Analysis of Cybercrime Activity: Perceptions from a South African Financial Bank

A

Research Report

By

Akwasi Obeng-Adjei

0202802J

MASTERS IN COMMERCE (INFORMATION SYSTEMS)

Research report submitted to the School of Economic and Business Sciences, University of the Witwatersrand in partial fulfilment of the requirements for the degree of Master of Commerce (Information Systems) by coursework and research.

Supervisor: Prof Ray M Kekwaletswe

28 February 2017

ABSTRACT

This study is informed by very little empirical research in the field of cybercrime and specifically in the context of South African banks. The study bridges this gap in knowledge by analyzing the cybercrime phenomenon from the perspective of a South African bank. It also provides a sound basis for conducting future studies using a different perspective. In order to achieve this, an interpretive research approach was adopted using a case study in one of the biggest banks in South Africa where cybercrime is currently a topical issue and one that is receiving attention from senior management. Cohen and Felson (1979) Routine Activity Theory was used as a theoretical lens to formulate a conceptual framework which informed the data collection, analysis and synthesis of cybercrime in the selected bank. Primary data was obtained via semi-structured interviews. Secondary data was also obtained which allowed for data triangulation. From the perspective of a South African bank, the study concluded that weak security and access controls, poor awareness and user education, prevalent use of the internet, low conviction rates and perceived material gain are the major factors that lead to cybercriminal activity. In order to curb the ever increasing rate of cybercrime, South African banking institutions should consider implementing stronger security and access controls to safeguard customer information, increase user awareness and education, implement effective systems and processes and actively participate in industry wide focus groups. The transnational nature of cybercrime places an onus on all banks in South Africa and other countries to collaborate and define a joint effort to combat the increasing exposure to cybercriminal activity. The use of the Routine Activity Theory provided an avenue to study the cybercrime phenomenon through a different theoretical lens and aided a holistic understanding of the trends and the behavioral attributes contributing to cybercriminal activity that can help South African banks model practical solutions to proactively combat the splurge of cybercrime.

Keywords: *Cybercrime, internet, crime, computer networks, Routine Activity Theory, South African banks.*

DECLARATION

I have read and understood the Senate Policy on Plagiarism

I understand that plagiarism is the "failure to acknowledge the ideas or writing of another" or "presentation of the ideas or writing of another as one's own" - whether such failure to acknowledge the ideas or writings of others is intentional or unintentional.

I understand what is expected of me in terms of referencing style and how to appropriately acknowledge the ideas or writing of others.

I am aware of the consequences of plagiarism.

_____
Akwasi Obeng-Adjei

_____day of_____ 2017

ACKNOWLEDGEMENT

The completion of this research report was made possible with the contribution of the following people:

- Prof Ray M Kekwaletswe (Supervisor) for the guidance and direction without which the completion of this research would not have been possible.
- My wife, Dr. Foriwah Obeng-Adjei and my two lovely children for the constant love, encouragement and understanding for the times I had to spend away from them to focus my energy on this research report.
- My line manager, Amanda Hoosen for her support in times when I had to take leave in the middle of busy periods to perform fieldwork. Her support was consistent and I am grateful.
- My father, Mr. Alex Adjei who called me almost every second day to obtain feedback on progress for the entire duration of study. His constant reminder and encouragement was a great source of strength.
- Pravitha Flockhart for opening her door to me at all times and referring me to the right people in the organisation to conduct the interviews.
- All the participants who made themselves available to partake in the interview.

TABLE OF CONTENT

CHAPTER 1 7

INTRODUCTION AND BACKGROUND 7

1.1 Introduction to the Field of Study 7

1.2 Background to the Research Problem 8

1.2.1 Cybercrime and South African Banks 9

1.3 Study Location and Context 10

1.4 Problem Statement 11

1.5 Goals and Objectives 12

1.6 Research Questions 12

1.6.1 Primary Research Question 12

1.6.2 Secondary Research Questions 12

1.7 Delineation 12

1.8 Research Contributions 13

1.8.1 Theoretical Contribution 13

1.8.2 Practical Contribution 13

1.9 Summary of the Chapter 14

CHAPTER 2 15

SURVEY OF SCHOLARSHIP AND THE THEORETICAL FRAMEWORK 15

2.1 Survey of Scholarship 15

2.1.1 Cybercrime 15

2.1.2 Types of Cybercrime 16

2.1.3 South Africa and the Global View on Cybercrime Activity 17

2.1.4 The Role of the Internet in Cybercriminal Activities 18

2.2 Theoretical Framework 19

2.3 Theory Underpinning the Study 20

2.3.1 Introduction 20

2.3.2 Application of the Routine Activity Theory 21

2.3.3 Contrasting Routine Activity Theory with Existing Social Science Theories 23

2.4 Conceptual Research Framework 25

2.5 Summary of the Chapter 27

CHAPTER 3 28

RESEARCH METHODOLOGY 28

3.1 Introduction 28

3.2 Research Approach 28
3.3 Research Paradigm 29
3.3.1 Positivist Research 29
3.3.2 Interpretive Research 30
3.3.3 Justification for Interpretive Research Selection 31
3.4 Research Strategy 32
3.4.1 Case Study 33
3.4.2 Justification for Case Study Selection 33
3.4.3 Disadvantages of a Case Study Research 35
3.5 Research Design 36
3.5.1 Unit of Analysis 36
3.5.2 Population and Sampling 36
3.6 Summary of the Chapter 45
CHAPTER 4 47
DATA ANALYSIS AND DISCUSSION **47**
4.1 Introduction 47
4.2 Analysis of Qualitative Data Used 47
4.3 Summary of the Chapter 61
CHAPTER 5 63
INTERPRETATION OF RESULTS AND THE CONCEPTUAL FRAMEWORK 63
5.1 Introduction 63
5.2 Causes of Cybercrime Construct 63
5.3 Revised Conceptual Framework 70
5.4 Summary of the Chapter 70
CHAPTER 6 73
VALUATION OF THE RESEARCH AND CONCLUSION 73
6.1 Introduction 73
6.2 Overview of Chapters 73
6.3 Research Questions 74
6.4 Study Limitations 77
6.5 Recommendations for Future Research 78
REFERENCES 79
APPENDIX A: Ethics Clearance 85
APPENDIX B: Interview Questions 86

CHAPTER 1

INTRODUCTION AND BACKGROUND

1.1 Introduction to the Field of Study

Using the Routine Activity Theory, this study explored and described the factors that influence cybercriminal activity in a South African bank and provided recommendations on how South African banks can minimise cybercriminal activity. In order to achieve this, interpretivist research paