime awareness is often overlooked especially during ICT infrastructure expansion (Matengu, 2012). The existence of a cybersecurity strategy shows that the banks have a tool that assists in addressing cybercrime activities. The response from the participants indicates that the alignment and sharing of the strategy with the relevant stakeholder is a commendable and encouraging effort.

5.3.4.1.2 Cybercrime conviction

Cybercrime conviction is very important in enforcing the culture of cybercrime resistance. Cybercrime resistance requires extensive, enterprise-wide focus, organization commitment, skills and funding to support and promote cybercrime prevention initiatives (Phil, 2016). A high cybercrime conviction rate strengthens the strategies and methods that an organisation utilizes in cybercrime prevention campaigns. One of the contributing factors in low conviction rates is failure of cybercrime victims to report and lack of evidence to support the case. Mutune (2023) emphasises that unreported cybercrimes contribute to a lower prosecution and conviction rate.

Cybercrime Conviction Rates

Conviction of cybercriminals is often low in cyberspace. This creates a huge and sensitive gap because the importance of convicting cybercriminals sends out a message that engaging in any type of criminality has its consequences. However, in the present state, the rate of conviction continues to be low. The cybercrime phenomenon needs a unique knowledge approach in receiving information on cybercrime incidents, arresting protocols, investigation, evidence collection and preservation and the understanding of the general law enforcement processes (Nodeland *et al.,* 2019).

Industry expert 2 mentions that:

> *"At our bank we have not arrested nor taken any measures to fully address cybercrime issues when it comes to arresting the cybercriminals. Normally we will hand over all the information we have about the incident. What makes the whole situation painful is that we have to wait for the police to update us about the case "*

A similar response was shared by Industry Expert 3:

> *"Internally – We have not had evidence of those types of activities in recent years (at least after I joined) Externally there have not been any that I know of. I have seen been wondering how as a unit of the bank are we going to attend to sudden cyber-attacks*"

Industry Expert 5 reported that:

> "*Cybercrime convictions are low. There have been many incidents where I would submit reports on cybercrime for all the branches to management, hoping that the criminals would be caught. But later in the following weeks when I make a follow up, I would be told that nothing has been done."*

A low conviction rate results in a high tendency for cybercriminals to continue to commit crime. One major risk of cybercrime is that the cybercriminal is seldom caught or even arrested, and such an act exposes organisations to numerous targeted attacks (Mutune, 2023). Once cybercriminals observe and succeed in the intended operation, the motivation to carry out more operations will be high. Furthermore, cybercriminals evade arrest through corrupt connections (Hall *et al.,* 2020), registering fake websites and using malicious domain names (Chen, 2023). This type of awareness will aid financial institutions to apply more rigid interventions that will further assist law enforcement in convicting future cybercriminals.

Table 5.5: Summary of Theme 2 – Cybercrime prevention

Theme 2: Cybercrime prevention (c.f 5.6.2)		
Subtheme 2.1 (c.f 5.6.2.1) Internal threat control	Subtheme 2.2 9 9 (c.f 5.6.2.2) Insufficient cybercriminal threat knowledge	Subtheme 2.3 (c.f 5.6.2.3) Target attractiveness
Categories		
• Responsibilities • Experience	• Cybercrime Management Approach • Monitoring and reporting • Organisation size and management support • Cybercrime methods • Management's cybercrime perception • Cybercriminal participants	• Cybercrime awareness encounter by staff members • Cybercrime understanding • Cybercrime loss due to the lack of enforced target security • Detection tools

Source: Author's own

5.3.4.2 THEME 2 – Cybercrime Prevention

The reliance on technology has become a gateway for cybercriminals to use for cybercrime activities. It is therefore important to place prevention methods as a top priority for individuals and organisations. Prevention of cyberthreats and attacks is one way of fighting cybercrime. This study sought to present the findings regarding the different aspects of cybercrime prevention in the banking context.

Three subthemes that describe the factors that contribute towards the challenges of preventing cybercrime within a financial institution appeared within theme 2.

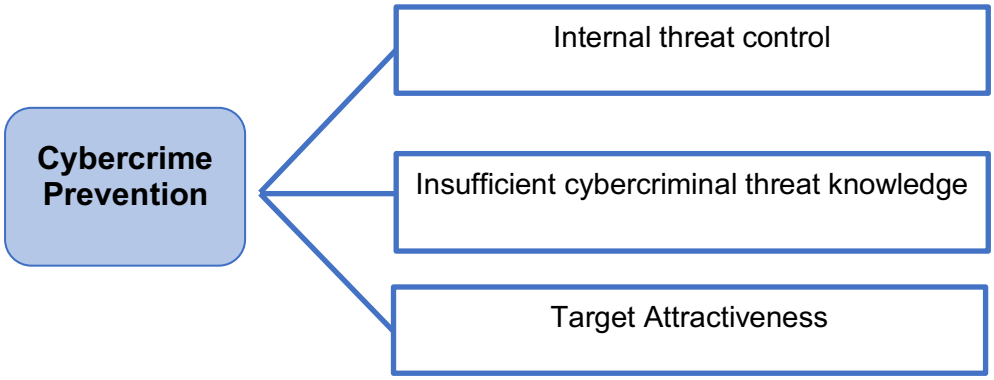


Figure 5.2: Layout of theme 2 with subthemes

5.3.4.2.1 Internal threat control

Cybercrime can be committed either from inside or outside an organisation. The threats that happen within the organisation are called insider threats, which normally are employees that will exploit a gap or an intentional violation of the company policies. Controlling the internal threat impact is important to prevent any reputational risk that an organisation can encounter. External attacks also exploit network and infrastructure gaps, and the added victim is unsuspecting customers.

Responsibilities

Participants were asked about the responsibility of developing and implementing the cybersecurity strategy. The responses show that most of the participants understood the importance and role of a cybersecurity strategy.

Industry Expert 1 stated that:

> *"The Chief Technology Officer has been given this task and also to coordinate with the other departments. Since we are a new bank, I am still learning the business approach of communication, however I must say I have observed that my supervisor is engaging me."*

Also, Industry Expert 2 said:

> *"This responsibility solely lies with the Chief Information Officer who then also makes sure that the strategy is cascaded to all departments and branches in the bank. We do meet at schedule meetings to update one another the progress that we have made"*

Industry Expert 3 was more elaborative saying:

> *"The IT Security organisation coordinates this activity at Group level. Involved are the Group IT Security resources as well as the operating companies' members of the IT Security cluster, e.g., IT Security team."*

It is imperative to note that the responsibility aspect in implementing cybersecurity plans or strategies must be held by the unit or a staff member responsible for information security issues. Since insider threats can do more damage than external forces, it is important that financial institutions develop and implement plans or strategies and assign the relevant person to drive them.

Industry Expert 5 reported that:

> *"Yes, at the headquarters we do have a unit that focuses on cybercrime and cybersecurity issues for the whole bank, and because we are a big bank, the headquarters makes sure that we contribute and make comments."*

The responses show that the banks have dedicated people to drive the implementation of the cybersecurity strategy as well as the processes to ensure proper

implementation. Pribanic (2020) mentions that while a majority of organisations have sufficient strategies implemented to protect against external cyberthreats, there is still a system lack in protection against internal threats. Therefore, a detailed and comprehensive cybersecurity strategy is a good starting point to map out how cybersecurity and cybercrime issues should be addressed, in particular the internal threats. According to Belaz, Krasznay & Szabo (2020), a cybersecurity strategy works well it if implements the contents and security goals.

Experience

Promptly dealing with cybercrime is very important due to the nature of the speed of change and adaptation. The industry experts were asked about the ways in which they deal with cybercrime in their units or departments in the organisation.

Industry Expert 1 said:

> *"We do not have a local unit yet. It is one of the strategic projects that will definitely introduced."*

In support, Industry Expert 2 said:

> "*We do have an IT Security Department that deals with crime issues including cybercrime."*

Industry Expert 3 concluded:

> *"Any matters of criminality, including cybercrime, are dealt by a separate unit called Fraud and Investigations. Specialist business units, such as IT Security, are involved to support the unit on a need-to-have basis."*

Based on the responses above, all the banks have a good foundation in terms of units and departments that address cybercrime issues. This further shows that the banks have allowance to improve and expand the departments or units to accommodate the ever-changing landscape of cybercrime. According to Ho, *et al.,* (2023) organisations are hiring cybersecurity managers at an alarming high rate and are using new techniques and various cybersecurity standards and frameworks to prevent cybercrime.

5.3.4.2.2 Insufficient cybercriminal threat knowledge

Sufficient knowledge about the behaviour of cybercriminals in the physical and virtual space is a major contributor in preventing cybercrime. Limited knowledge creates a gap that cybercriminals can exploit, and moreover for an organisation, this creates a bigger problem. Organisations will face an information and knowledge deficiency in addressing the everchanging cybercrime landscape.

Subtheme 2.1 is concerned with the existing and potential knowledge about cybercriminals which contributes to the planning and response approaches that can be applied in preventing cybercrime.

Cybercrime management approach

Approach is a very crucial aspect in understanding the dynamics of cybercrime in terms of awareness, investigation, detection, mitigation and reporting. Participants were asked about the types of cybercrime management approaches that they utilise in their organisations when addressing cybercrime. The application of the most appropriate and relevant management approach in addressing cybercrime in an organisation is an important element.

Industry Expert 1 responded:

> *"Since we have recently established in the country, we apply the preventative approach."*

In support, Industry Expert 3 focused on the engagement of other stakeholders and the aspect of controls by saying:

> *"There are a combination of activities and controls – proactive and reactive. In as far as cyber-crime prevention, mainly proactive controls are deployed that attempt to prevent successful crime execution. These include customer awareness activities that are performed in conjunction with the Eswatini Bankers Association. Some of these controls are inbuilt in products that attempt to make it harder to access customers banking information."*

Industry expert 2 responded:

> *"It is a deterrent approach as well as preventative. For externally threats we use firewalls and internally we use our customised approach called PPDR approach (Prevent, Prepare, Defense and Respond)"*

Similarly, Industry Expert 3 said:

> *"Looking at the seriousness of cybercrime we have adopted the zero-tolerance approach"*

Industry Expert 5 was more elaborative by saying:

> *"'We use a layered approach which is dependent on the technology adopted by the bank beginning of each year* and we have *introduced awareness initiatives, implemented technology that monitors and prevents cybercrime incidents across all our branches. In addition, we often get support from our main branch in Johannesburg through constant meetings, trainings and feedback sessions"*

The approaches used by these banks include preventative and responsive elements. The application of the chosen approach by the respective financial institution is dependent on the severity of the cybercrime incident or threat. The responses show that the banks are leaning more towards the preventative and reactive approaches to manage cybercrime threats and incidents. However, there is a need to implement the most appropriate approach that will address cybercrime issues.

Qasaimeh *et al.,* (2022) mentions that predictive systems effectively combact cybercrime and should be integrated with existing cybersecurity software of financial institutions. A proper implementation of management approaches reduces the possibility of cybercriminals to commit the crime, particularly the transition of the cybercriminal from physical space to cyberspace and from cyberspace to physical space. Furthermore, banks should not only be reactive but must also be proactive in order to effectively address future cyber risks (European Central Bank, 2016)

Monitoring and Reporting

Monitoring and reporting are important aspects in mitigating cybercrime through information and knowledge transfer. Keeping informed about the latest types of cyberattacks and incidents is crucial in addressing cybercrime.

The participants were asked about the existence of monitoring and reporting mechanisms within their organisations.

Industry Expert 1 reported that:

> *"We normally report to the board and within the board there is an IT Steering Committee where the IT Security Officer is a permanent member. The reporting period is quarterly. At the moment there are plans to develop an IT Security Board. In terms of monitoring, we use 3rd party organisations.*

In support, Industry Expert 3 said :

> *"For cybersecurity, yes…. A cyber security incident will only escalate to a cybercrime level as and when it has been determined to be a criminal activity or when reported from external sources"*

Industry Expert 5 confirmed:

> *"Yes we do have monitoring and reporting mechanisms, which are also updated together with the local team in the country and the team from the main branch in Johannesburg"*

From the responses provided, it is encouraging to note that the activity to report cybercrime threats it taken seriously. Encouraging a culture of reporting within the organisation, has a positive impact in addressing cybercrime incidents. The presence of effective reporting mechanisms is crucial in conjunction with employees in order to effectively mitigate the occurrence of cyber incidents (Bhatti, & Jamil, 2023). It is even more important to enforce it with the monitoring aspect so that a complete and stable mechanism is formed.

Organisation size and management support

Cybercrime activities detection and support has a correlation with the size of the organisation and level of support. An organisation that has many departments is more susceptible to cyber-attacks. Additionally, the support need for staff also increases exponentially. The participants were asked to respond to the support that management provides and the level of IT experience in the organization

Industry Expert 1 was of the view that:

> *"At the moment our awareness on this issue is low. The problem that I have seen is that there are many departments which are not coming forefront with information that can assist me to action on it"*

A similar response from Industry Expert 2 was noted:

> *"Yes, it does because we are a big bank and the number of branches that we have affect how to consolidate information from all the branches we have"*

Industry Expert 3 elaborated on another point about investment stating that:

> *"Investment that is made in preventive and detective controls indicate that the Bank's approach to cyber security is sensitive to the impact of the discipline"*

On a different response, Industry Expert 5 said:

> *"No, the size of the organisation does not influence the severity of cybercriminal activities. The support that I will receive from my colleagues in the other branches based in South Africa, made the cases easier to work on. As I mentioned earlier that the meetings we would hold daily and weekly, helped us a lot"*

Staff members are regarded as stakeholders and by obtaining their views on their understanding of cybercrime, mitigation and trends, it is therefore important to consolidate that information. This information needs to be aligned with the overall cybersecurity strategy to ensure that elements such as financial performance, customer and stakeholder satisfaction are maintained at a high level. As the organisation expands, the support from management in addressing cybercrime should synchronise with the other elements to limit the impact of cybercrime. Akinbowale, Klingelhofer and Zerihun (2022) affirm that the increasing rate of cybercrime is inversely proportional to the financial performance, stakeholder satisfaction and reputation of the financial institution. It is therefore important that banks should engage in research to determine innovative ways of counteracting cybercriminals (Njeru & Gaitho, 2019).

Cybercrime methods

Cybercriminals use every available resource to gain access to a system, therefore increasing the chances for gaining access. The participants were asked about the most common mechanisms cybercriminals use to perpetuate cybercrime.

Industry Expert 2 mentions:

> *"From the articles I read and conversations I share with my colleagues, Social Engineering is the number one method used by cybercriminals"*

A similar and more elaborate response from Industry Expert 3 was:

> *"There are quiet a lot of these methods. I am aware of bank card cloning and skimming, SIM Card swapping and cloning, credential exploitation, social engineering and phishing"*

Industry Expert 5 was on point by saying:

> *"Phishing and Social engineering"*

It is clear that the industry experts are informed about the mechanisms or techniques that cyber criminals use to engage in cybercrime activities, however cybercriminals are constantly implementing innovative ways to engage in cybercrime activities, and therefore cybercrime experts within financial institutions should keep abreast with the latest developments as a preventive approach to cybercrime. Financial organisations should deliberately make efforts to learn more and in detail, about each type of method used by cybercriminals. Phishing and social engineering methods are the most common methods used by cybercriminals due to their flexibility and adaptability to be contextualised to each cybercrime activity. Understanding the methods used to identify and find cybercriminals is an important part of cybersecurity because awareness of these methods increases the confidence and skill of the cybersecurity professional (Horan & Saiedian, 2021). It is important to point out that although the industry experts are aware of the mechanisms, however there is still a gap in understanding how the mechanisms or techniques work in the hands of the cybercriminals.

Management's cybercrime perception

Perception of cybercrime is a crucial element in preventing and addressing cybercriminal activities. The level of perception should be maintained to limit the chances of success for cybercriminals. In the case of management in organisations, this a top priority that should be cascaded across all the areas of the organisational structure, policy development and strategy. The participants' responses on the perception that management has towards cybercrime was recorded as follows.

Industry Expert 2 said:

> *"Management is comfortable with the situation, from the meeting we normally hold, they portray a picture of everything being under control"*

Industry Expert 3 noted that:

> *"Cyber Security is the number 1 thought in technology delivery within our banking group"*

Supporting the initiatives in addressing cybercrime is a very important aspect as highlighted by Industry Expert 5 who said;

> *"Management fully supports cyber security activities by investing in tools and people in order to mitigate the risks. Our management knows that cybercrime is highly likely to occur and the threat landscape is always evolving"*

In addition, when the participants were further asked about factors that contribute to cybercrime within their organisations, Industry Expert 1 said:

> "*Disgruntled employees, lack of awareness, poor IT security infrastructure, bad configuration of our IT systems definitely contribute to cybercrime within the organization"*

This was confirmed by Industry Expert 2 who said:

> *"Not applying the controls that are raised via the awareness activities causes the institution to suffer severe losses by cybercrime operations."*

The responses from above show that management does consider cybercrime to be a serious issue, however some responses show lack of urgency in addressing cybercrime.

Lack of commitment in enforcing stringent measures is a factor that influences cybercriminal activity to increase. Therefore, an inconsistency in cybercrime perception adoption results in a weakened cybersecurity culture in the organisation, and which is vulnerable to cybercrime.

Cybercriminal participants (Internal vs External)

Cybercriminals are constantly looking for new ways to penetrate systems by using new methods to remain anonymous in cyberspace. In addition, they also invest in upgrading their technical skills. Cybercriminals may be internal or even external agents, and a majority of these crimes is a common practice where they collaborate. The participants were asked if they believed cybercrime activities were conducted by insiders, disgruntled ex-employees or cybercriminals.

Industry expert 2 explained by saying:

> *"Ever since I joined the IT environment, I strongly believe that most of this fraud cases are a result of external people*"

However, a different response from Industry Expert 3 was:

> *"We have not had evidence of those types of activities in recent years (at least after I joined) the bank"*

Industry Expert 5 said:

> *"All the years that I have worked in the bank, I am strongly believe that insiders and cybercriminals are the two types of people who are behind the majority of these cybercrime cases"*

The responses show that there is a lack of knowledge on whether the cybercrime offender is external or internal. This is a crucial gap that results in cybercriminal activities to continue to occur as a result of this gap. It is fundamental that the personnel responsible for cybercrime analysis within the banking sector make efforts to understand the nature of the cyberattack, the factors and the motives that makes it attractive to cybercriminals. The major problem is the human factor in protecting the IT systems against cyber-attacks which is a caused by irresponsibility, carelessness and an improper induction of employees (Belaz, Krasznay & Szabo, 2020). This is where cybercriminals take the most advantage.

5.3.4.2.3 Target attractiveness

In cyberspace, the cybercriminal uses every available opportunity to attack the target, which includes physical and non-physical ways. In the physical world it is items such as cash, jewellery and objects with decent monetary value and easily portable or transferable (Hassan, 2022). In cyberspace, the target can range from confidential information such as passwords, bank balance statements, copyright documents and bank system files. In this situation, the target is more vulnerable since cybercriminals are able to use a wide variety of attack methods to attack the target. Cohen, Kluegel and Land (1981) define target attractiveness as the attractive features of an individual or object to potential offenders.

Cybercrime awareness encounter by staff members

Cybercrime awareness allows individuals and organisations to gauge their readiness to deal with cyber incidents and threats. This is further strengthened by the advice and guidance shared to individuals as an important component in the holistic approach in the cybercrime reduction campaign (Nzeakor, Nwokeoma & Ezeh, 2020). The participants were asked if they have witnessed or encountered a cybercrime activity in their work environment.

Industry Expert 2 responded:

> *"Yes, stealing of information is something I witness occasionally. In one situation, the teller mistakenly copied the IT Manager in an email that was destined for a person outside the bank. The email contained account numbers with the passwords"*

Industry expert 3 concurred by saying:

> *"On the customer side, yes, particularly with card skimming and SIM Swap issues. On the internal side, attempts have been made via phishing attempts"*

As well as Industry Expert 5 who said:

> *"Yes, during my job I would witness a number of cybercrime scenarios. One incident we caught one of the junior officers scanning a signature of a client. Obviously when we asked the lady what she was doing, she panicked and confessed on the spot"*

From the responses above, the participants were further asked about how they responded and actions or interventions that they took in addressing these incidents.

Industry Expert 2 said:

> *"We were able to recover the information and were able to retain as much of the information?.Moving forward I expected the bank to hold a workshop or a meeting so that we discuss the incident. To my surprise, the moment we handed over the information to our superiors, that was the last time we saw that information"*

Industry Expert 3 on the other hand gave a more informed answer by saying:

> *"We conducted customers awareness activities for all our branches, which included staff internal awareness sessions as well as for users. We even took a further step to make sure that we put more emphasizes in the investment of preventive and detective controls"*

A more elaborate response from Industry Expert 5 was:

> *"When I came across an incident, the first thing I would do was record the incident, isolate it. Depending on how sever or serious it was, I would escalate the incident to my supervisor and to the unit. The unit responsible for cybercrime will then evaluate the incident and recover data from the various data restoration points"*

The industry experts' responses conclusively suggest that cybercrime awareness is an important factor. This is in line with sentiments of Aloul (2010), who emphasised that the lack of cybercrime information awareness combined with high-speed Internet connections makes organisations appealing to cybercriminals. In most cases, cybercrime awareness is often overlooked when it comes to information security planning during expansion stages of ICT departments or units (Matengu, 2012).

Cybercrime understanding

The importance of grasping the knowledge about cybercrime provides guidance in addressing cybercrime issues. Information that is gathered on the overall aspect of cybercrime is crucial in order to gain a wide and informed understanding. The participants were asked about their understanding of cybercrime in the context of their organisation business processes.

Industry expert 1 responded by saying:

> *"Our focus is on our core business, therefore I am aware of the impact of cybercrime in our business processes"*

It was also echoed by Industry Expert 3 who said;

> *"My knowledge is minimal in this area, but it is growing at a swift pace because of the changing landscape of cybercrime"*

In agreement, Industry Expert 5 said:

> *"Our internal clients understand cybercrime because as a bank we conduct awareness programs. We also enforce training sessions which are mandatory. For external clients we rely on Eswatini Bankers Association who advocate for safer Internet banking engagement and issues around cybercrime"*

A thorough understanding of the dynamics of cybercrime is crucial in implementing security controls to guide against the target. A cybercriminal in most cases is motivated by the financial gain and therefore it is crucial that cybersecurity experts within the banking sector gain as much knowledge as possible. Understanding of the cybercrime involves a clear indication and classification of the types of cybercrime activities that exist.

The gathering of intelligence reports enforced internal policy control, constant monitoring of online activities and swift response to unfamiliar transactions intensifies the level of understanding of the cybercrime cases (Akinbowale, Klingelhofer & Zerihun, 2022).

> *"Cybercrime loss due to the lack of enforced target security"*

Banks suffer huge amounts of financial loss due to cybercrime. The participants were asked about the most common loss suffered by their organisation due to cybercrime and there was a sense of uncertainty and limited awareness in their responses. For instance, Industry Expert 2 mentions that:

> ” *In our bank we have not yet experienced any cybercrime loss”*

A different response from Industry Expert 3 was:

> *“Computer losses has been through staff members. Since I have joined the bank, I have witnessed these losses”*

While Industry Expert 5 mentions:

> *“For our bank, financial loss has been the most common type of loss experience.”*

Analysing the responses, it is evident that not enough attention is allocated to address the impact of the various types of losses occurring through cybercrime. One of the reasons can be due to the lack of policies and information withholding from top executive in order for them to protect the reputation of the organisation. The routine activity theory views crime from the offender’s view and if the presence of the target is high, combined with a weak guardian, there is a high chance of a crime occurring. This is mainly addressed as target hardening where the suitable targets are ‘hardened’ to discourage cybercriminals by adding more layers of security such as firewalls and multifactor authentication (Clarke, 1995).

Detection tools

Cybercrime detection contributes towards enforcing methods and knowledge to prevent future attempts. It is therefore important to conclude the level of awareness and application of detection methods in organisations. The participants commented about the tools and systems that their organisation used to mitigate cybercrime.

Industry Expert 1 said:

> *“No, we do not have tools and systems that track and even report any cyber incident. This is because our local branch is still under construction for such systems to be included”*

Industry Expert 2 emphasized on the cybersecurity operating center by saying:

> *"Cyber security incidents, yes. We operate a 24-hr cyber security operating center (CSOC) that is hosted in SA. The CSOC liaises and reports suspicious activities that impact Eswatini as and when noticed. The in-country team also runs threshold monitors that report through a tool called Slack.*

While Industry Expert 3 concluded saying:

Further, we operate and monitor dashboards for certain activities from which we learn behaviour of key nodes and systems that are utilised across our environment"

Industry Expert 5 mentioned:

> *"The centralized approach is utilized. Detection of cybercrime activities is based on all end point and network devices"*

The participants' responses to this theme lead to the conclusion that there is sufficient knowledge about the measures in place to address cyberthreats since some of the banks have security operating centres and local teams to address cybercrime detection. The reporting approach from the banks are a good foundation that allows cases to be followed up and addressed. The important issue is to ensure that the detection tools are consistent and readily upgraded. The availability of this technology further enhances the detection of cyberthreats however there is also a need to pay attention to unknown loopholes that are undiscovered that can make a cyberbreach unavoidable (Uddin *et al.,* 2020). Aligning the detection tools with cybersecurity settings to protect the target adds another level of protection.

Table 5.6: Summary of Theme 3 – Cybercrime detection

Theme 3: Cybercrime Detection (c.f. 5.4.3)		
Subtheme 3.1 (c.f. 5.6.3.1) Internal system control	Subtheme 3.2 (c.f. 5.6.3.2) Limited expertise in cybercrime investigation	Subtheme 3.3 (c.f. 5.6.3.3) Audit trail enforcement
Categories		
• Compliance • Intelligence sharing	• Responsibility clarity • Cybercriminal profiling • Cyber-attack vector mapping	• Limited law enforcement engagement

Source: (Author's own)

5.3.4.3 THEME 3 – Cybercrime detection

Cybercrime detection is an important step that determines the level and intensity of addressing cybercrime incidents. Insight is given into the magnitude of the cyber incident, affording the responsible entity dealing with the incident the right information for decision making. Cybercrime detection is made more difficult by the pace of advancement and the strength of modern information technology (Pillay, Ntuli & Ehiane, 2023). Detection is a function or an activity that often shows or discloses the existence of fraud behaviours in a system and its normally detected by tools, techniques and organisationally designed interventions (Deloitte, 2015).

Three subthemes that describe the factors that form part of the detection process emerged in theme 3.

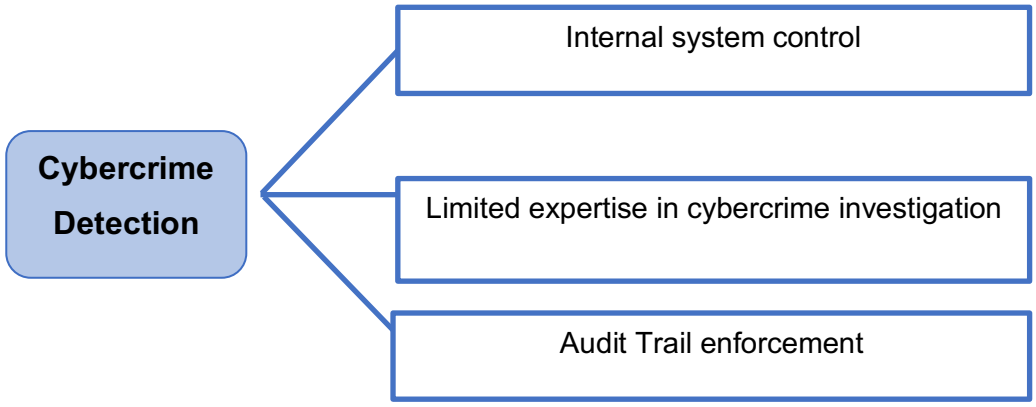


Figure 5.3: Layout of theme 3 with subthemes

5.3.4.3.1 Internal system control

The activity of system control can be controlled either from within an organisation's premises or externally. The deployment of IT systems in both physical and more especially in the virtual (cyberspace) has resulted in a constant system control monitoring. System control trends include virtual servers, online banks, Internet Banking and mobile banking services which are real life examples where system control is entirely virtual. Likewise, internal, external, current, historical, targeted, generic, private and public data is constantly harvested by cybercriminals to gain control of a system (Canelon, Huerta, Leal & Ryan, 2020). Cybercriminals therefore

continue to exploit this area aided by the anonymity factor that is encompassed in cyberspace. Therefore, it is of importance that the internal system control is made up of policies and procedures that are implemented to provide a robust assurance of the safety of company information, assets and compliance to cybersecurity laws (Canelon, Huerta, Leal & Ryan, 2020).

Compliance

Enforcement and adherence to compliance is very important in formulating the most appropriate steps in addressing cybercrime incidents. The majority of cybersecurity frameworks contain solid foundation elements that are guidelines for compliance conformity. An environment where compliance is enforced is normally an ideal model for an organisation to follow and adopt. The participants were questioned about the elements that contribute to a culture of compliance.

Industry Expert 1 mentioned the factors that contribute to a low level of compliance.

> "*Disgruntled employees, lack of awareness, poor IT security infrastructure, bad configuration of our IT systems definitely contributes to cybercrime within the organization"*

Furthermore, Industry Expert 1 also mentioned the engagement of management as part of the compliance phase:

> *"We normally report to the board and within the board there is an IT Steering Committee where the IT Security Officer is a permanent member. The reporting period is quarterly. At the moment there are plans to develop an IT Security Board. In terms of monitoring, we use 3rd party organisations.*

Industry Expert 1's responses highlight the importance of identifying and addressing factors that will hinder the process of meeting compliance requirements.

In support, Industry Expert 3 said:

> *"For cybersecurity, yes.... A cyber security incident will only escalate to a cybercrime level as and when it has been determined to be a criminal activity or when reported from external sources"*

A similar response from Industry Expert 5 focused on monitoring and reporting when he said,

"Yes we do have monitoring and reporting mechanisms, which are also updated together with the local team in the country and the team from the main branch in Johannesburg"

The responses from Industry Expert 3 and Industry Expert 5 shows that there is a need to strengthen the step of escalating a cybercrime incident, especially in the monitoring and reporting stages.

Industry Expert 5 confirmed:

The responses show that there is not enough effort applied to adopt a robust action to fully implement compliance across the organisation. Roohparvar (2022) affirms that compliance provides an additional precaution in cybercrime avoidance, and it also adopts an approach to prevent future cyberthreats. Compliance deliverables are done ad hoc, without following proper guidelines and even adopting a suitable cybersecurity framework. The responses further show that there are activities conducted that address compliance, but however they lack a structured approach of consolidating the compliance processes.

Intelligence sharing

The rate at which cybercrime occurs has a negative impact on the financial institutions. Limited knowledge and the timely sharing of information creates a gap that cybercriminals swiftly use to further exploit the situation. This gap can be addressed through threat intelligence sharing, in order to create a situational awareness platform of sharing information on the latest threats and vulnerabilities amongst stakeholders (Wagner, Mahbub, Palomar & Abdallah, 2019). Akinbowale, Klingelhofer and Zerihun (2022) further encourage the sharing of intelligence reports to address cybercrime threats. Additional intervention in intelligence sharing includes the incorporation of cybercrime awareness findings into a company's cybersecurity plan, guidelines and policies (Matengu, 2012). According to Coker (2021) the private sector, especially cybersecurity companies are a rich resource of cyberthreat intelligence data and information, and they also pave the way in formulating possible solutions.

Industry Expert 3 mentions the importance of conducting awareness activities with private sectors to enable an environment that promotes sharing of intelligence data, when he said;

> *"There are a combination of activities and controls – proactive and reactive. In as far as cyber-crime prevention, mainly proactive controls are deployed that attempt to prevent successful crime execution. These include customer awareness activities that are performed in conjunction with the Eswatini Bankers Association. Some of these controls are inbuilt in products that attempt to make it harder to access customers banking information."*

Industry Expert 5's response was:

> *"We use a layered approach which is dependent on the technology adopted by the bank beginning of each year and we have introduced awareness initiatives, implemented technology that monitors and prevents cybercrime incidents across all our branches. In addition, we often get support from our main branch in Johannesburg through constant meetings, trainings and feedback sessions"*

Furthermore, Industry Expert 5 highlights the support factor which is a crucial element in sharing information.

The responses above show that there is a good approach to sharing intelligence information, but however, there is a need to classify the information for each type of cyber incident case. One of the factors is that information is obtained from various sources, hence a structured process is required to limit information leakage, and information misplacement. Intelligence sharing is produces results that are sustainable over time, consisting of the right context and a dedicated resource plan to support the overall approach (Daniel, 2024). More importantly, intelligence sharing assists in identifying and understanding crucial evidence in the context of the cybercrime case (Arnes, 2020). The overall cybercrime environment needs a unique knowledge approach in receiving information on cybercrime incidents, arresting protocols, investigation, evidence collection and preservation and the understanding of the general law enforcement processes (Nodeland *et al.,* 2019).

5.3.4.3.2 Limited expertise in cybercrime investigation

Cybercrime investigation is a difficult, sensitive and unpredictable process, which is mainly affected by encrypted information, slow adaption to latest investigation tools and the high level of anonymity of the cyberspace. More importantly, it is a complex and critical process that requires collection of data and detailed analysis of information to deliver an outcome to a crime or event. The current trend nowadays is that law enforcements have to investigate cybercrime including traditional crimes (Borges, 2021). This additional work requires investment into equipping personnel with the right tools and techniques on how to deal with cybercrimes. Cybercrime investigation requires a solid combination of utilisation of different techniques and tools for proper navigation at a cyber or digital crime scene (Borges, 2021). Furthermore, the success of cybercrime investigative efforts entails the application of metrics and not the traditional ways normally used in physical crime investigation (Monaghan, 2020).

Lack in expertise

Expertise in any field is very important in order to execute the required activities. In the cybercrime environment, the lack of expertise in addressing cybercrime is major problem. From an angle of a cybercriminal, it increases the chance and possibilities to continue committing more illegal activities. For government, law enforcements, private sector and individuals, it requires a lot of investment in training, qualifications and collaboration. A key issue is the blending of all these activities in a harmonious manner to ensure that cybercrime is prevented and mitigated successfully. Game based training of cybercrime specialists is one approach that allows for real-world simulation of cybercrime (Ebru & Baykan, 2017).

The participants were asked about the impact of cybercrime investigation.

Industry Expert 5 said:

> *"All the years that I have worked in the bank, I am strongly believe that insiders and cybercriminals are the two types of people who are behind the majority of these cybercrime cases"*

The response from Industry Expert 5 shows that there is an interest to engage further into the investigation of the cybercrime case.

Industry Expert 2 said:

> *"We were able to recover the information and were able to retain as much of the information?.Moving forward I expected the bank to hold a workshop or a meeting so that we discuss the incident. To my surprise, the moment we handed over the information to our superiors, that was the last time we saw that information"*

Industry Expert 3 on the other hand gave a more informed answer by saying:

> *"We conducted customers awareness activities for all our branches, which included staff internal awareness sessions as well as for users. We even took a further step to make sure that we put more emphasizes in the investment of preventive and detective controls"*

Responses from industry experts 2 and 3 show that there is an interest to obtain more information of the cybercrime incident. A more elaborate response from Industry Expert 5 highlighted other investigative approaches that were applied

> *"When I came across an incident, the first thing I would do was record the incident, isolate it. Depending on how severe or serious it was, I would escalate the incident to my supervisor and to the unit. The unit responsible for cybercrime will then evaluate the incident and recover data from the various data restoration points"*

Furthermore, Industry Expert 5 mentions more intense involvement;

> *"Yes, during my job I would witness a number of cybercrime scenarios. One incident we caught one of the junior officers scanning a signature of a client. Obviously when we asked the lady what she was doing, she panicked and confessed on the spot"*

The industry experts' responses show that there is a need to upskill, so that the investigation process is incorporated at the first occurrence of the incident to the last step of the investigation process. Cybercrime investigations need to be tackled with all the relevant stakeholders involved, since information received and shared will contribute towards a strong defence case. The information that is collected and shared during cybercrime detection stage goes a long way in solving the cybercrime cases.

There is need for governments to establish efficient mechanisms in private public partnerships to enhance the transfer of skills (Swiatkowska, 2020).

Responsibility clarity

The responsibility aspect in cybercrime is related to the action that is taken by stakeholders when encountering a cybercrime incident. Although Government has the responsibility to protect its citizens from all forms of harm and threats, there is still a need to engage other stakeholders especially the private sector. Adopting a well-researched approach to delegating responsibilities amongst stakeholders improves the effectiveness of dealing with cyberthreats. The goal is creating a network that updates on cyberthreat incidents in a dependable manner. A gap within a set responsibility framework enables the cybercriminals to exploit the situation. In this situation, it often becomes difficult for law enforcement agents and the affected stakeholder to build a case against the cybercriminal. One of challenging tasks faced by stakeholders in the responsibility realm is the depth and scope of engagement when faced with cybercrime incidents. The unpredictability of activities in cyberspace has an impact on the allocation of the different responsibility tasks aligned to the cybercrime incident. The segregation of duties and responsibility should also be taken into account as one of many ways to fight cybercrime.

In support, Industry Expert 3 said:

> *"For cybersecurity, yes.... A cyber security incident will only escalate to a cybercrime level as and when it has been determined to be a criminal activity or when reported from external sources"*

Industry Expert 5 confirmed:

> *"Yes, we do have monitoring and reporting mechanisms, which are also updated together with the local team in the country and the team from the main branch in Johannesburg"*

The findings show that there is need to clearly outline the roles and duties of each stakeholder in dealing with cybercrime issues. The roles are a good starting point to address cybercrime issues because each stakeholder will focus on their mandate.

This makes it easier to allocate each cybercrime incident to the right stakeholder mandate. Furthermore, the roles and duties enable the stakeholder to expand, accommodate and improve on aspects that address cybercrime. Arief & Adzmi (2015) emphasise that the best way to combat cybercrime is to gather and understand all cyberthreat information and share it with the stakeholders.

Cybercriminal profiling

Cybercriminal profiling focuses on assisting organisations and cybersecurity experts in understanding and consolidating the cybercriminal behaviours and characteristics. It is a strategic process that is jointly and cooperatively conducted by law enforcement agencies (Doktor, 2023). Cybercriminal profiling is a technique used by forensic investigators or law enforcements to obtain and analyse the behavioral, personality traits and overall criminal pattern behaviour that occurs in cyberspace (Lickiewicz, 2011). The goal is to understand the behaviour of the cybercriminal, and the anonymity element of cyberspace makes it difficult for cybercrime investigators to gather a full and comprehensive cybercrime incident information. The gathering and consolidating of the profile of a cybercriminal plays an important role in an organisation's ability to tighten security measures, contextualise cyber awareness trainings and strengthen mitigation strategies.

Industry expert 2 explained by saying:

> *"Ever since I joined the IT environment, I strongly believe that most of this fraud cases are a result of external people*"

However, a different response from Industry Expert 3 was:

> *"We have not had evidence of those types of activities in recent years (at least after I joined) the bank"*

Industry Expert 5 said:

> *"All the years that I have worked in the bank, I am strongly believe that insiders and cybercriminals are the two types of people who are behind the majority of these cybercrime cases*

The findings show that the participants have the basic profiling understanding. However, there is a need for aggressive intervention towards strengthening the cybercriminal profiling process, especially in the early stages of the awareness of the cybercrime incident. Kipane (2019) mentions three stages of criminal profiling, stage one involves collection of data, stage two involves analysis of the data and stage three is the prediction of the cybercriminal behaviour and traits. The response from the participants highlighted that only the first stage is achieved, while the other two stages are not within their duties. It is imperative therefore, that financial institutions implement all three stages in order to have enough information that will be useful in dealing with future cybercrime incidents.

Cyberattack vector mapping

An attack vector is used by cybercriminals to gain unlawful access to computer systems. Tunggal (2023) lists email attachments, pop-ups, text messages, viruses and social engineering as the most common attack vectors used by cybercriminals. Cybercriminals are constantly scanning for points of weak entry in systems and any misalignment that is discovered, they take full advantage. With this approach, the scanning process is even more effective because cybercriminals exploit a wide area of entry points, further increasing the chances of success. Investigators therefore need to combine historical data, shared threat intelligence information and cyber threat mapping information to address each cybercrime incident categorically and contextually.

Industry Expert 2 responded:

> *"Yes, stealing of information is something I witness occasionally. In one situation, the teller mistakenly copied the IT Manager in an email that was destined for a person outside the bank. The email contained account numbers with the passwords"*

When comparing the utilisation of the various attack vectors to the conviction of cybercriminals, Industry Expert 5 highlighted;

> "*Cybercrime convictions are low. There have been many incidents where I would submit reports on cybercrime for all the branches to management, hoping that*

the criminals would be caught. But later in the following weeks when I make a follow up, I would be told that nothing has been done."

This response further shows that low cybercrime convictions have a direct impact on repeated attack vector attempts. Further confirmation is evident that attack vectors offer a huge benefit for cybercriminals to gain unauthorised access to unsuspecting victims. Cybercriminals are constantly probing for weak points in systems and once the opportunity avails itself, there is no hesitation in exploiting that vector point. Lenaerts-Bergmans (2023) therefore emphasises that focusing more attention and resources in recognising and tracking a cybercriminal's vectors can assist organisations to better defend existing or forthcoming cyberattacks.

5.3.4.3.3 Audit trail enforcement

An audit trail is very important in detecting cybercrime incident, by allowing system administrators and cybercrime investigators to identify the causes and potential cybercrime breaches. The detailed record of all the access information in a system is an important factor in cybercrime detection. After all, the overall goal of an audit trail is to highlight and follow the steps of how an incident occurred, and the enforcement part is to identify the responsible entity. Organisations can take advantage of existing audit programmes to consolidate and compare findings that can enhance prevention and mitigation cybercrime. The greatest benefit of an audit trail when implemented properly is that the data captured cannot be modified or deleted (Imprivata, 2019).

Limited law enforcement engagement

Law enforcement agencies rely on reported information to carry out their mandate. A gap that exists in submission of information tends to limit the chances of addressing and solving cybercrime incidents. A resultant outcome to this is the further exploitation by cybercriminals and a tendency of law enforcement not being able to maintain the pace of solving the issues. Cybercrime threats are constantly evolving, and this has become a major problem for law enforcements, due to the slow approach in updating on current trends. The issue of engagement is a problem because there is no defined engagement between law enforcement and other stakeholders. Law enforcement agencies need to shift from policing strategy to focusing on dealing with computer-related incidents (Hull *et al.,* 2018). Success in dealing with cybercrime requires a high level of engagement, because cybercrime occurs at a rapid rate and across multiple

spaces in cyberspace. This becomes difficult for law enforcements to address the huge influx of cyber incidents. Therefore, cybercriminals continue to engage in illegal activities as a result of a lack of global cooperation among law enforcements (Broadhurst, 2006).

Industry Expert 1 said:

> *"No, we do not have tools and systems that track and even report any cyber incident. This is because our local branch is still under construction for such systems to be included"*

Similar and more defined responses from Industry Expert 2 and 3 were as follows;

Industry expert 2 said

> "*Cyber security incidents, yes. We operate a 24-hr cyber security operating center (CSOC) that is hosted in SA. The CSOC liaises and reports suspicious activities that impact Eswatini as and when noticed. The in-country team also runs threshold monitors that report through a tool called Slack"*

Industry Expert 3 said,

> "*Further, we operate and monitor dashboards for certain activities from which we learn behaviour of key nodes and systems that are utilised across our environment"*

The responses underline the level of awareness and initiatives taken to implement audit trail activities. There is also a positive step whereby an independent third party is incorporated into the whole audit process in capturing the cyber incident issues. In order to strengthen the credibility of the audit trail process, financial institutions need to enforce the concept of separation of duties. Duncan & Whittington (2016) state that this approach reduces the opportunity for fraud, and minimises data or information concealment.

Table 5.7: Summary of Theme 4 – Cybercrime compliance

Theme 4: Cybercrime Compliance (c.f. 5.6.4)
Subtheme 4.1 (c.f. 5.6.4.1) Change Management
Categories
• Cybersecurity culture • Coordinated sharing culture

Source: Author's own

5.3.4.4 THEME 4 - Cybercrime compliance

The purpose of compliance is to identify and contain risks that are part of the business processes. In the cybercrime domain, the adoption and enforcement of compliance assists organisations in preventing and detecting cybercrime incidents. It is even a bigger problem when compliance is compromised through cybercrime incidents. This is more serious because cybercrime occurs in cyberspace, where cybercriminals are constantly conducting crime anonymously while using innovative methods. The costs of fighting cybercrime can be greatly reduced if financial institutions invest in compliance interventions. Maluvu (2023) emphasises that financial institutions in Africa should make efforts to reduce compliance costs. The SWIFT network is one organization that securely transmits financial information between financial institutions through a unique code (Seth, 2023).

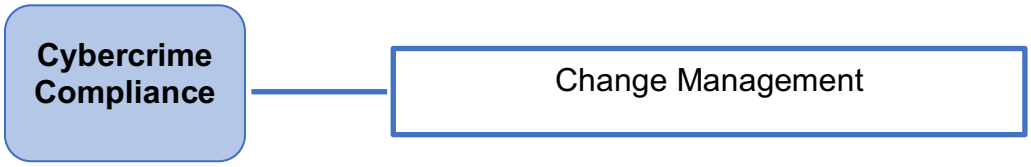


Figure 5.4: Layout of theme 4 with subthemes

5.3.4.4.1 Change Management

Change management is a process that an organisation follows in preparing, implementing and driving change within itself. It plays a crucial role in the planning, implementation and solidifying the cybercrime changes within an organisation. Encouraging employees to comply with organisational security policies, guidelines and procedures is a major challenge (D'Arcy & Greene, 2014). Kortan & von Solms (2012) therefore mention that the main objective of change management is to ensure proper alignment of employees and the organisational culture to cybersecurity best practices, with the overall aim of maintaining, mitigating and supporting the proposed change. In the context of cybercrime, change management ensures that the implementation of cybercrime initiatives is successfully managed. One of the benefits that change management provides for an organisation is the ability to adjust and keep pace with constantly evolving cybercrime threats and incidents.

Cybersecurity Culture

The approach and behaviour that top management displays across an organisation and supported by policies and guidelines are essential elements for a resilient cybersecurity culture. The European Union Agency for Network and Information Security (2017) includes beliefs, attitudes, values, perceptions and knowledge that people possess towards implementing and maintaining the desired cybersecurity culture. The participants were asked about the importance and impact of a cybersecurity culture.

Industry Expert 5 said;

> *"Management fully supports cyber security activities by investing in tools and people in order to mitigate the risks. Our management knows that cybercrime is highly likely to occur and the threat landscape is always evolving"*

Industry Expert 1 and 2 mention the cybersecurity strategy as an important approach that contributes to the formation and enhancement of a cybersecurity culture.

Industry Expert 1 commented that:

> *"The Chief Technology Officer has been given this task and also to coordinate with the other departments. Since we are a new bank I am still learning the business approach of communication, however I must say I have observed that my supervisor is engaging me."*

In support, Industry Expert 2 said:

> *"This responsibility solely lies with the Chief Information Officer who then also makes sure that the strategy is cascaded to all departments and branches in the bank. We do meet at schedule meetings to update one another the progress that we have made*

The responses above show that management support is important for the creation of a workable cybersecurity culture. There is a need to instill the message of an employee's role in protecting an organisation's information assets at all levels of engagement in the workplace. The right tools, human resources and understanding of the environment are factors required. Gelnaw (2018) emphasises that focusing more on training employees to be cautious and observant while utilising technology enhances a robust cybersecurity awareness culture.

This type of training approach, combined with empowering employees to raise or report cybercrime incidents, enhances the cyber security awareness culture. As a result, the cybersecurity culture maintains a robust standard that is able to withstand potential cyber threats.

Coordinated sharing culture

Cooperation is the activity where a group of people work together to accomplish a certain goal or task. It forms part of coordination which focuses on the utilizing different elements or skills to achieve a set goal or objective. Cybercriminals collaborate at a level that focuses on the set goal and since cybercrime incidents are constantly happing at a very high pace, it often leads to investigators struggling to reduce the gap.

The importance of sharing information and knowledge is important in this regard, if it is conducted in a structured manner. A coordinated sharing culture encourages employees to exchange information and expertise. There are many methods through which such information can be gathered and shared in order for cybercrime incidents to be mitigated and resolved.

The sharing approach will greatly assist cybercrime handlers within the organisation to gain more confidence in dealing with cybercrime related incidents. One of the most efficient ways of strengthening security against cybercrime is through sharing of best practices and lessons learned (Vez, 2017). Threat intelligence information can also be easily shared among security teams and cybersecurity group communities (Blog, 2023).

The Society for Worldwide Interbank Financial Telecommunications (SWIFT) has demonstrated this through the launch of their Information Sharing and Analysis Centre that focuses on facilitating access to cyber security threat intelligence within their network (SWIFT, 2023).

Industry Expert 3 mentions that:

> *“We conducted customers awareness activities for all our branches, which included staff internal awareness sessions as well as for users. We even took a further step to make sure that we put more emphasizes in the investment of preventive and detective controls”*

"Our internal clients understand cybercrime because as a bank we conduct awareness programs. We also enforce training sessions which are mandatory. For external clients we rely on Eswatini Bankers Association who advocate for safer Internet banking engagement and issues around cybercrime"

The response highlights that there are initiatives and approaches in place to fully realise the desired outcomes. The involvement of external stakeholders enforces the sharing platform as well. The World Economic Forum (2016) recommends that private and public sectors should work together to share cybercrime related information. Klenka (2021) mentions that there is a global cyberwar and to combat it, all stakeholders must be active, vigilant and properly implement strong and effective cyber security laws.

Furthermore, solving cybercrime needs all available stakeholders to work together, due to the innovative speed that cybercriminals use to try different attack methods. This approach is a good base in creating a coordinated sharing culture. Likewise, the different aspects of African culture need to be contextualised to enhance information sharing behaviours (C3SA, 2022). Moreover, the sharing of cyber threat intelligence information has expanded from organisation to organization level, to a country-to-country level (Coker, 2021).

5.4 Summary of findings

This chapter analysed the data and discussed the study findings. The interviews were analysed using thematic analysis techniques, and four predetermined themes emerged from the research data. Data was collected from five (5) participants using interviews. The major findings of the study were summarized below.

There is currently no cybercrime framework in Eswatini banks that addresses cybercrime. The framework must focus on cybercrime awareness, prevention, detection and compliance. To ensure a thorough understanding of a cybercrime incident or threat, awareness is the starting point towards gaining proper recognition, understanding and situational impact of the incident.

A majority of the responses from the industry experts demonstrate that cybercrime is aggressively progressing and in the context of Eswatini Banks, the existence of preventive and detection controls together with programs, policies and control measures need more reinforcement to prevent cybercriminal activities.

All the participants agree that the more emphasis must be placed in strengthening cybercrime awareness for internal and external customers. Furthermore, it is evident that the banks must have documents which include the cybercrime strategy and various IT policies that support the addressing and dealing with cybercrime issues.

In terms of cybercrime prevention, the industry experts noted the importance of aligning qualifications to the job descriptions. The issue of change management is another important element that the industry experts mentioned, in relation to compliance.

The next chapter interprets the study findings and subsequently provides the cybercrime framework

CHAPTER SIX

INTERPRETATION OF RESULTS AND FRAMEWORK

6.1 Introduction

The interpretation explains how the findings relate to the study's research objectives and the participants' questions. The study utilized the Routine Activity Theory, Space Transition Theory and Deterrence Theory as lenses and this chapter interprets and links the findings with the literature from research in the preceding chapters. This chapter provides a narrative of the case, the interpretation and theme emergence underpinned by the routine activity, deterrence and space transition theories. The interpretation of the results will be followed by the recommendations which include the proposed cybercrime framework for financial institutions.

The findings were obtained through interviews from five (5) industry experts through a qualitative study. The interpretation of the study findings is based on thematic analysis from interviews. The findings were interpreted according to the study objectives, which are synonymous with the study themes.

6.2 The primary aim

This study aimed to conceptualise a cybercrime framework for Eswatini

6.3 Study Objectives

- To analyse the effectiveness of Space Transition in the combatting of cybercrime activities in the banking sector.
- To appraise the effectiveness of Routine activity in the combatting of cybercrime activities in the banking sector
- To assess how deterrence theory of a financial institution can combat cybercrime.
- To determine how banks in Eswatini can minimise cybercrime activities in order to preserve their business.

6.4 Interpretation of the study findings

This section outlines the interpretation of the findings obtained from the thematic analysis of the data collected through interviews.

6.4.1 Objective 1: To analyse the effectiveness of Space Transition in the combatting of cybercrime activities in the banking sector (Synonymous to Theme 1: Competence in cybercrime awareness)

This objective is synonymous with theme 1, which addresses the effectiveness of the space transition theory in combatting cybercrime activities in the banking sector. The findings which are categorised into two sections, show that there is insufficient experience in addressing cybercrime in the banking sector and also, there is a need to enforce and strengthen cybercrime conviction rates.

Insufficient experience in cybercrime prevention and mitigation

The importance of cybercrime prevention and the level of experience in addressing cybercrime incidents was highlighted by the participants. It was also deduced from the findings that knowledge of cybercrime attacks is important in finding ways to apply mitigation strategies. Therefore, is it critical that cybercrime interventions should contain a wide pool of experienced staff, with relevant qualifications and work experience to enforce awareness and vigilance in preventing cybercrime activities. In addition, by aligning to the space transition theory which highlights that persons that repress criminal behaviour in the physical space have a propensity to commit crime in cyberspace, it is important for the designated staff who deal with cybercrime to gather all the information in order to prevent and mitigate cybercrime.

Literature states that most cybercrime activities are a shift in operations from physical space to cyberspace, therefore without the proper knowledge and experience, it becomes difficult for the cybercrime guardians to predict, assess and analyse the cybercrime incident. The categories that emerged from the subthemes are banking services, vulnerability to cybercrime, qualifications, guidelines and cybercrime conviction rates.

Banking services

The major issue is that the availability of the various banking services, and the interlinking functionalities provide a wide opportunity for cybercriminals to conduct criminal activities. It is paramount that banking institutions should strengthen their cybercrime awareness knowledge especially in the expansive nature of cyberspace where the anonymity element is exploited by cybercriminals to their advantage.

Vulnerability to cybercrime

The findings highlight the need for an adoption of a more proactive approach in protecting the financial assets that are highly targeted by cybercriminals. Part of the reason is that the internet has made it easy for cybercriminals to exploit the targets and also conceal their online identity. Another factor is the different and unequal access that exists in cyberspace, which makes it difficult to apply a standard technique of protection. The situation is worse in cyberspace because it is difficult to detect a cybercriminal's physical attributes such as height, movement and body shape and aligning it to the offence. This vulnerability can be addressed by focusing on each financial asset threat then move towards enforcing the applicable mitigation step.

Qualifications

The majority of the industry experts mentioned that acquiring a qualification that is aligned to the respective job position increases and improves the chances to mitigate cybercrime activities. Moreover, qualifications that are aligned to cybercriminal behaviour are more applicable.

Guidelines

The findings indicate that guidelines are implemented as part of the business process to drive the overall cybercrime awareness and prevention initiatives. Local banking institutions should concentrate on creating and improving the guidelines in order to keep abreast with the cybercrime related issues in cyberspace. Literature argues that guidelines should be a framework that enables an organisation to use technology to identify and exploit opportunities that are typically targeted by cybercriminals (Ben Romdhane Ladib & Lakhal, 2015).

Cybercrime conviction rates

Although cybercrime is rapidly on the increase, there is still a low reporting culture from the victims, and the determinants of cybercrime reporting differ between traditional crime and cybercrime (van de Weijer, Leukfeldt & Bernasco, 2019). The Royal Fraud unit in the Royal Eswatini Police Service is responsible for investigating, recording cybercrime cases and identifying the perpetrators. However, like other law enforcement forces across the world, the Royal Eswatini Police Service continues to face difficulties in conducting investigations, collecting electronic evidence and prosecuting cybercrimes. Peters & Jordan (2020) affirm that law enforcement agencies face challenges in attributing and bringing justice to cybercriminals due to the transnational nature of cybercrime.

The study findings revealed that there is generally low conviction rate for cybercriminals including the approaches utilised to convict the perpetrators. This is even emphasised by the industry experts;

> *"At our bank we have not arrested nor taken any measures to fully address cybercrime issues when it comes to arresting the cybercriminals. Normally we will hand over all the information we have about the incident. What makes the whole situation painful is that we have to wait for the police to update us about the case*" – Industry Expert 2

> *"Internally – We have not had evidence of those types of activities in recent years (at least after I joined) Externally there have not been any that I know of*" – Industry Expert 3

These findings are further supported by literature where Mutune (2023) emphasises that unreported cybercrimes contribute to a lower prosecution and conviction rate. In this context, low levels of cybercrime conviction contribute to an increase in cybercrime attacks, as a result of identity flexibility, dissociative anonymity, casual online association and general lack of deterrence (Karuppannan & Chandra, 2017). These elements are major factors in attracting traditional criminals into cyberspace.

6.4.2 Objective 2: To evaluate the effectiveness of Routine activity in the combatting of cybercrime activities in the banking sector (Synonymous with Theme 2)

The second objective attempts to gauge the effectiveness of the routine activity theory in combatting cybercrime activities in the banking sector.

Internal threat control

The findings established that the majority of the financial institutions understand and address the allocation of responsibility to the right departments, units and people. However, there is still a huge gap in addressing internal cyberthreats compared to external cyberthreats. The participants are of the opinion that internal threats and lack of policy enforcement are the major contributors to the cybercrime phenomenon. Financial sectors suffer the most due to internal threats as a result of the highly sensitive information that is valuable to cybercriminals. Cappelli, Moore and Trzeciak (2012) affirm that the banking sector has the most cases that are related to fraud which is often carried out by malicious insiders. The low level of awareness and user education interventions particularly on internal threats further contribute to the rise of cybercriminal activities. The study findings further show that mitigation of internal threat control is influenced by responsibilities and experience of the personnel assigned to deal with cybercrime.

Responsibilities

The routine activity theory argues that crime occurs when the motivated offender is able to exploit the vulnerability of a target and in the absence of a capable guardian (Cohen & Felson, 1979). The findings show that the management does provide support through dedicated units with properly assigned roles for the industry experts to focus on cybercrime issues. These interventions are important because from a criminological approach, the offender's profile is not easily known in a cyberspace environment (Sinca, 2015).

Experience

The findings conclude that the range of work experience in the cybercrime space is over 10 years. It is important that financial institutions hire, develop and continuously improve the skills of the assigned cyber industry experts.

Insufficient cybercriminal threat knowledge

Cyberspace is a transit place, where offenders have taken advantage, by allowing them to visit and exit like any other place, virtually. This further allows cybercriminals to migrate from one location to another, masking their online location through proxy servers, eventually making the cyberspace an ideal place for them to commit cyberspace and disappear thereafter (Jaishankar, 2008). This is synonymous with the respondents' comments:

> *"Ever since I joined the IT environment, I strongly believe that most of this fraud cases are a result of external people*" – Industry Expert 2

> *"We have not had evidence of those types of activities in recent years (at least after I joined)"* – Industry expert 3

Information about cybercriminal threats from the angle of the routine activity theory elements, motivated offender, suitable target and lack of guardianship enables the cybercrime practitioner to mitigate the threats with greater impact and a more robust approach. The gathering of cybercriminal threat information is important, although the anonymity and secrecy opportunities existing in cyberspace, often taken advantage of by cybercriminals is a tough hurdle to overcome. The categories that emerged from the theme are: cybercrime management approach, monitoring and reporting, organisation size and management support, cybercrime methods, management's cybercrime perception and cybercriminal participants.

Cybercrime management approach

The issue of approach in dealing with cybercrime issues was found to be a challenge. The findings confirm that the industry experts applied the approaches in an inconsistent manner. Although the chosen approach lacks a justified reason of implementation, it was however noted that it was dependent on the type and severity of the cybercrime incident. It is important to note that any chosen approach should be well researched for applicability and alignment to the cybercrime incident or threat. The approach should be able to address the cybercrime elements of the routine activity theory.

Monitoring and Reporting

Monitoring and reporting are important stages in addressing cybercrime prevention issues. The purpose of monitoring is to ensure that planned activities and deliverables are observed for any changes, and if there is a need, implemented accordingly. The findings confirm that there is a high-level standard in the monitoring and reporting process of cybercrime issues in the financial institutions. The financial institutions apply a wide range of methods and communication paths to the relevant bodies that are tasked to address cybercrime issues.

An organisation that complies with monitoring and reporting, promotes and enhances a strong cyber awareness and prevention work culture. Erin, Kolawole & Noah (2020) emphasise that a stronger management oversight and a more transparency risk approach will go a long way to minimize the threat of cybercrime Moreover, monitoring and reporting should be supported by properly updated technological systems (Yesmen & Ahmed, 2022). In this context, cybercrime issues can be mitigated more efficiently.

Organisation size and management support

The size of an organisation has an impact on how cybercrime is addressed. The assumption is that a smaller organisation has a compact approach to address cybercrime due to the small number of employees where information is easily shared. However, the vulnerability for smaller organisations is higher because cybercriminals take advantage of the limited resources and lack of advanced cybersecurity measures (Forbes, 2023).

The findings show that it is important to share and consolidate information for consistency purposes and it should involve an organisation's management. Beaumier & Reese (2023) emphasises that greater alignment of an organisation's risk framework will provide senior management with an oversight of the wider support horizon.

Cybercrime methods

Findings show that phishing and social engineering methods are the most common methods used by cyber-criminals due to their flexibility and ease of modification for each cybercrime activity. Lastdrager (2014) affirms that phishing is the most common method used to entice bank and card account valuable information from unsuspecting targets.

Management's cybercrime perception

The findings show that the management in the financial institutions are aware of the cybercrime impact, however, there is a lack of urgency in interventions implemented to bridge the gap. In addition, there is concern in the inconsistency of gathering and sharing cybercrime related information that will strengthen and improve the cybersecurity culture. To address this weakness at management level, a dedicated cybercrime unit can address the impact of prevention, detection, investigation and prosecution of cybercrime for the benefit of citizens and the institution (INTERPOL, 2023). Jonker (2015) affirms that an important component in combatting cybersecurity threats is through the development of a cybersecurity culture.

Cybercriminal participants (Internal vs External)

Cybercriminal participants can either be insider threats or outsider threats, and they equally possess a high level of difficulty in detection and mitigation. Findings support that there is a lack of knowledge from the participants in distinguishing whether a cybercrime incident is orchestrated by an external or internal offender. Although organisations implement sophisticated technology to monitor employees, it is not always easy to distinguish between an insider and an outside attacker (Ja, 2015). Additionally, the findings also highlight that the industry experts do not have the proper approach to consolidate information that will assist in handling the incidents. In order to strengthen this approach, organisations often adopt a secrets management strategy that securely manages and monitors sensitive information (Alvas, 2023). Moreover, implementing a training program that ensures that employees are not only informed about threats, but also be able to recognize and deal with those threats and vulnerabilities in the environment of the organization (Bada & Sasse, 2014).

Target attractiveness

The findings show that the more value a target has, the more chances that the offender will take towards obtaining it. The gain is one that motivates the cybercriminal and is visible, accessible and susceptible to be misappropriated (Felson & Clarke, 1998). Target attractiveness consists of two dimensions, where the victim's routine activities make them conceivable targets and also, the attributes that the victims possess contribute to the attractiveness (Cohen, Kluegel & Land (1981).

Cybercrime awareness encounter by staff members

A level of awareness of any cybercrime incident is an important factor to increase the cybersecurity knowledge base. Findings show that the industry experts lack the ability and necessary methods to share the experience, which should be part of the overall planning sessions of the organisation for cybercrime prevention interventions. Converting the cybercrime awareness into meaningful and achievable goals increases confidence amongst the staff as well as enhancement of the cybersecurity culture.

A majority of the industry experts believed that there is not enough cooperation between the departments or units in the bank with the staff responsible for cybercrime issues. This gap will affect the way cybercrime issues are prevented and detected due to the concealing practice of the superiors. However, in other banks, the cooperation was deemed to be very effective, in conjunction with the application of policies, guidelines and a sharing culture. There should be forums, engagement sessions where cybercrime incidents are discussed with the relevant stakeholders. Moreover, there is need for the financial institution to embrace all forms of communication towards increasing awareness of cybercrime. Matengu (2012) further affirms that organisations should not overlook the impact of cybercrime awareness contributions from staff members, since such information is important for inclusion in cybersecurity plans, policies and guidelines improvement.

Cybercrime understanding

The findings show that the industry experts have a good understanding of the cybercrime impact from the business process perspective. Furthermore, the findings show that the industry experts are well aware of the reporting channels to use when sharing the information. Limited understanding and awareness of cybercrime results in a lack of planning and development of policy framework to safeguard critical information assets (Crisanto & Prenio, 2017). According to Akinbowale, Klingelhofer and Zerihun (2022), intelligence reports, enforced internal policy control, continuous monitoring of online activities and swift responses to unfamiliar business transactions intensifies the level of understanding of cybercrime cases.

Cybercrime loss due to the lack of enforced target security

The link between cybercrime loss and the affected target is a very important piece of information that financial institutions can utilise for informed decision making. The findings demonstrate that the industry experts have limited information regarding the impact of cybercrime loss in relation to the target security settings. Banking institutions need to strengthen the information sharing aspect combined with policy reviewing to strengthen this link. Increasing the target security will generally reduce the perceived cybercrime loss from cybercrime threats.

Detection tools

The findings of the study highlight a level of compliance and implementation of detection tools in the banking institutions. Also, the industry experts expressed a positive approach regarding the usage of detection tools in monitoring and counteracting cybercrime incidents. Moreover, Uddin *et al.,* (2020) further supports the availability of this technology by stating that it increases the detection of cyberthreats.

6.4.3 Objective 3: To assess how deterrence theory of a financial institution can combat cybercrime (Synonymous with Theme 2 and 4)

The third objective was to assess how the deterrence theory can combat cybercrime. The main objective of deterrence is about convincing a potential criminal that the planned criminal activity is not worth pursuing for potential gain. The findings show that a thorough understanding of the dynamics of cybercrimes is crucial in implementing security controls to guard against the target and intercept the offender.

The deterrence theory is based on discouraging likely criminals from engaging in criminal activities by implementing methods that will create fear towards the intended activity. Literature supports that in order for deterrence to be effective, prospective attackers need to be sufficiently concerned that their identity would be revealed and that they would be the target of retaliation (Hsiang Wei, 2015). Furthermore, punishment for cybercrime should be conducted in a transparent manner in order to achieve the desire deterrent effect on cybercriminals (Tan, 2018).

A financial institution should take into consideration all the options available to catch a cybercriminal, and therefore anticipate the likelihood of the capture. This can be consolidated with the speed and severity of the punishment. The outcome of these actions will have a great impact on cybercriminals from committing a crime. Furthermore, cybercriminals tend to be concerned about their online identity exposure, which contributes positively to the deterring effect (Hsiang Wei, 2015).

The importance of understanding cybercrime activities especially the financial attractiveness or value of the target, the approaches used by the offenders and the defensive methods used by the financial institutions contribute immensely towards limiting cybercrime threats. This type of approach, combined with knowledge sharing, increases the cybersecurity knowledge for all stakeholders in the cybercrime prevention space. To further support deterrence, the issue of compliance adds more value to cybercrime prevention due to the collective efforts in sharing information with all stakeholders.

6.4.4 Objective 4: To determine how banks in developing countries can minimize cybercrime activities in order to preserve their business (Synonymous with Theme 1, 2 and 3)

This objective was to determine how banks in developing countries can minimise cybercrime activities within the organisation. According to the findings, the industry experts have a good knowledge base of the different methods, tactics and approaches that they currently implement for cybercrime awareness and prevention. The findings further show that banks should focus on gathering and documenting cybercrime incidents and threats, strengthen internal threat incidences, reduce and limit the target attractiveness with the bank.

The overall aim is to reduce the complexity of cybercrime attack as well as increase the cybercrime conviction rates. In addition, literature states that banks can further apply measures such as a good understanding of cyber resilience, adoption of an approach that is comprehensive and adaptive, placing of competent people and controls and swift cyber-threat information sharing culture (Boer & Vazquez, 2017).

Regarding external factors that also address the minimisation of cybercrime, such as laws and legislation – both within the country and internationally, the findings emphasise the

importance of adopting and contributing towards the development and amendment of cybersecurity and cybercrime protocols mandated to fight cybercrime. Literature further shows that there is a need to speed up the development and have swift response to cybercrime legislation in order to avoid the ineffective application of cybercrime prevention efforts committed in cyberspace (Kshetri, 2010).

Internal factors should focus on system control, as the first point of contact normally targeted by cybercriminals. Organisations should focus more on enforcing audit trails and gathering of information during cybercrime investigations.

In deterring a cybercriminal from committing a crime, emphasis must be enforced on the severity of punishment, the public awareness messages about the consequences of the crime committed and swiftness in implementing the punishment. Furthermore, punishment should be handled in a transparent manner in order to achieve the desired deterrent effect (Tan, 2018).

6.5 Conceptual Framework

The overall purpose of this study is to foster a cybercrime framework for Eswatini banks. The analysis, interpretation and discussion of the data collected assisted in answering the research questions. The interpretation therefore resulted in the development of a conceptual framework, made up of the themes and subthemes, that will address the cybercrime phenomenon in Eswatini banks.

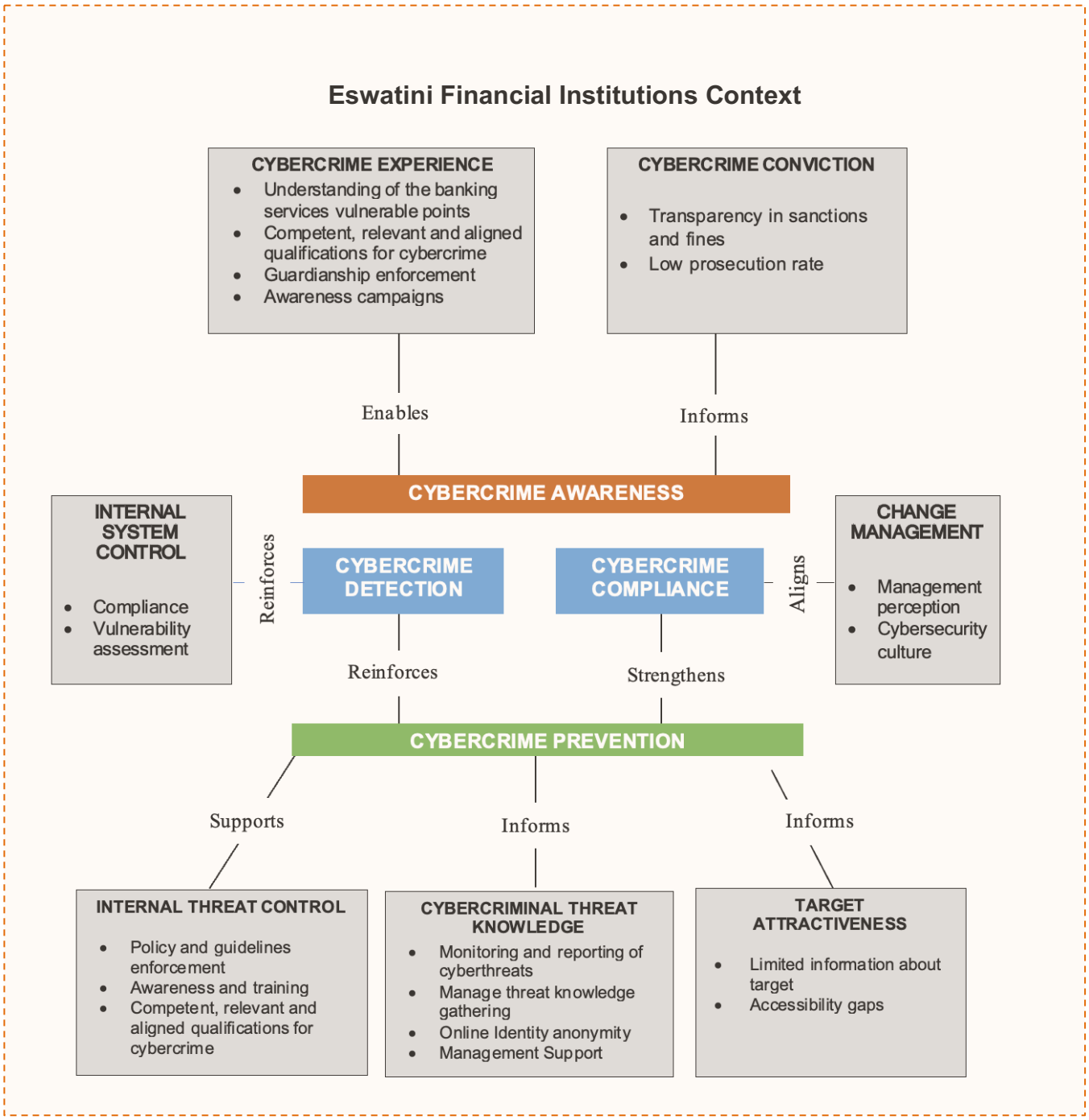


Figure 6.1: A cybercrime conceptual framework for Eswatini banks

The limited knowledge of the offenders, both internal and external are a major contributor for cybercriminal activities to occur. Banks in Eswatini should invest in time and efforts towards implementing context-based intelligence interventions and gather and learn as much as possible about the characteristics of internal and external threats. This will deter the cybercriminals. Elements of the space transition theory and Deterrence theory address the routine activity tenets with the intention to reduce the likelihood of a cybercrime activity to occur.

Table 6.1: Elements of the conceptualised framework

Factors	Elements
Cybercrime Experience	Enables the financial institutions to gain an understanding of the reasons that cause cybercrime to occur.
Cybercrime Conviction	The approach enforced to punish the cybercriminal for the offence committed. It includes fines, sanctions and jail sentences
Internal Threat Control	The approach used to limit and prevent an internal person from exploiting a system with the aim to cause damage. Preventative methods include policy and guidelines enforcement, awareness trainings, competent and aligned qualifications
Cybercriminal threat knowledge	The knowledge that allows a cybersecurity practitioner to apply techniques in order to prevent or mitigate cyberthreats by examining the gathered data.
Target attractiveness	The attributes and perceived value that motivates a cybercriminal.
Internal System Control	The interventions that enable the awareness and understanding of how to mitigate cybercrime
Change Management	The processes followed to implement, control and assist people and an organisation to adapt to change

6.5.1 The framework as recommendations

The factors and elements of the framework are further discussed as recommendations towards addressing cybercrime in Eswatini financial institutions:

(a) Cybercrime experience

Experience in addressing cybercrime is crucial for financial institutions in order to address cyberthreats and incidents. Lack of knowledge will greatly affect the overall cybersecurity framework of the financial institutions due to the limited cybercrime experience. Evidence

shows that financial institutions should vigorously and continuously improve the skills of the assigned cyber industry experts. Cyberattack prevention methods are good defence strategies in preventing cyberthreats such as phishing, and card cloning. In Eswatini banks, this is the major factor that has led to cybercriminal activities.

(b) Cybercrime conviction

Conviction is all about ensuring that an offender is punished for the crime committed. One of the issues that contribute to the high cybercrime incidents is the low conviction rates. The findings have shown a low cybercrime conviction rate, and the cause is the lack of evidence and the complexity of the cybercrime activity. The insufficient or lack of evidence gives cybercriminals an advantage to continue in engaging in criminal activities due to this gap. Although the industry experts complied with the cybercrime investigation principles, the findings point to the final prosecution step as the major weakness, where there is lack of transparency in terms of reporting and the inability to prosecute the criminals. Literature highlights that the law enforcements lack the legal permission to arrest the individual (Mutune, 2023).

To counteract this gap, law enforcement organisations should ensure that punishment for cybercrime should be conducted in a transparent manner to deter cybercriminals. Therefore, the study recommends that financial institutions need to form a greater enforcement capacity with regional and international cybercrime organisations, advocate for a higher severity of punishment and capacitate assigned cyber staff in collecting, preservation and presentation of cybercrime evidence.

(c) Internal Threat Control

Internal threat control is regarded as the steps taken to reduce the risk posed by internal staff in engaging in criminal activities targeted at an organisation's assets. Insider threats have destructive effects in an organisation's operations, reputation and financial portfolio. Therefore, it is important that financial institutions adopt and apply the most stringent measures to limit this risk. The findings established that the majority of the financial institutions understand and address the allocation of responsibility to the right departments, units and people to control and maintain internal threats. Furthermore, the mitigation of internal threat control is influenced by responsibilities and experience of the personnel assigned to deal with cybercrime. However, there is still a huge gap in addressing internal cyberthreats compared to external cyberthreats. The study

recommends that financial institutions should strengthen user awareness training for both internal staff and customers. These trainings can include virtual training sessions, consultations and audits which will bridge the gap in understanding the characteristics of the cybercriminals, and both external and internal threats. Furthermore, these user awareness programmes need to be contextually designed to address cybercrime detection, prevention and mitigation issues within the banking and financial environment.

(d) Cybercriminal threat knowledge

Cyberspace is a platform that has provided the anonymity and options for secrecy and it is fully utilised by cybercriminals to conduct crime. Cybercriminal threat knowledge is the process of gathering data from cybersecurity systems in order to assist cybersecurity personnel to take appropriate actions in dealing with cyberthreats. Inadequate information and knowledge acquisition creates a gap that cybercriminals can exploit and therefore be motivated towards committing the crime. The study recommends that financial institutions should strengthen the monitoring and reporting of cyberthreats at all levels of management and ensure proper and safe management of threat knowledge. This becomes part of the management approach, that consolidates and informs the formation of a responsive cybersecurity culture.

Literature highlights the issue of anonymity in cyberspace, which plays a significant role in motivating cybercriminals to commit crime. The findings show that there is lack of knowledge on whether a particular cybercrime offender is an external or an internal offender, which further affects the knowledge deficiency in addressing the problem in an everchanging cybercrime landscape. The study recommends that financial institutions should request for additional information from customers and stakeholders such as emails as well as implement two factor and multiple factor authentication methods, to mitigate against potential cyberthreats.

(e) Target attractiveness

Target attractiveness consists of features that an individual or object possesses or displays and having a motivation effect to potential offenders to obtain or capture it. In financial institutions, customer data, financial assets (money) are the main targets which are of interest to cybercriminals. The problem is that although financial institutions have in place measures to protect the target, cybercriminals are constantly findings new ways to exploit the security measures. Cybercriminals are often motivated by the perceived

financial gain and furthermore accelerated by the lack of deterrent measures implemented by the financial institutions for protection of the target. The study recommends a robust and contextually designed cybercrime awareness interventions and detection tools deployment, focusing on creating a clear indication and classification of each type of cybercrime linked to the target.

(f) Internal System Control

Systems are the main entry points or gateways that cybercriminals use to gain access to information. It is therefore important that system administrators and users are well equipped in protecting and using the systems within the scope of cybersecurity. As cybercriminals are constantly looking for weaknesses in systems to exploit, the very same approach and resilience should be adopted to protect systems. Banks should be able to detect both publicy known and unknown cyberattacks and should be able to establish and implement multi-layered detection controls that cover processes, technology and employees (BIS & IOSCO, 2016). The study recommends that compliance with standards and frameworks that enhance system control should be adhered to.

Furthermore, conducting of vulnerability assessments combined with threat intelligence sharing, forms a solid foundation in detecting cybercrime. It is important that timely sharing of information strengthens the awareness, preventative and detection of cyberattack incidents.

(g) Change Management

Change management is a tool that focuses on encouragement, engagement and supporting people through a process of change. The main idea behind change is to reduce the habit of assumption especially from a top management level perspective. In the situation of cybercrime, where the speed of threats and attacks are at a high rate, the application of change management is very important. Neglecting this process automatically exposes an organisation, its processes, information and vulnerability of its employees to devastating levels. The study therefore recommends that organisations should focus on establishing a cybersecurity culture that will promote cyber awareness behaviors. In addition, as the cybersecurity culture grows towards a mature stage, the aspect of information sharing amongst the employees is also strengthened.

Figure 6.3 below provides a summary of the study's goals, themes, conclusions, and suggestions regarding the use of theoretical lenses.

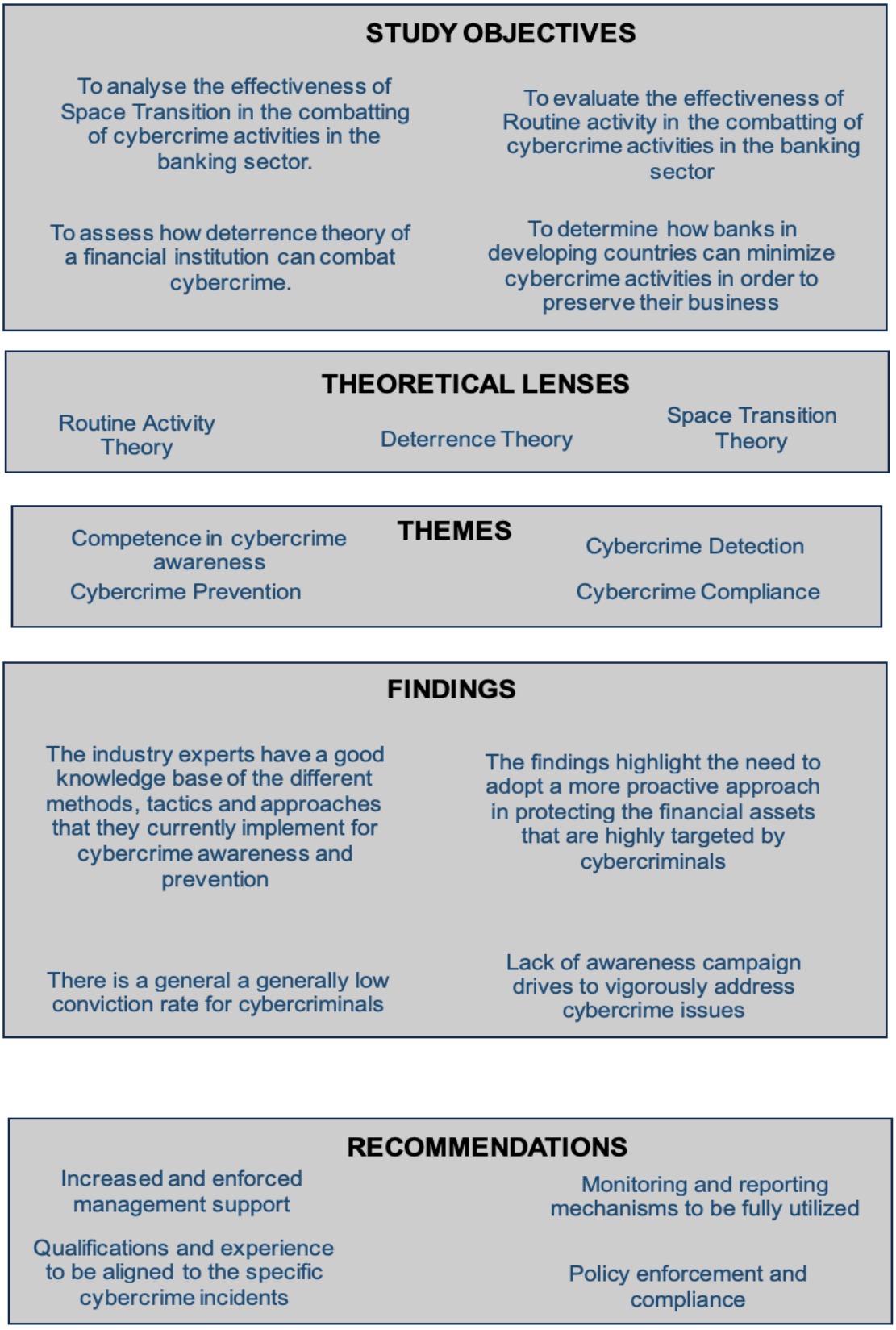


Figure 6.2: Summary of the objectives, themes, theoretical lenses, findings and recommendations

6.6 SUMMARY

This chapter explored and described the factors that contribute to cybercrime activities in the Eswatini banking sector. The cybercrime framework highlights the themes which are based on the routine activity, deterrence and space transition theories. The framework outlines that the absence of a capable guardian, the lack of deterrent measures, the lack of knowledge about cybercriminal characteristics and threats, as well as the weak law enforcement interventions are all major factors that influence cybercriminal activities in the banking sector. From the data analysis and interpretation, it is evident that insufficient control measures, lack of awareness of cyber risks, internal and external cybercriminal knowledge increases the cybercrime activity rate to escalate. The next chapter reflects on research journey by evaluating and concluding the thesis.

CHAPTER SEVEN

EVALUATION OF THE RESEARCH, THESIS CONTRIBUTIONS, AND CONCLUSION

7.1 Introduction

In this chapter, the main goal is to address the research questions and fulfil the study goals. Aligning the findings and the literature review clearly shows that the cybercrime phenomenon is a great concern for the financial sector. The banking sector in Eswatini faces a big threat regarding cybercrime due to the ever-increasing cyber-attacks and the lack of research in this field further adds to the complexity of the subject. The study aimed to bridge the gap by providing an in depth and detailed understanding of cybercrime activities in Eswatini Banks through the development of a conceptual framework in perspective of Eswatini Banks using the space transition theory, deterrence theory and routine activity theory. The concluding chapter provides a summary of the findings, limitations and recommendations for this cybercrime phenomenon.

7.2 The Research Problem

The general research problem for this study is that cybercrime is a global problem that affects all industries particularly the banking sector. The increased adoption of technology by financial institutions especially banks has elevated countries' cyber-attacks risk, further exposing them to financial customer loss. One of the major contributors is that cybercriminals are demonstrating a growing knowledge of the banks' financial systems and the potential weaknesses that exist. The problems associated with cybercrime are normally research based, therefore, to address the cybercrime phenomenon in the Kingdom of Eswatini a request to follow a similar approach should be applied. The specific research problem is that there is insufficient literature that addresses the cybercriminal activities particularly in the context of Eswatini Banks. Thus, this study responded to the research problem by developing a conceptual framework that will address the cybercrime phenomenon in Eswatini banks. Prior to the development of the framework, the research objectives and findings were incorporated in the development of the framework.

7.2.1 Study Goal

The goal of the research was to conceptualise a cybercrime framework for Eswatini banks and this goal was achieved and a cybercrime framework for the banking sector is provided in the previous chapter.

7.2.2. Primary Research Question

In line with the goal, the question directing the study was *How should a cybercrime framework for Eswatini be conceptualized?*

By utilising the three theories, routine activity, deterrence and space transition theories as theoretical lenses, the above research question was answered. Furthermore, the cybercrime framework of how banks should address cybercrime is discussed in the previous chapter.

7.2.3 Sub research questions

RQ1: How should a cybercrime framework for Eswatini be conceptualised?

Cybercrime is influenced by many factors, and from the banks perspective cybercriminal activities are influenced by the following factors;

- Insufficient experience in cybercrime in identifying and applying proper controls for each specific type of attack
- Low cybercrime conviction rates that are a result of lack of evidence and the complexity of the cybercrime activity
- Internal threat control
- Insufficient cybercriminal threat knowledge
- Target attractiveness
- Internal system control
- Change Management

RQ2: How effective is Space Transition in combatting cybercrime in the banking sector?

The space transition theory is about the behaviour of the person as they move from physical space to cyberspace and vice versa. The analysis in the preceding chapter shows that by focusing on the potential internal and external cyber threats, the anonymity and deterrence factors, greatly reduces the probability of the cyber activity from happening. In order for the space transition theory to be effective in combatting cybercrime, the focus should be on limiting the freedom and anonymity factors since they are major drivers in the behavioural intention to commit cybercrime.

RQ3: How can Routine Activity be utilised in combatting cybercrime in the banking sector?

From the analysis above, the Routine Activity theory shows that it is a tool that can be used to identify, gauge and address cybercrime activities in the banking sector. By addressing the conditions necessary for cybercrime to take place, the impact will be greatly reduced. Yar (2005) strongly affirms that the Routine activity theory has the potential to be adapted in addressing cybercrime in cyberspace. A well informed and strategically placed guardian will have a big impact in ensuring that crime does not occur. The likely offender will not only be deterred by the presence of the guardian but will also take an active role in preventing the crime. The overall objective is for the guardian to be effective in deterring cybercrime. Argun and Dagla (2016) affirm that the routine activities theory has suitable practical implications for prevention of crime and therefore, experts in the criminology field should apply the routine activities theory for cybercrime prevention interventions.

RQ4: How can the Deterrence theory assist in combatting cybercrime activities in banking?

For deterrence to work, potential attackers must be satisfactorily concerned that their identity will be exposed, and retaliation will be carried out on them (Hsiang Wei, 2015). Compliance to standards and frameworks that promote cybersecurity are necessary interventions. Furthermore, punishment for cybercrime should be conducted transparently to achieve a deterrent effect on cybercriminals (Tan, 2018). Normally this requires a combination of certainty, severity and celerity to work properly, and to generate an expected cost of committing a crime (Mendes & McDonald, 2001). Certainty is defined

as the risk of getting caught after engaging in a prohibited act, severity is the degree of severity applied in penalties for violation of certain laws or rules and celerity is the swiftness of sanctions after violation of certain laws or rules (Abed & Weistroffer, 2016). In order for the deterrence theory principles to work for the benefit of financial institutions, it is important that the entities involved understand the concept and the level of punishment linked with each cybercrime activity (Howe & Pelser, 2020).

7.3 Limitations of the study

The study was conducted during a period when Eswatini was under Covid-19 lockdown restrictions, where movement of the public were restricted and physical meetings were not encouraged. Interviews that were conducted were under strict Covid-19 rules, that included wearing of masks and social distancing protocols.

The study was limited to interviewing the industry experts within the banks who met the inclusion criteria, however an additional perspective of findings from other banks' stakeholders and customers would bring more in-depth findings and a broader picture into this phenomenon. Nonetheless, the interviews yielded sufficient empirical evidence to provide equitable informed findings and interpretations.

The other limitation is the time frame of the study, and a longitudinal study would provide more evidence over a longer period of time. In addition, access to more data such as reports, strategy documents and contextual observations would give more in-depth insight into this phenomenon.

7.4 Recommendations for future research

This study has highlighted enough information regarding cybercrime in Eswatini Banks, that can be utilized to further explore ways on how to detect, prevent and mitigate cybercrime.

In relation to policy awareness, it is obvious that cybercrime prevention and detection mechanisms will work if the internal designated staff members enforce compliance to cybercrime prevention initiatives. The findings show that without the proper mechanisms of strengthen policy and prevented mechanisms, cybercrime will continue to happen.

The aspect of education which includes awareness and training sessions, should be encouraged and monitored. The involvement of all stakeholders should be the first priority so that in the long run, the coordinate sharing culture can reach a matured state. Additionally, the change management element also plays an important factor to assist the internal staff, stakeholders and customers to adopt and implement cybercrime awareness knowledge for each situation. Future research should consider implementing the conceptualised framework in existing banking institutions. Lastly, the study focused on one area under the financial sector, which was banks. Future studies could incorporate the other areas such as insurance companies and microlending institutions.

7.5 Thesis contributions

The contributions emanating from this study fall under four categories: theoretical, practical, methodological and contextual.

7.5.1 Theoretical

The theoretical contribution of this thesis is in the conceptual cybercrime framework for Eswatini Banks. The literature review has shown the need for more research on cybercrime in the banking sector and how Eswatini banks can benefit from it. This thesis triangulated three theories, namely the routine activity theory, the deterrence theory and the space transition theory. These theories were used as lenses in the collection, analysis and interpretation of the data, and the applicable elements incorporated in the development of the cybercrime framework.

7.5.2 Practical

Eswatini banks have experienced a high and ever-increasing level of cybercrime for quite a period of time. Although many studies have investigated this problem, none have highlighted the magnitude of cybercrime amongst Eswatini Banks. The practical contribution of this thesis is in the implementation of the framework and how the different elements address the cybercrime phenomenon. The practical value is in aligning the standards, policies and practices to the Eswatini banking sector.

7.5.3 Methodological

This study followed an interpretivist approach where the data described the practical influence and relevance of the cybercrime phenomenon. The case study strategy provided an understanding of the cybercrime phenomenon in a real-world scenario. This thesis through the combination of the interpretivist approach and case study strategy provided the platform to enhance better understanding of the cybercrime framework in the banking sector.

7.5.4 Contextual

The operation and existence of banking sectors differ among countries and this thesis acknowledges that fact. The wide variety of frameworks, methods, approaches have been contextualised through the cybercrime framework, specifically for the Eswatini banking sector. This gap has been bridged in the previous chapter.

7.6 Conclusion

The research problem was that financial institutions in Eswatini are affected by an ever-increasing cybercrime attack and despite the overwhelming adoption of technology to mitigate the threats, the impact of cybercrime still persists. The major contributor is the lack of a robust approach in addressing cybercrime since cybercriminals are constantly exploiting the weaknesses in bank financial systems. The specific problem that this study attempted to solve was that there is inadequate literature that addresses the cybercriminal activities particularly in the context of Eswatini Banks. Four objectives were developed to fulfil the main aim of the study, with the outcomes projected towards development of the framework. The first objective was to analyse the effectiveness of Space Transition in the combatting of cybercrime activities in the banking sector, the second objective was to evaluate the effectiveness of Routine Activity in the combatting of cybercrime activities in the banking sector, the third objective was to assess how deterrence theory of a financial institution can combat cybercrime and the last objective was to determine how banks in developing countries can minimise cybercrime activities in order to preserve their business. The objectives were achieved by following the qualitative research method, where data was collected using interviews. To address the research problem, this thesis has conceptualised a framework for financial institutions to address cybercrime in Eswatini banks.

REFERENCES

Abatong, A. B. 2022. Africa commits to Lome Declaration on Cybersecurity. ITWeb Limited. https://itweb.africa/content/dgp45qa6eEbvX9l8 Date of access: 17 June 2023

Abayomi, A.A. 2020. Applying space transition theory to cybercrime: A theoretical analysis of revenge pornography in the 21st century. *International Journal of Innovative Science and Research Technology,* 5(11) pp:631 – 637.

Accenture Analytics Innovation Center, 2015. Protecting the Customer: Fighting Bank Fraud in a New Environment. https://www.accenture.com, 1-9 Date of access: 21 September 2021.

Ade Bilau, A., Witt, E. & Lill, I. 2018. Research methodology for the development of a framework for managing post-disaster housing reconstruction. *Procedia Engineering*, 212:598-605.

Adams, M. & Makramalla, M, 2015. Cyber security skills training: An attacker centric gamified approach. http://timreview.ca/article/861 Date of access: 2 Nov. 2022.

Afripol, 2023. African Union Mechanism for Police Cooperation https://afripol.africa-union.org/.Date of access: 12 August 2023

Ahmad, R & Thurasamy, R. 2022. A systematic literature review of routine activity theory's applicability in cybercrimes. *Journal of Cyber security and Mobility, 11(3),* pp: 405 - 432

Ahmed, N. 2019. Cyberstalking: A content analysis of gender- based offenses committed online. Masters. University of KwaZulu-Natal

Alanezi, F & Brooks, L. 2014. Combatting Online Fraud in Saudi Arabia using General Deterrence Theory (GDT). *Twentieth Americans Conference on Information Systems*, Savannah.

Ali AL- Badran, O.R. 2021. The impact of electronic crimes on the risks of banking financial services in light of the increasing use of banking information technology and communications. Academy of Entrepreneurship Journal, 27(6), 1-9.

Al-Khater, W.A., Al-Maadeed, S., Ahmed, A.A., Sadiq, A.S & Khan, M.K. 2020. Comprehensive review of Cybercrime detection techniques. *Special section on emerging approaches to cyber security, 8*

Allen, N & van der Waag-Cowlin, N. 2021. How African states can tackle state-backed cyber threats. https://www.brookings.edu/articles/how-african-states-can-tackle-state-backed-cyber-threats/. Date of access: 09 February 2024

Alharahsheh, H.H & Pius, A. 2020. A review of key paradigms: Positivism vs interpretivism.. *Global academic journal of humanities and social sciences, 2(3),* pp: 39 - 43

Allmark, P. & Machaczek, K. 2018. Realism and pragmatism in a mixed methods study. Journal of Advanced Nursing, 74(6):1301-1309.

Aloul, F. A. 2010. Information security awareness in UAE: A survey paper. Internet Technology and Secured Transactions (ICITST) 2010 International Conference.

Alvas, I. 2023. An insider threat vs an outsider threat – Which is worse and why?. https://entro.security/blog/an-insider-threat-vs-an-outsider-threat-which-is-worse-and-why/ . Date of access: 16 February 2024

Anshori, 2021. Cybercrime in a criminology perspective. *International journal of sociology, policy and law,* 2(3), pp. 120 - 125

Antonescu, M & Birau, R. 2015. Financial and non-financial implications of cybercrimes in emerging countries. *Procedia Economics and Finance,* 32, pp.618-621

Amarachi, A. A., Okolie, S. O., and Ajaegbu, C. 2013. Information Security Management System: Emerging Issues and Prospect. IOSR Journal of Computer Engineering, 12(3), 96-102.

Arbak, E. 2005. Social Status and Crime. GATE Working Paper No. W.P.05-10. https://ssrn.com/abstract=906771 Date of access: 23 October 2023

Archer, E. 2018. Qualitative data analysis. A primer on core approaches. *Online Raedings in Research Methods, 1 (4),*pp: 1 - 23

Arcuri, D. 2018. How to protect your access control system against cybercrime. https://www.securitymagazine.com/articles/89681-how-to-protect-your-access-control-system-against-cybercrime Date of access: 15 November 2023

Arief, B., Adzmi, M. A. B., & Gross, T. 2015. Understanding cybercrime from its stakeholders' perspectives: Part 1 - attackers. IEEE Security & Privacy, 13(1), 71-76.

Arief, B & Adzmi, M.A.B. 2015. Understanding cybercrime from its stakeholders' perspectives: Part 2 – Defenders and Victims. IEEE Computer and Reliability Societies.

Arnes, A. 2020. Introduction in Arnes, A. (ed.). Cyber Investigations. Unpublished book.

Asal V, Mauslein J, Murdie A, Young J, Cousins K, Bronk C. Repression, education, and politically motivated cyberattacks. J Glob Secur Stud. 2016;1(3):235–247. doi: 10.1093/jogss/ogw006.

Arcuri, M.C., Brogi, M & Gandoli, G. 2017. How does cybercrime affect firms? The effect of information security breaches on stock returns. *First Italian Conference on Cybersecurity*.

Aggarwal, P., Arora, P., Neha & Poonam. 2014. Review on Cyber Crime and Security. *International Journal of Research and Applied Sciences*. ISSN: 2249-9210, 2(1).

Akinbowale, O.E., Klingelhöfer, H.E. and Zerihun, M.F. 2022. Analytical hierarchy processes and Pareto analysis for mitigating cybercrime in the financial sector. Journal of Financial Crime. 29 (3), pp. 948 - 1008

Akua, E.., Ongoa, I.M & Jones, C.R. 2011. Combating Cyber Crime in Sub-Sahara Africa: A Discourse on Law, Policy and Practice. Journal of Peace, Gender and Development Studies, 1(4), pp. 129-137

Alkaabi, A. 2010. Combating Computer Crime: An International Perspective

Arachchilage, N.A.G., & Love, S. 2014. Security Awareness of computer users: A phishing threat avoidance perspective. Computers in Human Behavior, 38, 304 – 312

Argun, U & Dagla, M. 2016. Examination of routine activities theory by the property crime. *International Journal of Human Sciences,* 13, (1), 1188 - 1198. doi:10.14687/ijhs.v13i1.3665

Arpana, M., & Chauhan, M. 2012. Preventing cybercrime: A study regarding awareness of cybercrime in Tricity. *International Journal of Enterprise Computing and Business Systems*, 2(1), pp. 1-10

American Bankers Association, 2022. Ransomware Attacks. https://www.aba.com/advocacy/community-programs/consumer-resources/protect-your-money/ransomware-tips Date of access: 23 July 2022

Ayofe, A.N. & Oluwaseyifunmitan, O. 2009. Towards ameliorating cybercrime and cybersecurity. *International Journal of Computer Science and Information Security,* 3(1)

Babbie, E. 2010. The Practice of Social Research. Wadsworth Cengage Learning. 10 Davis Drive, Belmont, USA

Bada, M & Sasse, A. 2014. Cyber Security Awareness Campaigns: Why do they fail to change behaviour?

Bahari, S.F. 2010. Qualitative versus quantitative research strategies: contrasting epistemological and ontological assumptions. *Sains Humanika*, 52(1).

Bajrami, D., Dika, Z., Shabani, A & Selimi, N. 2020. Cyberspace – Awareness of Vulnerabilities of the Technology enabled communication environment. Management International Conference, 12 – 13 November 2020.

Bande, L.C. 2018. Legislating against Cyber Crime in Southern African Development Community: Balancing International Standards with Country-Specific Specificities. International Journal of Cyber Criminology, 12 (1)

Bank for International Settlements & International Organization of Securities & Commissions. (2016). Guidance on cyber resilience for financial markets infrastructures. https://www.bis.org/cpmi/publ/d146.pdf. Date of Access: 18 February 2024

Bansal, P., Corley, K. (2011). The coming age of qualitative research: Embracing the diversity of qualitative methods. Academy of Management Review,54(2), 233-237

Baram, G. 2008. Israeli Defense in the Age of Cyber War, Middle East Quarterly, Winter 2017 http://www.meforum.org/6399/israeli-defense-in-the-age-of-cyber-war#.WFensTExXws.gmail ; Austin Long, Deterrence: From Cold War to Long War: Lessons from Six Decades of RAND Deterrence research, Santa Monica, CA: RAND Date of access: 17 March 2022

Baron, A. 2021. What is a Bank? https://www.investopedia.com/terms/b/bank.asp Date of access: 04 April 2021

Bawane, M.S. & Shelke, C.J. 2014. Analysis of increasing hacking and cracking techniques. International Journal of Application or Innovation in Engineering & Management, Volume 3(2), February 2014

Beaumier, C & Reese, B. Collaboration: The key to better management of cybercrime and financial crime. Protiviti. https://www.protiviti.com/us-en/whitepaper/the-key-to-better-management-of-cybercrime-and-financial-crime. Date of Access: 13 February 2024

Belaz, A., Krasznay, C & Szabo, Z. 2020. Cybesecurity Strategy and Leadership Management Issues. *International May Conference on Strategic Management,* 16 (1) pp. 242 - 252

Bello, M. 2018. Investigating cybercriminals in Nigeria: A comparative study. PhD. University of Salford

Ben Romdhane Ladib, N. & Lakhal, L. 2015. Alignment between business model and business strategy and contribution to the performance: Empirical evidence from ICT Tunisian venture. *The Journal of High Technology Management Research, 26(2),* pp:168-176

Bhatti, M.A & Jamil, S. Factors effecting cyber incident occurrence: Mediating role of cyber incident reporting mechanism. *International Journal of Cyber Criminology, 17(2)* pp: 112 – 133.

Bhattacherjee, A. 2012. Social science research: principles, methods and practises. Textbooks Collection.

Bishnoi, T.R & Devi, S. 2017. Information technology in banking system. In Palgrave Macmillan Studies in Banking and Financial Institutions. Palgrave Macmillan: n.p. 57. https://www.palgrave.com/gp/series/14678 Date of access: 05 March 2018

Bickman, L. & Rog, D. J. 2008. The SAGE handbook of applied social research methods, Sage publications.

Blog, R. 2023. Top 8 cyber threat maps to track cyberattacks. https://www.redlegg.com/blog/cyber-threat-maps. Date of access: 15 November 2023

Boateng, R., Longe, O. B., Mbarika, V., Avevor, I., & Isabalija, S. R. 2010. Cybercrime and criminality in Ghana: Its forms and implications. Paper presented at the Americas Conference on Information Systems.

Boer, M & Vazquez, J. 2017. Cyber Security & Financial Stability: How cyberattacks could materially impact the global financial system. Institute of International Finance.

Borg, B. 2019. As cybercrime grows, banks are increasingly being targeted. Fintech News. https://www.fintechnews.org/as-cybercrime-grows-banks-are-increasingly-being-targeted/ Date of access: 14 March 2020

Borges, E. 2021. Cybercrime investigation tools and techniques explained. https://securitytrails.com/blog/cyber-crime-investigation. Date of access: 13 November 2023

Brackney, R., & Anderson, R. 2004. Understanding the insider threat (technical report). Santa Monica, CA, USA: RAND Corporation.

Brantly, A.F. 2018. The Cyber Deterrence Problem. In T.Minarik, R. Jakschis, & L. Lindstrom (Eds.),10th International Conference on Cyber Conflict, pp.31-54.

Braun, V. & Clarke, V. 2006. Using thematic analysis in psychology. Qualitative research in Psychology, 3(2), pp. 77-101.

Bridges, D., & Smith, R. D. (Eds.) 2007. Philosophy, methodology and educational research (1st ed.) Wiley-Blackwell.

Britannica. 2023. Commission. Encyclopedia Britannica. https://www.britannica.com/topic/commission-government. Date of access: 12 February 2024

Britz, T. 2009. Computer forensic and cybercrime. New Jersey Pearson Education

Broadhurst, R. 2006. Developments in the Global Law Enforcement of Cyber-Crime. Policing: An International Journal of Police Strategies and Management 29, no. 3 (2006): 408–433.doi:10.1108/13639510610684674.

Brown, C. 2015. Investigating and prosecuting cybercrime: forensic dependencies and barriers to justice. International Journal of Cyber Criminology, 9(1), 55 -119.

Bryman, A. (Ed.) 2012. Social research methods (4th ed.). Oxford: Oxford University Press.

Brynard, D.J., Hanekom, S.X. & Brynard, P.A. 2014. Introduction to Research. 3rd ed. Pretoria: Van Schaik Publishers

Buono, L. Fighting cybercrime through prevention, outreach and awareness raising. ERA Forum 15, 1–8 (2014). https://doi.org/10.1007/s12027-014-0333-4 Date of access: 23 June 2021

Burns, A. J., Posey, C., Courtney, J. F., Roberts, T. L., & Nanayakkara, P. (2017). Organizational information security as a complex adaptive system: insights from three agent-based models. Information Systems Frontiers, 1-16. https://doi.org/10.1007/s10796-015-9608-8

C3SA. 2022. Southern African Development Community Cybersecurity Maturity Report 2021. C3SA

Cacaho, M. 2021. Cyber security policy in developing countries: Rowing in an unfamiliar world withour. a paddle. https://seconcyber.com/cyber-security-developing-countries/ Date of access: 12 June 2022

Canelon, J., Huerta, E., Leal, N & Ryan, T. 2020. Unstructured data for cybersecurity and internal control. *Proceedings of the 53rd Hawaii International Conference on system sciences.pp.5411 - 5420*

Cappelli, D., Moore, A., & Trzeciak, R. 2012. The CERT Guide to Insider Threats: How to Prevent, Detect, and Respond to Information Technology Crimes (Theft, Sabotage, Fraud). Addison-Wesley Professional.

Carter, B. Bolstering Africa's Cybersecurity. https://www.darkreading.com/cybersecurity-analytics/bolstering-africa-cybersecurity. Date of access: 11 February 2024

Cassim, F. (2011). Addressing the growing spectre of cyber crime in Africa: evaluating measures adopted by South Africa and other regional role players. The Comparative and International Law Journal of Southern Africa, 44 (1): 123-138. Available from: https://0-www-jstor-org.ujlink.uj.ac.za/stable/23253117

Cevidalli, A. & Austen, J. 2010. The challenge of combating organised crime. *Computer Weekly;* December 2010. http://www.computerweekly.com/feature/A-new-approach-to-fighting-varied- types-of-cybercrime-cases Date of access: 10 April 2022

Center for Internet Security, 2018. *CIS controls. East Greenbush, NY: CIS.* https://www.cisecurity.org/ Date of access: 20 May 2022

Central Bank of Eswatini, 2024. CBE Guidelines on cybersecurity for financial institutions no. 1 of 2021 https://www.centralbank.org.sz/wp-content/uploads/2021/03/CBE-GUIDELINES-ON-CYBERSECURITY-FOR-FINANCIAL-INSTITUTIONS.pdf. Date of access: 11 February 2024

Chang, L.Y.C. 2020. Legislatie Frameworks against cybercrime: The Budapest Convention and Asia

Chavali, S. 2020. How Insider Threats Impact the Financial Services Industry. Proofpoint. https://www.proofpoint.com/uk/blog/insider-threat-management/how-insider-threats-impact-financial-services-industry Date of access: 14 August 2022

Charter of Trust. 2021a. “Charter of Trust: About.” Charter of Trust. https://www.charteroftrust.com/ about/ Date of access: 17 June 2022

Chawki, M. 2006. Phishing in cyberspace: Issues and Solutions. *Computer Crime Research Center.* https://www.crime-research.org/articles/phishing-in-cyberspace-issues-and-solutions Date of access: 12 May 2021

Chetty, M. (2007). United Nations Definitions of African Regions Original Graphic. Environment and Behavior, 38(1), 5–21.

Choi, S. 2020. Center for Internet Security (CIS) is a Center for Information Security. https://sonraisecurity.com/blog/center-for-information-security-cis-offers-cybersecurity-solutions/ Date of Access: 09 February 2024

Choo, K.K.R. 2011. The cyber threat landscape: Challenges and future research directions. Computers and Security, 308: 719-731

Ciglic, K & Hering, J. 2021. A multi stakeholder foundation peace in cyberspace. Journal of Cyber Policy, 6(3), pp. 360-374

Cisternelli, E. 2020. 7 Cybsersecurity frameworks that help reduce cyber risk. https://www.bitsight.com/blog/7-cybersecurity-frameworks-to-reduce-cyber-risk#:~:text=What%20is%20a%20cybersecurity%20framework,and%20those%20of%20their%20vendors Date of access: 29 May 2022

Clarke RV 1995 ‘Situational crime prevention’ Crime and Justice vol 19 pp 91-150

Cloudfare, 2024. What is credential stuffing? Credential stuffing vs brute force attacks. https://www.cloudflare.com/en-gb/learning/bots/what-is-credential-stuffing/. Date of access: 10 February 2024

Cohen, L. & Felson, M. 1979. Social change and crime rates trends: A routine activity approach. American Sociological Review,44, pp. 588-608.

Cohen, L. & Manion, L. 1994. Research methods in education. London. Routledge

Coker, J. 2021. Sharing is caring: Using intelligence to fight cybercrime. https://www.infosecurity-magazine.com/magazine-features/using-intelligence -to-fight/. Date of access: 01 Nov 2023

Cohen, L.E., Kluegel, J.R & Land, K.C. 1981. Social Inequality and Predatory Criminal Victimization: An Exposition and Test of a Formal Theory, *American sociological review. 45(5), pp: 505 – 524.* https://doi.org/ 10.2307/2094935

Council of Europe, 2019. Cybercrime legislation. https://www.coe.int/en/web/octopus/country-wiki/- /asset_publisher/hFPA5fbKjyCJ/content/swaziland/pop_up?inheritRedirect=false Date of access: 12 May 2022

Council of Europe. 2018a. Convention on Cybercrime of the Council of Europe (CETS No.
185. https://www.coe.int/en/web/conventions/full-list/- /conventions/treaty/185 Date of access: 12 October 2021

Creswell, W.J. 2008. Educational Research: Planning, Conducting and Evaluating Quantitative and Qualitative Research. 3rd Ed, Upper Saddle River, NJ: Pearson Education

Creswell, J.W. 2009. Research Design Qualitative, Quantitative and mixed methods approaches. New Delphi: SAGE Publications, Inc.

Creswell, J.W. 2013. Qualitative inquiry and research design: Choosing among five approaches. 3rd edition. London: SAGE.

Crisanto, C & Prenio, J. 2017. Financial stability insights on policy implementation No 2. Regulatory approaches to enhance banks' cybersecurity frameworks. https://www.bis.org/. Date of Access: 15 February 2024

Cummings, A., Lewellen, T., McIntire, D., Moore, A., & Trzeciak, R. (2012). Insider Threat Study: Illicit Cyber Activity Involving Fraud in the U.S. Financial Services Sector (Special Report CMU/SEI-2012-SR-004). CERT Program. Retrieved from www.sei.cmu.edu/reports/12sr004.pdf

CyberPeace Institute, 2021. Paris Call for Trust and Security in Cyberspace Working Group 5 Building aa Cyberstability Index Final Report.https://cyberpeaceinstitute.org/publications/paris-working-group-report/. Date of Access: 16 February 2024

D'Arcy, J., & Greene, G. 2014. Security culture and the employment relationship as drivers of employees' security compliance. Information Management & Computer Security, 22(5), 474-489. doi: 10.1108/IMCS-08-2013-0057

Dahir, A.L 2018. Cybercrime is costing Africa's businesses billions. Quartz Africa. https://qz.com/africa/1303532/cybercrime-costs-businesses-in-kenya-south-africa-nigeria-billions/ Date of access: 03 March 2020

Dalla, E.H. & Geeta, M.S. 2013. Cybercrime a threat to persons, property, government and societies. International Journal of Advanced Research in Computer Science and Software, 3(5), pp. 997-1002.

Daniel, M. 2024. Sharing threat intelligence isn't easy: Lessons learned from practice. https://www.cyberthreatalliance.org/sharing-threat-intelligence-isnt-easy-lessons-learned-from-practice/#:~:text=Sharing%20only%20produces%20useful%20results,cyber%20threat%20information%20becomes%20noise. Date of access: 04 February 2024

Deloitte Fraud Survey. 2015. The Deloitte India banking fraud survey. (No. Report Edition II). Press Trust of India Report.

Denning, D. 2000. Reflections on cyberweapons controls. Computer Security Journal, 16(4), 3-53.

Denzin, N.K. & Lincoln, Y.S. (Eds.). (2005). Handbook of qualitative research (3rd ed.). London: Sage.

Desai, A. 2018. Cybercrime cyber surveillance in South Africa. Acta Criminologica: South African journal of criminology 31 (3), 149-160.

Devi, R.S. & Mohankumar, M. 2019. An empirical study on cyber security threats and attacks. *International Journal of Scientific Research and Review, 7 (3)* pp.2271-2276

Dicks, J.(2012.*Uncover the secret scams and tricks to profit in the world's largest financial market.* USA: McGraw-Hill.

Dhillon G., Silva, L. & Backhouse, J. 2004. Computer crime at CEFORMA: a case study, International Journal of Information Management, 24 (6), pp. 551-561.

Dlamini, S. & Mbambo C. 2019. *Understanding policing of cybercrime in South Africa the phenomena challenges and effective responses.* Cogent Social Sciences 5 (1), 1675404,

Dogaru, O. (2012). Securing critical infrastructures. https://www.academia.edu/14172231/osint_in_the_globalization_of_the_access_to_information Date of access: 18 September 2021

Douligeris, C. and Serpanos, D.N. 2007. Network Security: Current Status and Future Directions. Hoboken, NJ, USA: Wiley, 2007

Duncan, B & Whittington, M. 2014. Compliance with standards, assurance and audit: does this equal security?. In *Proceedings of the 7th International Conference on Security of Information and Networks* , pp:77-84.

Duncan, B & Whittington, M. 2016. Cloud Cyber-Security: Empowering the Audit Trail. *International Journal on Advances in Security, 9(3) pp 169 – 183. http://www.iariajournals.org/security/* Date of access: 10 February 2021

Dzomira, S. (2014). Electronic fraud (cyber fraud) risk in the banking industry, Zimbabwe. Risk Governance & Control: Financial Markets & Institutions, 4(2): 17-27. https://doaj.org/article/1d7c01313790408b9735408e4d2f43d6 Date of access: 04 July 2021

Easterby-Smith, M., Thorpe, R., & Lowe, A. 2008. Management research: theory and practice (3rd ed.). London: Sage Publishers.

EastWest Institute, 2020. Global Commission on the Stability of Cyberspace. https://www.eastwest.ngo/in-focus/global-commission-stability-cyberspace Date of Access: 15 February 2024

Ebru, A & Baykan, B. 2017. Discover the world's research. Turk J Neurol, 23.pp. 88 – 89.

Educative, 2024. What are IOT attacks? https://www.educative.io/answers/what-are-iot-attacks. Date of access: 09 February 2024

Eisenhardt, K.M. & Graebner, M.E. 2007. Theory building from cases: Opportunities and challenges. Academy of management journal, 50 (1), pp. 25–32.

Elder, A. D. 2002. Characterizing fifth grade students' epistemological beliefs in science. 347-364.

Emhemed, E. & Pandey, R. 2017. A Study of Computer Application in Resource Management and Developing a Model Network Adoption in Construction Projects. International Journal of Scientific Engineering and Technology Research, 06(08): 1670–1675

Ennin, D. 2015. Cybercrime in Ghana: A study of offenders, Victims and the law. University of Ghana.

Erhabor, I.M. 2008. Cybercrime and the Youths (PGDE Thesis), Department of Education, Ambrose Alli University, Ekpoma, Nigeria, p.37.

Erin, O. A., Kolawole, A.D & Noah, A. O. Risk governance and cybercrime: the hierarchical regression approach. *Future Business Journal, 6(1),* pp: 1 - 15

ESCCOM, 2024. Eswatini Computer Incident Response Team. https://ncsirt.org.sz/who-we-are/. Date of access: 10 February 2024

Eswatini Bankers Association, 2024. Fraud Awareness. https://eba.org.sz/fraud/. Date of access: 21 February 2024

Eswatini Communications Commission, 2022. Annual Report 2022.

European Central Bank. 2016. Cyber resilience oversight expectations (CROE) for financial markets infrastructures. Available from: https://www.ecb.europa.eu/paym 59 /pdf/cons/cyberresilience/cyber_resilience_oversight_expectations_for_FMIs.pdf . Date of Access: 12 February 2024

European Commission, 2013. Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, JOIN 1 Final, European Commission, Brussels. https://eeas.europa.eu/ archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf Date of access: 16 November 2022

Ewuga, S.K., Egieya, Z.E., Omotosho, A & Adegbite, A.O. 2023. ISO 27001 In Banking: An evaluation of its implementation and effectiveness in enhancin information security. *Finance & Accounting Research Journal, 5 (12)* pp: 405-425

Fadayo, O.M. 2018. An Examination of E-Banking Fraud Prevention and Detection in Nigerian Banks. De Montfort University.

Felson, M., & Clarke, R. V. 1998. Opportunity makes the thief: Practical theory for crime prevention. Policing and Reducing Crime Unit: Research, Development and Statistics Directorate, 98, 1-36.

Fleming, M. J., Greentree, S., Cocotti-Muller, D., Elias, K. A., & Morrison, S. (2006). Safety in Cyberspace: Adolescents' Safety and Exposure Online. *Youth & Society, 38(2),* pp: 135–154. https://doi.org/10.1177/0044118X06287858

Filipkowski, B. 2021. The four biggest risks cyber-attacks pose for financial institutions. https://fieldeffect.com/blog/financial-institutions-cyber-risks/ Date of access: 04 October 2021

Forbes, 2023. The effects of cybercrime on small businesses. https://www.forbes.com/sites/forbestechcouncil/2023/05/11/the-effects-of-cybercrime-on-small-businesses/?sh=4ee339372f68. Date of access: 17 February 2024

Fortinet, 2022. Pharming. https://www.fortinet.com/resources/cyberglossary/pharming Date of access: 23 May 2022

Fusch, P.I. & Ness, L.R. 2015. Are we there yet? Data saturation in qualitative research. The Qualitative Report, 20(9), pp. 1408-1416. http://www.nova.edu/ssss/QR/QR20/9/fusch1.pd Date of access: 11 March2020

Gaumer, Q., Mortier, S & Moutaib, A. 2016. Financial institutions and cyber crime: Between vulnerability and security. Financial Stability in the digital era. Financial Stability Review, 20, pp. 45 - 51

Ghazi-Tehrani, A.K & Pontell. H.N. 2021. Phishing Evolves: Analyzing the Enduring Cybercrime, Victims & Offenders, 16 (3), pp.316-342, DOI:10.1080/15564886.2020.1829224

Gibbs, J.P. 1985. Deterrence Theory and Research Nebraska Symposium on Motivation: The Law as a Behavioral Instrument. Lincoln: University of Nebraska Press, 33.

Gillespie, A. A. 2015. Cybercrime: Key Issues and Debates Florence, Kentucky, pp.17.

Given, L.M. 2016. 100 Questions (and Answers) About Qualitative Research. Sage, Thousand Oaks

Grady, M.P. 1998. Qualitative and Action Research: A Practitioner Handbook. Phi Delta Kappa Educational Foundation, Bloomington

Goel, S. Cybercrime in developing countries. *Journal of Law Students and Researchers. (1) 4*

Gordon, S. & Ford, R. 2006. On the definition and classification of cybercrime. *Journal of Computer Virol*, 2, pp. 13-20.

Gordon, L.A., Loeb, M.P. & Sohail, T. 2003. A framework for using insurance for cyber-risk management, Communications of the ACM, 46 (3), pp.81-85

Government of Eswatini. 2019. Status of proposed legislation. http://www.gov.sz/index.php/component/content/article/141-test/2002-bills# Date of access: 12 January 2020

Graneheim, U.H. & Lundman, B. 2004. Qualitative content analysis in nursing research: Concepts, procedures and measures to achieve trustworthiness. Nurse Education Today, 24(2): 105–112.

Goodman, M. 2010. International dimensions of cybercrime. In: Cybercrimes: A multidisciplinary analysis, ed. S. Ghosh and E. Turrini. Berlin and Heidelberg: Springer-Verlag

Grobler, M, Van Vuuren, JJ & Zaaiman, J. 2013. Preparing South Africa for Cyber Crime and Cyber Defence. In: Systemics, cybernetics and informatics, 11(7), pp.32-41

Grohe, B. R. 2006. Perceptions of crime, fear of crime and defensible space in fort worth neighborhoods. PhD. The University of Texas at Arlington

Hall T, Sanders B, Bah M, King O, Wigley E. (2020) Economic geographies of the illegal: the multiscalar production of cybercrime. Trend OrganCrime 24: pp.282–307

Harguem, S. & Echatti, H. (n.d). IT Governance Status in the Tunisian Banking Sector. http://0-eds.a.ebscohost.com.ujlink.uj.ac.za/eds/pdfviewer/pdfviewer?vid=1&sid=e0c7a18b-8776-49d9-84ad-5c8b4c463f4b%40sessionmgr4009 Date of access: 02 March 2019

Hanlon, B. & Larget, B. 2011. Samples and population. Department of Statistics-University of Wisconsin-Madison. http://www.stat.wisc.edu/~st571-1/03-samples-4.pdf Date of access: 12 April 2020

Hassan, M.N. 2022. Applicability of routine activity theory: An analysis based on cybercrime in Bangladesh. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4265385 Date of access: 19 May 2020

Hassan, A.B., Lass, F.D & Makinde, J. 2012. Cybercrime in Nigeria: Causes, Effects and the Way Out.ARPN. *Journal of Science and Technology*, 2(7) pp. 626 – 631.

Herselman, M. & Warren. M. 2004. Cyber Crime influencing businesses in South Africa. *Journal of issues in informing Science and Information Technology*, 1, pp. 253 -266.

Holt, T. J., & Bossler, A. M. 2008. Examining the applicability of lifestyle-routine activities theory for cybercrime victimization. Deviant Behavior, 30(1), 1-25.

Ho, H., Gilmour, J., Mazerolle, L & Ko, R. (2023). Utilizing cyberplace managers to prevent and control cybercrimes: a vignette experimental study. Secur J (https://doi.org/10.1057/s41284-023-00371-8

Horan, C & Saiedian, H. 2021. Cyber Crime Investigation: Landscape, Challenges, and Future Research Directions. *Journal of Cybersecurity and Privacy. 1(4)* pp: 580-596. https://doi.org/10.3390/jcp1040029

Howe, E.L & Pelser A.M.F. 2020. Cybercrime in Eswatini: The deterrence theory approach. Ensovoort. Journal of Cultural Studies. 41 (11) pp. 1 – 17

Howe, EL and Prof Pelser Anna-Marie. 2022. Cybercrimes in the Eswatini banking sector: Implementing routine activity theory analysis. Ensovoort. Journal of Cultural Studies. Vol 43. No.07

Hsiang Wei, M.L. 2015. The challenges of cyber deterrence. *Journal of the Singapore armed forces*, Vol 41, No. 1, pp 12 – 22

Hui, K., Kim, S. H and Wang, Qiu-Hong, W. 2017. Cybercrime deterrence and international legislation: Evidence from distributed denial of service attacks. *MIS Quarterly*. 41, (2), 497-523. Research Collection School of Information Systems.

Hull, M., Eze, T., & Speakman, L. 2018. Policing the cyber threat: Exploring the threat from cyber crime and the ability of local law enforcement to respond. 2018 European Intelligence and Security Informatics Conference (EISIC). https://doi.org/10.1109/eisic.2018.00011

Hull, G., John, H & Arief, B. 2019. Ransomware deployment methods and analysis: views from a predictive model and human responses/. Crime Science, *8, 2* pp: 1-22.https://doi.org/10.1186/s40163-019-0097-9

ISMS.online, 2024. ISO 27001 for the banking sector. https://www.isms.online/sectors/iso-27001-for-the-banking-sector/. Date of access: 09 February 2024

Joffe, H. 2012. Thematic analysis. (In Harper, D. & Thompson, A.R., eds. Qualitative research methods in mental health and psychotherapy: Ka guide for students and practitioners. West Sussex: Wiley- Blackwell.

Lenaerts-Bergmans, B. 2023. Attack vectors: What they are and how they are exploited. https://www.crowdstrike.com/cybersecurity-101/threat-intelligence/attack-vector/ Date of access: 12 October 2023

Lenaerts-Bergmans, B. 2023. Advanced Persistent Threat (APT). https://www.crowdstrike.com/cybersecurity-101/advanced-persistent-threat-apt/. Date of Access: 13 February 2024

Lippert, K.J & Cloutier R. Cyberspace: A Digital Ecosystem. Systems. 2021; *9(3):* pp48. https://doi.org/10.3390/systems9030048

Ibor, B. I. 2016. An empirical investigation of the human resources nexus to frauds in the nigerian banking sector.*International Journal of Scientific and Research Publications, 6*(6), 231-247.

Ikechi, K.S. & Okay O.E. 2013. The Nature, Extent and Economic Impact of Fraud on Bank Deposits in Nigeria. *Interdisciplinary Journal of Contemporary Research in Business*, 4 (9) pp. 253-265

Internet World Stats. 2020 Usage and population statistics https://www.internetworldstats.com/stats1.htm Date of access: 13 August 2022

Interpol, 2021. Interpol report identifies top cyberthreats in Africa. https://www.interpol.int/en/News-and-Events/News/2021/INTERPOL-report-identifies-top-cyberthreats-in-Africa Date of access: 12 June 2021

Interpol, 2021. African Cyberthreat Assessment Report. Interpol's key insight into cybercrime in Africa.

Interpol, 2022. Cybercrime cross borders and evolve rapidly. https://www.interpol.int/en/Crimes/Cybercrime Date of access: 30 May 2022

Interpol, 2023. African cyberthreat assessment report cyberthreat trends: Outlook by the African Cybercrime Operations Desk. https://www.interpol.int/content/download/19174/file/2023_03%20CYBER_African%20Cyberthreat%20Assessment%20Report%202022_EN.pdfDate of access: 07 February 2024

International Telecommunications Union, 2007. Cybersecurity guide for developing countries. https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-SECU-2007-PDF-E.pdf Date of access: 25 May 2020

Imprivata, 2019. Who, What,When, Where; The power of the audit trail in data security. https://www.imprivata.com/blog/who-what-when-where-the-power-of-the-audit-trail-in-data-security Date of access 03 July 2022

Ja. A. 2015. Insider vs outsider threats: identify and prevent. https://resources.infosecinstitute.com/topics/insider-threat/insider-vs-outsider-threats-identify-and-prevent/. Date of access: 09 February 2024

Jabareen, Y. 2009. Building Conceptual Framework: Philosophy, Definitions, and Procedure. *International Journal of Qualitative Methods*, 8(4).

Jackson, A. 2023. Cyberattack increase across Africa threatens digital growth. https://cybermagazine.com/cyber-security/cyber-attack-increase-across-africa-threatens-digital-growth. Date of access: 13 February 2024

Jaishankar, K. 2008. Space Transition Theory of cyber-crimes. In Schmallager, F. & Pittaro, M. (Eds.), Crimes of the Internet. Upper Saddle River, NJ: Prentice Hall, pp .283-301

Jang-Jaccard, J., & Nepal, S. (2014). A survey of emerging threats in cybersecurity. Journal of Computer and System Sciences, 80, 973-993. doi:10.1016/j.jcss.2014.02.005

Javapoint, 2024. Types of cyber attackers. https://www.javatpoint.com/types-of-cyber-attackers#:~:text=In%20computer%20and%20computer%20networks,unauthorized%20use%20of%20an%20asset. Date of access: 11 February 2024

Jonker, M. 2015. One in ten SA businesses have experienced cyberattacks. https://www.grantthornton.co.za/insights/articles/one-in-ten-sa-businesses-haveexperienced-cyber-attacks-in-the-past-year/ Date of access: 12 October 2022

Krambia-Kapardis, M. 2002. A fraud detection model: A must for auditors. Journal of Financial Regulation and Compliance, 10(3) pp:266-278.

Kimani, W. 2013. EAC banks grapple with fraud cases. Daily Nation, Smart Company, pp. 2-3.

Kipane, A. 2019. Meaning of profiling of cybercriminals in the security context. SHS Web of Conferences. https://doi.org/10.1051/shsconf/20196801009 Date of access: 12 August 2020

Klenka, M. 2021. Aviation cyber security: legal aspects of cyber threats. *Journal of transportation security, 14(3-4)*, pp:177-195. https://doi.org/10.1007/s12198-021-00232-8

Kovalova, O & Kovalova, V. 2021. Ways to improve protection against cybercrime in the banking sphere. *Advances in Economics, Business and Management Research, 188. pp.149 - 154*

Kranenbarg, W.M. (2021). The challenges of empirically comparing cybercriminals and traditional criminals. In A. Lavorgna, & T. J. Holt (Eds.), Researching Cybercrimes: Methodologies, Ethics, and Critical Approaches, pp. 107-126. Palgrave / MacMillan. https://doi.org/10.1007/978-3-030-74837-1_6

Kortan, N & von Solms, R. 2012. Fostering a cyber-security culture: a case of South Africa. *Proceedings of the 14th Annual Conference of World Wide Web Applications, 7-9 November 2012, Durban, South Africa*

KPMG, 2018. Staying ahead of cybercrime. UK Finance. [Online] https://www.ukfinance.org.uk/system/files/Staying-ahead-of-cyber-crime.pdf

Karuppannan, J., & Chandra, R.R. (2017). Space Transition Theory of Cyber Crimes. Module 23, e-Pathsala, University Grants Com- mission. Online. http://epgp.inflibnet.ac.in/ahl.php?csr- no=1608 Date of access: 07 June 2022

Jaleshgari, R. 1999. Document trading online. Information Week, 755: 136.

Keranen, A.M. 2022. Rising cyber threats targeting the banking sector. University of Jyvaskyla. thesis

Kilani, M. Al & Kobziev, V. 2016. An Overview of Research Methodology in Information System (IS). Open Acess Library Journal, 03(11): 1–9. http://www.oalib.com/paper/pdf/5275653.

Kshetri, N. (2010) “Diffusion and Effects of Cybercrime in Developing Economies,” Third World Quarterly, 31(7), 1057 – 1079.

Kirgel, A. 2012. Routine Activity Theory and the determinants of high cybercrime countries. *Social Science Computer Review,* 30(4), pp. 470-486

Kivunja, C. & Kuyini, A.B. 2017. Understanding and Applying Research Paradigms in Educational Contexts. *International Journal of Higher Education.* 6(5).

Kethineni, S., Cao, Y. & Dodge, C. 2017. Use of Bitcoin in Darknet Markets: Examining Facilitative Factors on Bitcoin-Related Crimes. *American Journal of Criminal Justice*. doi:10.1007/s12103-017-9394-6.

Korolov, M. 2021. Supply chain attacks show why you should be wary of third-party providers.https://www.csoonline.com/article/561323/supply-chain-attacks-show-why-you-should-be-wary-of-third-party-providers.html Date of access: 09 February 2024

KPMG (2012). Cybercrimes: A Financial Sector Review. Government and Public Sector

Khan, S. R. (2018). Implication of cyber warfare on the financial sector. An exploratory study. *International Journal of Cyber-Security and Digital Forensics*, *7*(1), 31–38.

Khumalo, S. 2019. Recent Bank Fraud Cases. *Times of Swaziland,* p.3

Kodellas, S., Fisher, B. S. & Wilcox, P. 2015. Situational and dispositional determinants of workplace victimization: The effects of routine activities, negative affectivity, and low self control. *International review of victimology*, 21 (3), pp. 321-342

Kothari, C.R. 2004. Research Methodology: Methods and Techniques. New Age International Publishers.

Kost, E. 2022. The 6 Biggest Cyber Threats for Financial Services in 2022. UpGuard. [Online] Available at: https://www.upguard.com/blog/biggest-cyber-threats-for-financial-services

Kraemer-Mbula, E., Tang, P. & Rush, H. 2013. The cybercrime ecosystem: Online innovation in the shadows? *Technological Forecasting and Social Change*, 80 (3), pp. 541-555.

Kranenbarg, M.W., Holt, T.J. & van Gelder, J. 2019. Offending and Victimization in the Digital Age: Comparing Correlates of Cybercrime and Traditional Offending-Only,

Victimization-Only and the Victimization-Offending Overlap, *Deviant Behavior*, 40(1), pp. 40-55.

Kshetri, N. 2010. Diffusion and Effects of Cyber-Crime in Developing Economies. Third World Quarterly. Vol. 31, Issue 7 pp.1057-1079 https://www.tandfonline.com/doi/abs/10.1080/01436597.2010.518752 Date of access: 12 September 2020

Kshetri, N. 2019. Cybercrime and Cybersecurity in Africa. *Journal of Global Information Technology Management*. DOI: 10.1080/1097198X.2019.1603527

Kirwan, D. 2017. An Investigation of the Attitudes and Environmental Factors that Make People more Willing to Participate in Online Crime, Masters Dissertation, Dublin Institute of Technology.

Kundu, S., Islam, K. A., Jui, T. T., Rafi, S., Hossain, A. & Chowdhury, I. H. (2018). Cyber crime trends in Bangladesh, an analysis and ways out to combat the threat. International Conference on Advanced Communications Technology. Doi:10.23919/ICACT.2018.8323800. Available at: https://0-ieeexplore-ieeeorg.ujlink.uj.ac.za/stamp/stamp.jsp?tp=&arnumber=8323800 (Accessed on 27 June 2018).

Kumar, S. 2018. Understanding Different Issues of Unit of Analysis in a Business Research.

Lagazio, M., Sherif, N., Cushman, M., 2014. A multi-level approach to understanding the impact of cyber crime on the financial sector, *Computers & Security,* Elsevier, 45, pp. 58-74

Lakshmanan, A. 2019. Literature review of cybercrimes and its prevention mechanisms. 10.13140/RG.2.2.16573.51684.

Lathar, P. 1992. Critical frames in educational research: Feminists and post-structural perspectives Theory into practice, XXXI, 2, pp. 87-99

Latham, B. (2007). Sampling: What is it? Quantitative Research Methods, ENGL, 5377.

Lastdrager, E,E,H. 2014. Achieving a consensual definition of phishing based on a systematic review of the literature. *Crime Science, 3(1)* pp: 1 - 10 doi: 10.1186/s40163-014-0009-y.

Lewis, J. 2018. Economic Impact of Cybercrime – No slowing down. McAfee, Santa Clara, pp. 1-28

Liao, R., Balasinorwala, S., & Rao, H. R. (2017). Computer assisted frauds: An examination of offender and offense characteristics in relation to arrests. *Information Systems Frontiers, 19*, 443-455.

Lickiewicz, J. 2011. Cybercrime psychology-proposal of an offender psychological profile. *Problems of forensic sciences,* pp: 239 – 252.

Liebl, D. 2022. How to manage your bank's cybersecurity risk with CIS critical security controls. Date of access: 10 February 2024

Lec, I. S. O. (2013). Information technology - Security techniques - Information security management systems - requirements. https://www.iso.org/standard/54534.html Date of access: 05 November 2023

Lechner, N. H. 2017. An overview of cybersecurity regulations and standards for medical device software. Central European Conference on Information and Intelligent Systems, 237-249. Faculty of organization and informatics varazdin. http://archive.ceciis.foi.hr/app/public/conferences/2017/06/QSS-3.pdf

LII, 2021. Treaty.Cornell Law School. https://www.law.cornell.edu/wex/treaty. Date of access: 16 February 2024

Linneberg, M.S & Korsgaard, S. 2019. Coding qualititative data: A synthesis guiding the novice. *Qualitative Research Journal*

Livesey, C. 2006. The relationship between Positivism, Interpretivism and sociological research methods. *AS Sociology.* http://www.sociology.org.uk Date of access: 24 November 2020

Long, L. (2012). Profiling Hackers. SANS Institute. http://www.sans.org/readingroom/whitepapers/hackers/profiling-hackers-33864 Date of access: 12 November 2022

Lohr, S. (2009). Sampling: Design and Analysis. Nelson Education.

Lubua, E.W. 2014. Cyber Crimes Incidents in Financial Institutions of Tanzania. *International Journal of Computer Science and Business Informatics*, 14 (3), pp. 37-48.

Leuprecht, C. (2019). Mitigating cyber risk across the financial sector. https://www.cigionline.org/articles/mitigating-cyber-risk-across-financial-sector Date of access: 06 August 2021

Luce, R. Duncan & Howard R. (1957). Games and Decisions. New York; NY: Dover.

Nesovic, D & Jerotijevic, D. 2018. Role and Importance of International Agreements in regulating International relations in Modern conditions. *Ekonomika, 64(3)* pp: 89 - 102

Njeri, P.W & Gaitho, V. 2019. Investigating extent to which cybercrime influences performance of commercial banks in Kenya. *International Journal of Economics, Commerce and Management, 7 (8),* pp: 489 - 514

Ndubueze, P. (2016). Cyber Criminology and the Quest for Social Order in Nigerian Cyberspace. The Nigerian Journal of Sociology and Anthropology. 14. 32-48. 10.36108/NJSA/6102/14(0130).

Ngulube, P., Mathipa, E.R. & Gumbo, M.T. 2015. Theoretical and Conceptual Frameworks in the Social and Management Sciences. In: *Addressing Research Challenges: Making Headway for Developing Researchers*, Boordwyk: Mosala-Masedi, pp.43-66

Nzeakor, O. F., Nwokeoma, B.N & Ezeh, P.J. 2020. Pattern of cybercrime awareness in Imo State, Nigeria: An empirical assessment. *International Journal of Cyber Criminology, 14 (1)* pp. 283 - 299

Mandelcorn, S. 2013. An explanatory model of motivation for cyber-attacks drawn from criminological theories. Dissertation. University of Maryland

Mackenzie, N. & Knipe, S. 2006. Research dilemmas: Paradigms, methods and methodology. Issues in Educational Research, 16(2): 193 – 205.

Malby, S., Mace, R., Holterhof, A., Brown, ., Kascherus, S & Ignatuschtschenko, E. 2013. Comprehensive Study on Cybercrime. *United Nations Office on Drugs and Crime,*

Malik, M.S & Islam, U. 2019. Cybercrime: an emerging threat to the banking sector of Pakistan. Journal of Financial Crime, 26(1), pp. 50-60. Date of access: 07 July 2022

Maluvu, A. 2023. Corruption, Cybercrime and Compliance – Managing the risks. https://www.thebanker.com/Corruption-cybercrime-and-compliance-managing-the-risks.Date of access: 10 November 2023

Maree, K. 2010. First Steps in Research. Pretoria: Van Schaik Publishers.

Maat, S. 2004. Cybercrime: A Comparative Law Analysis (Doctoral thesis), University of South Africa, Pretoria, South Africa, p. 23

Marshall, M. N. (1996). Sampling for qualitative research. Family Practice,13(6), 522-526.

Matengu, S. 2012. Cybercrime awareness and reporting in the public sector in Botswana. Dissertation. University of Cape Town.

Matthew, O.F. 2016. Sociological and technological factors that enhance cybercrime and cyber security in Nigeria. *International Journal of Law and Legal Studies,* 4(5), pp. 207-2016

Marco, G. 2012. Understanding cybercrime: Phenomena, challenges and legal response. *International Telecommunication Union.*

Matengu, S. 2012. Cybercrime awareness and reporting in the public sector in Botswana. Thesis. University of Cape Town

Mayunga, J. 2013. Cybercrimes Investigation in Tanzania. Morogoro: Mzumbe University
Merriam, S.B. 2002. Introduction to qualitative research. *Qualitative research in practice: Examples for discussion and analysi*ns, 1(1):1-17.

Maurer, T & Nelson, A. 2021. The global cyber threat. https://www.imf.org/external/pubs/ft/fandd/2021/03/global-cyber-threat-to-financial-systems-maurer.htm. Date of access: 12 February 2024

Mays, N., & Pope, C. 1995. Rigour and qualitative research.BMJ: British Medical Journal, 311(6997), 109.

McQuade, S.C. 2006. Understanding and Managing Cybercrime. New York: Allyn and Bacon.

McQuade III, S.C. (2009). Encyclopedia of Cybercrime, Westport, Connecticut: Greenwood Publishing Group, Inc., pp. 181-182.

Mercer, E. (2016). Causes of cyber-crime. It StillWorks Website. http://techin.oureverydaylife.com/causes-cyber-crime-1846.html Date of access: 20 July 2021

Merriam, S.B. 2009. Qualitative Research: A Guide to Design and Implementation. Revised and Expanded from Qualitative Research and Case Study Applications in Education. San Francisco: Jossey-Bass.

Miller, J. (2013). Individual offending, routine activities, and activity settings: Revising the routine activity theory of general deviance. Journal of Research in Crime and Delinquency, 50(3), 390-416.

Mitchell, J. 2022. Africa faces huge cybercrime threat as the pace of digitalization increases https://www.investmentmonitor.ai/analysis/africa-cyber-crime-threat-digitalisation#:~:text=Cybercrime%20is%20estmated%20to%20cost,m%20and%20Kenya%20%2436m Date of access: 12 August 2022

Minniti, R. (2016). Identifying business risk factors of identity theft. Doctoral dissertation. Washington: Walden University.

Monaghan, R.M. 2020. Cybercrime response capabilities and capacity: An evaluation of local law enforcement's response to a complex problem. Thesis.

Mondragon, L. 2021. What are state-sponsored cyberattacks? https://blog.f-secure.com/what-are-state-sponsored-cyberattacks/. Date of Access: 10 February 2024

Moon, A. 2019. State sponsored cyberattacks on banks on the rise. https://www.reuters.com/article/idUSKCN1R32OB/. Date of access: 12 February 2024

Morgan, O.M. 9 Patrick M. Morgan, "Saving face for the sake of deterrence," in Psychology & Deterrence, by Robert Jervis, Richard Ned Lebow, and Janice Gross Stein (eds.), Baltimore, Maryland: Johns Hopkins University Press, 1985.

Morgan, S. 2017. Cybercrime damages $6 Trillion by 2021. Cybersecurity Ventures. https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/ Date of access: 16 June 2021

Muncie, J., Talbot, D. & Walters, R. 2010. *Crime: Local and Global.* UK: Willan Publishing

Muncaster, P. 2018. McAfee: Global Cybercrime Costs Hit $600bn. https://www.infosecurity-magazine.com/news/mcafee-global-cybercrime-costs-hit/ Date of access: 09 August 2020

Munda, C. 2019. Rising cybercrime gives banks sleepless nights. Business Daily. https://www.businessdailyafrica.com/corporate/tech/Rising-cybercrime-gives-banks-sleepless-nights/4258474-4980450-t4bgavz/index.html 22 June 2022

Mutune, G. 2023. Top 6 ways how many cybercriminals are caught. CyberExperts. https://cyberexperts.com/how-many-cybercriminals-are-caught/#:~:text=An%20estimated%205%25%20of%20cybercriminals,arrest%20and%20prosecute%20the%20offenders 16 March 2020

Mustaine, E. E., & Tewksbury, R. (2000). Comparing the Lifestyles of Victims, Offenders, and
Victim-Offenders: A Routine Activity Theory Assessment of Similarities and Differences for Criminal Incident Participants. Sociological Focus, 339-362.

Mwai, M.N. 2015. Factors contributing to occurrence of cybercrime on e-banking in commercial banks in Kenya. Thesis.

Nagin, D.S. 1998. Criminal deterrence research at the outset of the twenty-first century. Crime and Justice, 1-42.

Neuman, W.L. 2014. Social Research Methods: Qualitative and Quantitative Approaches. Pearson New International Edition, Edinburgh Gate, Harlow, pp, 1- 594.

Nhlabatsi, S. 2017, November 13. Swaziland loses E40 yearly through cybercrime. *Swazi Observer,* p.3

National Institute of Standards and Technology (NIST). (2018). Framework for improving critical 154 infrastructure cybersecurity.

https://csrc.nist.gov/publications/detail/whitepaper/2018/04/16/cybersecurity-framework-v11/final 02 June 2021

Ohanian, C. 2022. The UN Cybercrime Treaty has a Cybersecurity problem in it. https://www.justsecurity.org/83582/the-un-cybercrime-treaty-has-a-cybersecurity-problem-in-it/ Date of access: 15 February 2024

Nodeland, B., & Belshaw, S., & Saber, M. (2019). Teaching cybersecurity to criminal justice majors. Journal of Criminal Justice Education, 30(1), pp. 71-90.

O'hanley, R. (2013). Information security management handbook. CRC Press; NewYork.

Olayemi, O.J. 2014. Combating the Menace of Cybercrime. International Journal of Computer Science and Mobile Computing, Vol.3 Issue.6, June- 2014, pg. 980-991

O'Leary, Z. 2007. The social science jargon buster: the key terms you need to know. SAGE.

Oliveira, I. & Stickings, A. 2016. Financial Institutions and Cybercrime: Threats, Challenges and Opportunities

Olowu, D. 2009. Cyber-Crimes and the Boundaries of Domestic Legal Responses: Case for an Inclusionary Framework for Africa, *Journal of Information, Law & Technology (JILT),* 1, pp. 1 -18

Okonigene, R.E (2010). Cybercrime in Nigeria. *Business Intelligence Journal*, 93-95.

Oira, 2013. Analyzing and Interpreting Data. https://oira.syr.edu/assessment/assesspp/Analyze.htm Date of access: 5 July 2022

Onchomba, S.N. 2018. The Challenges of cybercrimes in international business operations among commercial banks in Kenya, University of Nairobi, Kenya.

Orji, U. J. 2015. Multilateral Legal responses to Cyber Security in Africa: Any Hope for Effective International cooperation? A paper presented during the 7th International Conference on Cyber Conflict: Architectures in Cyberspace,

Packetlabs, 2021. Cybersecurity threats in banking sector. https://www.packetlabs.net/posts/banking-and-cybersecurity/ Date of access: 06 October 2022

Patton, M.Q. 2002. Qualitative research and evaluation methods, 3rded. Thousand Oaks, CA: SAGE

Paoli, L., Visschers, J., & Verstraete, C. 2018. The impact of cybercrime on businesses: a novel
conceptual framework and its application to Belgium. Crime, Law & Social Change, 70(4), 397–420. https://doi-org.proxy1.ncu.edu/10.1007/s10611-018-9774-y

Payne, B. K (2020). Defining cybercrime. The Palgrave handbook of international cybercrime and cyberdeviance. Palgrave Macmillan. pp. 3–25

Peters, A & Jordan, A. 2020. Countering the Cyber Enforcement Gap: Strengthening Global Capacity on Cybercrime. Third Way. https://www.thirdway.org/report/countering-the-cyber-enforcement-gap-strengthening-global-capacity-on-cybercrime. Date of Access: 19 February 2024

Phil, 2016. Cyber resilience: Part Two Resistance. Black Swan Security. https://blog.blackswansecurity.com/2016/02/cyber-resilience-part-two-resistance/ . Date of Access: 21 February 2024

Pillay, P., Ntuli, P.N & Ehiane, S.O. 2023. Exploring the prevalence of Cybercrime in the Banking Industry in KwaZulu-Natal, South Africa. *International Journal of Membrane Science and Technology, (10), 1,*pp: 1763 - 1775

Plessis, A.G. 2021. Cybersecurity and Governance Framework of Information Systems in the South African Mining Industry. Master's Thesis. University of South Africa.

Polit, F.D. & Beck, C.T. 2012. Nursing research: Principles and methods. 7th edition. Lippincott, Williams Wilkins.

Ponemon Institute. 2016. Cost of Cyber Crime Study & the Risk of Business Innovation. https://saas.hpe.com/sites/default/ files/assets/4AA6-8392ENW.pdf. Date of access: 07 October 2020

Ponterotto, J.G. 2005. Qualitative research in counseling psychology: A primer on research paradigms and philosophy of science. Journal of Counseling Psychology, 52(2):126.

Pratt, T.C., Holtfreter, K. & Reisig, M.D. 2010. Routine Online Activity and Internet Fraud Targeting: Extending the Generality of Routine Activity Theory. *Journal of Research in Crime and Delinquency*, 47(3), pp. 267-296.

Pratt, T. C., Cullen, F.T., Blevins, K.R., Daigle, L.E. & Madensen, T.D. 2006. The Empirical Status of Deterrence Theory: A Meta-Analysis. In F. Cullen, J. Wright & K. Blevins (Eds.), *Taking Stock: The Status of Criminological Theory*. New Brunswick: Transaction Publishers.

Pribanic, E. 2020. 10 ways to prevent insider threats. [Online] Available at: https://www.techfunnel.com/information-technology/10-ways-to-prevent-insider-threats/

Qasaimeh, M., Rand, A.H.,, Muneer, B.Y.,Raad S. A., Juan, A.L.T., & David, L. 2022. Advanced security testing using a cyber-attack forecasting model: A case study of financial institutions. *Journal of Software: Evolution and Process*, *34(11)*

Quarshie, H.O & Odoom, A.M. 2012. Fighting Cybercrime in Africa. *Computer Science and Engineering.* 2(6)

Raghavan, A.R. & Parthiban, L. 2014. The effect of cybercrime on a bank's finances. *International Journal of Current Research and Academic Review,* 2, pp. 173 -178.

Rama, P. 2016. An evaluation of information technology security threats: A case of the University of Johannesburg. (Mini Dissertation). Auckland Park, Johannesburg: University of Johannesburg. Available from: http://hdl.handle.net/10210/237303 Date of access: 04 July 2020

Reciprocity, 2021. What is a cybersecurity framework. https://reciprocity.com/resources/what-is-a-cybersecurity-framework/ Date of access: 21 July 2022

Reyns, B.W. 2013. Online routines and identity theft victimization: Further explaining routine activity theory beyond direct-control offenses. *Journal of Research in Crime and Delinquency*, 50(2), pp.216-238

Reyns, B.W, Henson, B & Fisher, B.S. 2016. Guardians of the Cyber Galaxy: An Empirical and Theoretical Analysis of the Guardianship Concept from Routine Activity Theory as It Applies to Online Forms of Victimization. *Journal of Contemporary Criminal Justice*, *32 (2),* pp: 148 – 168. 10.1177/1043986215621378.

Rogers, M. K., Siegfried, K., & Tidke, K. (2006). Self-reported computer criminal behavior: A psychological analysis. Lafayette: The Digital Forensic Research Conference

Rogers, M. K. 2010. The Psyche of Cybercriminals: A Psycho-Social Perspective. In S. Ghosh, & E. Turrini, Cybercrimes: A Multidisciplinary Analysis (pp. 217–235). Berlin: Springer-Verlag.

Roohparvar, R. 2022. The role of compliance in cybersecurity. https://www.infoguardsecurity.com/the-role-of-compliance-in-cybersecurity/. Date of Access: 02 November 2023

Sabillon, R., Serra-Ruiz, J., & Cavaller, V. 2019. An effective cybersecurity training model to support an organizational awareness program: The Cybersecurity Awareness TRAining Model (CATRAM). A Case Study in Canada. Journal of Cases on Information Technology (JCIT), 21(3), 26-39. https://doi.org/10.4018/JCIT.2019070102

Saleh, N.M & Selamat, S.R. 2022. A review on the criminology theory in understanding cyber violent extremism (Cyber-VE). *Journal of Advanced Computing Technology and Application, 4(1)* pp:67 - 82

Sarannia, A. & Padma, U., R. (2014) Prevention Model for Phishing Attacks In Web Applications Using Linkguard Algorithm. International Journal of Innovative Research in Computer and Communication Engineering Vol.2, Special Issue 1.

Saunders, M.N.K., Lewis, P. & Thornhill, A. 2016. Research methods for business students. Seventh edition.: Pearson Education

Sawaneh, I.A. 2018. Examining the effects and challenges of cybercrime and cybersecurity within the cyberspace of Sierra Leone. *International Journal of Intelligent Information Systems.* 7(3), pp. 23-27.

Schneider, A. 2019. Deterrence Theory in Paraguay: Exploring Fraud and Violation of Trust Cases. *Social Sciences,* 8(23)

Shalaginov, A., Johnsen, J. W. & Franke, K. 2017. Cyber crime investigations in the era of big data. IEEE International conference on big data: 3672-3676, doi:10.1109/BigData.2017.8258362. https://0-ieeexplore-ieee-g .ujlink.uj.ac.za/stamp/stamp.jsp?tp=&arnumber=8258362 Date of access: 23 July 2022

Sharma, A.,K & Nanda, G., L. 2006. Frauds in Credit Card Business. Banking Finance, 7

Siddique, I. & Rehman, S. 2011. Impact of Electronic Crime Sector. *International Journal of Business Information Technology*, 1.

Singh, M.M., Frank, R & Wan Zainon, W.M.N, 2021. Cyber-criminology defense in pervavise environment: A study of cybercrimes in Malaysia. *Bulletin of Electrical Engineering and Informatics,* 10 (2), pp. 1658 – 1668

Sloan, R.H. & Warner, R. (2014). Unauthorised access: The crisis in online privacy and security. NY, USA: CRC Press

Solomon, W.A. 2019. Information security standards and policies compliance by Nigerian Banks. Dissertation. University of Kwazulu-Natal.

Sonepat, R. & Sonepat, S. 2014. Analysis on Credit Card Fraud Detection Methods. International Journal of Computer Trends and Technology (IJCTT) – volume 8 (1)

Staal, F. 2015. Cybercrime and the impact on banks' frontline service employees. Masters. University of Twente.

Saunders, M., Lewis, P. & Thornhill, A. 2009. Research Methods for Business Students. 5th ed. Pearson Education. http://books.google.com/books?id=u-txtfaCFiEC&pgis=1 Date of access: 19 July 2020

Standard Bank, 2017.Standard Bank Group Risk and Capital Management Report 2017. http://annualreport2017.standardbank.com/downloads/Standard_bank_AIR2017_standard_bank_group_risk_and_capital_management_report_2017.pdf Date of access: 19 May 2020

Seth, S. 2023. What is the SWIFT Banking System. https://www.investopedia.com/articles/personal-finance/050515/how-swift-system-works.asp Date of access: 11 November 2023

Scott, M. (n.d.). Social Explanations of Crime. PowerPoint presentation http://slideplayer.com/slide/4533937/ Date of access: 08 July 2020

Shenoy, B. 2019. India PC Market Registers Strong Growth in 2Q19 Driven by ELCOT Shipment, Despite the slowdown in Consumer PC Demand. IDC India Reports.

Shinder, D. 2010. IT Security. *TechRepublic/Tech & Work;* July 19, 2010. http://www.techrepublic.com/blog/it-security/profiling-and-categorizing- cybercriminals/ Date of access: 19 July 2021

Sinca, G.M. 2015. Cybercriminology transition from traditional criminal techniques to cybercrime. *AGORA International Journal of Juridical Sciences, 1,* pp: 62 - 66

Smit, B. 2002. Atlas TI for qualitative data analysis. *Perspectives in Education*, 20 (3).

Smith, T & Stamatakis, N. 2020. Defining cybercrime in terms of Routine Activity and Spatial Distribution: Issues and Concerns. *International Journal of Cyber Criminology*, 14 (2), pp. 433 – 459

Smith, B. & McGannon, K.R. 2017. Developing rigor in qualitative research: problems and opportunities within sport and exercise psychology. *International Review of Sport and Exercise Psychology*, 11(1), pp: 101-121.

Straub, D. W. & Welke, R. J. 1998. Coping with systems risk: Security planning models for management decision making. *Management Information Systems Quarterly,* 22 (4), 441

Strom, B. E. et al., 2017. Finding Cyber Threats with ATT&CK-Based Analytics, ,s.l.: The MITRE Corporation

Swiatkowska, J. 2020. Tackling cybercrime to unleash developing countries' digital potential. The European Cybersecurity Forum – CYBERSEC and AGH University of Science and Technology. https://pathwayscommission.bsg.ox.ac.uk/sites/default/files/2020-01/tackling_cybercrime_to_unleash_developing_countries_digital_potential.pdf.e Date of access: 14 August 2021

Sulfab, M. 2014. Challenges of cybercrime in South Africa. American Military University.

Sun, J.R., Shih, M.L. & Hwang, M.S. 2015. A survey of Digital Evidences Forensics and Cybercrime Investigation Procedure. International Journal of Network Security, 17(4), pp. 497-509

Sussmann, M.A. 1999. 'The Critical Challenges from International High-Tech and Computer-Related Crime at the Millennium', Duke J. of Comp. & Int'l L., 9:451.

Sutherland, E. & Cressey D. 1960. Principles of criminology, sixth edition, Chicago: Lippincott, p. 3.

Swift, 2023. Swift launches the Swift Information Sharing and Analysis Centre. https://www.swift.com/news-events/news/swift-launches-swift-information-sharing-and-analysis-centre Date of access:18 November 2023

Symantec Corporation, 2015. 2016 Internet Security Threat Report, Volume 21. Symantec; April 2016. https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016- en.pdf. Date of access: 19 January 2020

Szentgyorgyi-Siklosi, A. 2023. Cybesecurity challenges in Financial Institutions: How the NIST Framework can help. https://www.lepide.com/blog/nist-framework-for-cybersecurity-challenges-in-financial-institutions/#:~:text=Applying%20the%20NIST%20Framework%20in%20Financial%20Institutions,-The%20NIST%20Framework&text=It%20also%20aids%20in%20GDPR,the%20risk%20of%20data%20compromise. Date of access: 10 February 2023

Szyjka, S. 2012. Understanding research paradigms: Trends in Science Education research. Problems of Education in the 21st Century, 43.

Taddeo, M. 2018. The limits of Deterrence Theory in Cyberspace. *Philosophy and Technology*, 31.

Tan, E.E. 2018. Cyber deterrence in Singapore, Framework and recommendations. (RSIS Working Paper, No. 309). Singapore: Nanyang Technological University.

Taylor, R.W., Fritsch, E.J., Liederbach, J., Saylor, M.R & Tafoya, W.L. 2017. *Cyber crime and cyber terrorism.* 4th ed. Hoboken, NJ: Pearson. http://www.csrc.gov.cn/pub/csrc_en/affairs/AffairsIOSCO/201307/W020130719521960468495.pdf Date of access: 09 July 2021

Thangiah, Basri, S & Sulaiman, S. A framework to detect cybercrime in the virtual environment. *International Conference on Computer & Information Science, pp. 553. - 557*

Thomson Reuters, 2014. Cyber crime: The fast moving menace – a special report. [Online] Available at: https://www.thomsonreuters.com/content/dam/openweb/documents/pdf/governance-risk-compliance/report/cyber-crime-special-report.pdf

Thwala, N. 2019. Central Bank wary of cybercrime. *Swazi Observer*, p.15

Tillyer, M.S. 2011. Routine Activities Theory and Rational Choice Theory, Routledge Handbook of Deviant Behavior, ed. by Clifton D. Bryant, Routledge, New York, NY, pp. 143-149.

Tracy, S.J. 2013. Qualitative Research Methods: Collecting Evidence, Crafting Analysis, Communicating Impact. Wiley-Blackwell, West Sussex, UK.

Tomlinson, K.D. 2016. An examination of Deterrence theory: Where do we stand? https://www.uscourts.gov/sites/default/files/80_3_4_0.pdf Date of access: 16 September 2020

Tropina, T. 2012. The evolving structure of online criminality. How cybercrime is getting organized. Eucrim, 4, pp: 158 - 165

Tropina, T. 2013. Organized Crime in Cyberspace. 10.1515/transcript.9783839424957.47.

Trozze, A., Kamps, J., Akartuna, E., Hetzel, F., Kleinberg, B., Davies, T., & Johnson, S. (2022). Cryptocurrencies and future financial crime. Crime Science, 11(1), pp. 1-35.

Tunggal, A.T. 2023. What is an attack vector? 16 critical examples in 2023.

Ula, M., Ismail, Z., & Sidek, Z. M. 2011. A framework for the governance of information security in banking system. Journal of Information Assurance & Cyber Security, 2011, 1–12

Uddin, M. H., Hakim, A. M. & Hassan, M. K. 2020. Cybersecurity hazards and financial system vulnerability: A synthesis of literature. Risk Management, 22(4), 239-309

UN Institute for Disarmament Research. (2014). Cyber stability seminar 2014: preventing cyber conflict.

United Nations, 2022. Least Developed Countries. Department of Economic and Social Affairs: Economic Analysis. https://www.un.org/development/desa/dpad/least-developed-country-category.html Date of access: 12 February 2022

Uma, M and Padmavathi, G. 2013. A survey on various cyber-attacks and their classification. *International Journal of Network Security*, 15 (1), pp. 390-396.

van de Weijer, S.G., Leukfeldt, R & Bernasco, W. 2019.Determinants of reporting cybercrime: A comparison between identity theft, consumer fraud and hacking. *European Journal of Criminology, (16) 4,* pp: 486 – 508, https://doi.org/10.1177%2F1477370818773610

Van Ommeren, E., Borrett, M. & Kuivenhoven, M. 2014. Staying ahead in the Cyber Security Game: What matters Now.

Varga, G. 2020. Global Cybercrime Report: Which countries are most at risk? https://seon.io/resources/global-cybercrime-report/ Date of access: 16 May 2022

Vasylenko, O. 2012. Problem of cybercrime in Ukraine: Spread of, specific nature and methods of fighting. *Internal Security,* pp. 153 - 162.

Veiga, A., Loock, M & Renaud, K. 2021. Cyber4Dev-Q: Calibrating cyber awareness in the developing country context. *The Electronic Journal of Information Systems in Developing Countries, pp. 1 – 19*

Vez, J.L. 2017. Guidance on Public-Private Information Sharing against cybercrime. World Economic Forum. https://www3.weforum.org/docs/WEF_Guidance_Cybercrime_report_2017.pdf Date of access: 19 May 2020

Venables A (2021) Modelling Cyberspace to Determine Cybersecurity Training Requirements. Front. Educ. 6:768037. doi: 10.3389/feduc.2021.768037

Vrancianu, M. & Popa, L.A. 2010. Considerations Regarding the Security and Protection of E-Banking Services Consumers Interests. *The Amfiteatru Economic Journal* 1228: pp.388-403

Yaseen, Q. (2016). *Insider threat in banking systems.* 10.4018/978-1-5225-0864-9.ch013.

Yesmen, N & Ahmed, N. 2022. The nature and challenges of cyber policing: A study on criminal investigation department (CID), Dhaka, Bangladesh. *Asian Journal of Sociological Research, 5(1)* pp: 210 - 214

Wada, F. & Odulaja, G.O. 2012. Assessing Cyber Crime and its Impact on E-Banking in Nigeria Using Social Theories. *African Journal of Computing & ICT*, 5, pp.69-82

Wagner, T.D., Mahbub, K., Palomar, E & Adballah, A.E. 2019. Cyber threat intelligence sharing: Survey and research directions. https://www.sciencedirect.com/science/article/abs/pii/S016740481830467X. Date of access: 03 Nov 2023

Wall, D.S. 2007. Cybercrime: The transformation of crime in the Information Age. Polity Press. Cambridge.UK

Wall, D.S. 2012. The devil drives a lada: the social construction of hackers as cybercriminals. The Construction of Crime, 4–18.

Wani, M. 2017. The impact of context collapse and privacy on social network site disclosures. Journal of Broadcasting and Electronic Media, 56, 451–470.

Weber, R. 2004. The Rhetoric of Positivism versus Intepretivism: A personal View. MIS Quarterly Vol. 28 No 1, pp. iii-xii/

Whitman, M.E. 2004. In defence of the realm: *Understanding the threats to information security. International Journal of Information Management* 24(1), pp 43 – 57

Williams, M. L. 2015. Guardians upon high: An application of routine activities theory to online identity theft in Europe at the country and individual level. British Journal of Criminology, 56(1), 21-48

Wint, A (2003), Competitiveness in Small Developing Economies, UWI Press, Kingston.

Winit-Watjana, W. 2016. Research philosophy in pharmacy practice: necessity and relevance. The International Journal of Pharmacy Practice, 24(6):428-436.

Wu, L., Peng, Q., & Lemke, M. (2023). Research trends in cybercrime and cybersecurity: A review based on Web of Science core collection database. International Journal of Cybersecurity Intelligence and Cybercrime, 6(1), pp. 5-28.

Yar, M. (2005). The novelty of 'Cybercrime' an assessment in light of routine activity theory. European Journal of Criminology, 2(4), pp: 407-427.

Yin, R.K. 2009. How to do better case studies. The SAGE handbook of applied social research methods, 2, pp.254-282.

Yin, R.K. 2013. Case study research: Design and methods. Sage publications.

ANNEXURE A: ETHICAL APPROVAL LETTER

NORTH-WEST UNIVERSITY
YUNIBESITI YA BOKONE-BOPHIRIMA
NOORDWES-UNIVERSITEIT

Private Bag X6001, Potchefstroom
South Africa 2520

Tel: 018 299-1111/2222
Web: http://www.nwu.ac.za

Economic and Management Sciences Research
Ethics Committee (EMS-REC)

25 November 2020

Prof A Pelser,
Per e-mail
Dear Prof Pelser,

EMS-REC FEEDBACK: 20112020
Student: Howe, EL (32484186)(NWU-00691-20-A4)
Applicant: Prof A Pelser – PhD in Business Administration

Your ethics application on, *A conceptualized cybercrime framework for a developing country: A case of the Kingdom of Eswatini,* which served on the EMS-REC meeting of 20 November 2020, refers.

Outcome:

Approved as a minimal risk study. A number **NWU-00691-20-A4** is given for one year of ethics clearance.

Due to the Covid-19 lock down ethics clearance for applications that involve data collection or any form of contact with participants are subject to the restrictions imposed by the South African government.

Kind regards,

Mark Rathbone

Digitally signed by Mark Rathbone
DN: cn=Mark Rathbone, o=North-West University, ou=Business management, email=mark.rathbone@nwu.ac.za, c=ZA
Date: 2020.11.26 06:32:10 +02'00'

Prof Mark Rathbone
Chairperson: Economic and Management Sciences Research Ethics Committee (EMS-REC)

ANNEXURE B: LANGUAGE EDITING CERTIFICATE

4488 Motswetswejane Crescent

Unit 13

Mmabatho

Mafikeng

2735

26 November 2023

TO WHOM IT MAY CONCERN

CERTIFICATE OF EDITING

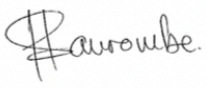
I, Hazvineyi A. Saurombe, confirm and certify that I have read, and language edited the entire thesis titled: ***Developing a cybercrime framework for a developing country: A case of Eswatini***, by Emmanuel L. Howe, Student number: 32484186.

This thesis was submitted for the degree Doctor of Philosophy in Business Management at the North-West University.

Emmanuel L. Howe was supervised by Professor Anna-Marie Pelser.

The views and research procedures detailed and expressed in this thesis remain those of the student.

Yours sincerely,



Dr H. A. Saurombe

0840290454

ANNEXURE C: INDUSTRY EXPERT INFORMATION AND CONSENT FORM

Private Bag X6001, Potchefstroom
South Africa 2520
Tel: 018 299-1111/2222
Web: http://www.nwu.ac.za

Faculty of Economics and management sciences

Researchers: Emmanuel L. Howe

Tel: +268 76443038
Email: lunile.howe@gmail.com

Date: 25 February 2020

Dear Industry Expert

RESEARCH ON CYBERCRIME ACTIVITIES IN ESWATINI BANKS

You are herewith invited to partake in an interview as part of my PhD research project at the North-West University (NWU). In this research, we are interested in your knowledge in understanding cybercrime activities in Eswatini Banks. It will take you approximately 30 to 45 minutes to complete the exercise. We can assure you that all the information we receive will remain confidential. Please note that the responses from each individual will not be identified, but rather the results of the group as a whole will be used in this study.

Please answer all questions as accurately and honestly as possible. Once you have completed the interview, the researcher will analyse the data, and the summary findings will be presented to participating institutions, and we will work with them on how to respond to the results. In this way, your contribution to the research could benefit you and your colleagues in the future.

It is important that you understand that it will not be to your disadvantage if you choose not to participate. Participating is completely voluntary and you can withdraw from the study at any time. If you are comfortable with the content and meaning and you have no objections, please complete the attached questionnaire. *By completing this interview, you give consent that this information may be used for research purposes.*

If you have any queries that we have not addressed and would like to discuss these with us, please do not hesitate to contact us.

Yours faithfully

Emmanuel L. Howe
Primary researcher
North-West University
(+268) 76443038
lungile.howe@gmail.com

Prof Anna-Marie Pelser
Study supervisor
North-West University
+27 82 375 6636
Anna.Pelser@nwu.ac.za

ANNEXURE D: INTERVIEW GUIDE

INTERVIEW PROTOCOL

Interview time:	
Place (location):	
Interviewer:	Emmanuel L. Howe
Interviewee:	
Designation of interviewees:	

Project description: This study sought to explore and analyse the cybercrime phenomenon and lead to provide measures that the Kingdom of Eswatini banks can adopt to minimise their risk and exposure to cybercrime.

Company Profile

1. Which banking services are mostly accessed by your clients?
2. Of those mentioned banking services, which ones do you think are mostly vulnerable to cybercrime?
3. Does the bank have policies and guidelines addressing Cybercrime?

Personnel

1. How long have you been in this position?
2. What qualifications do you possess?
3. Do you feel you are equipped to address cybercrime issues in your position?

Factors influencing cybercriminal activity

1. Does the bank have a cybersecurity strategy? If yes, how is it implemented?
2. Who is responsible for the development and implementation of the cybersecurity strategy?
3. Is there a unit or department in your organisation that deals with cybercrime issues?
4. What approach does your organisation use to address cybercrime?
5. Are there any monitoring and reporting mechanisms on cybercrime activities?
6. Does your organisation have tools and systems to detect cybercriminal activities? If yes, how does the detection work?
7. What is the overall understanding of cybercrime in your organisation especially with your clients?
8. Is cybercrime management in your organisation proactive, preventative or detection approach based?
9. Do you think the size of the organisation, management support and level of IT experience influence cyber-criminal activities
10. What are the most common mechanisms cybercriminals use to perpetuate cybercrime?
11. Based on the trends of cybercrime activity, what is management's perception of cybercrime in your organisation?

Cybercrime encounter activity

1. Have you come across any cybercrime activity during your occupation?
2. If yes, how did you respond to it?
3. Do you think that cybercrime is conducted by insiders, disgruntled ex-employees or cybercriminals?
4. What are the conviction rates for cybercriminal activities in your organisation?
5. Which is the most common loss due to cybercrime for your organisation?
6. What other factors do you think lead to cybercriminal activities in your organisation?

ANNEXURE E: VIRTUAL GUEST LECTURE POSTER



ANNEXURE F: LETTER OF APPRECIATION

MCA

NEW HORIZON COLLEGE OF ENGINEERING

Autonomous College, Permanently Affiliated to VTU, Approved by AICTE & UGC
Accredited by NAAC with 'A' Grade, Accredited by NBA
The Trust is a recipient of prestigious Rajyotsava State Award 2012 conferred by Government of Karnataka

Date: 16-05-2022

To

Mr. Emmanuel L. Howe
Senior Lecturer, Faculty of Computing
Botho University (eSwatini Campus)
Botswana

Letter of Appreciation

Dear Mr. Emmanuel L. Howe,

It is a great pleasure to extend appreciation and gratitude for your effortful participation as an Expert Speaker from a Foreign University, in the Teaching-Learning process of the Department of MCA, New Horizon College of Engineering, Bengaluru, India. The session entitled "**Preventing Cybercrimes in Financial Institutions"** delivered by you on the 06th of May 2022, was remarkable and raised curiosity amongst the participants for further learning in the field.

I thank your parent institution for facilitating this collaboration. We look forward to your intellectual association in the future too.

Wishing you all the best in your future endeavors.

Principal
New Horizon College of Engineering
Ring Road, Bellandur Post,
Bangalore - 560 103

Principal
New Horizon College of Engineering
Bengaluru, Karnataka, India

ANNEXURE G: TURNITIN REPORT SUMMARY

Emmanuel_Howe_PhD_Thesis_2023.docx

ORIGINALITY REPORT

18%	16%	3%	7%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	ensovoort.com Internet Source	3%
2	Submitted to Pathfinder Enterprises Student Paper	2%
3	www.researchgate.net Internet Source	2%
4	repository.nwu.ac.za Internet Source	1%
5	core.ac.uk Internet Source	1%
6	uir.unisa.ac.za Internet Source	1%
7	docs.neu.edu.tr Internet Source	1%
8	researchspace.ukzn.ac.za Internet Source	1%
9	ir.nust.na Internet Source	<1%

	Publication	
138	Muhammad Shoukat Malik, Urooj Islam. "Cybercrime: an emerging threat to the banking sector of Pakistan", Journal of Financial Crime, 2019 Publication	<1 %
139	Pierre-Luc Pomerleau, David L. Lowery. "Chapter 4 The Evolution of the Threats to Canadian Financial Institutions, the Actual State of Public and Private Partnerships in Canada", Springer Science and Business Media LLC, 2020 Publication	<1 %
140	Qussai Yaseen. "chapter 13 Insider Threat in Banking Systems", IGI Global, 2017 Publication	<1 %

Exclude quotes	On	Exclude matches	Off
Exclude bibliography	On		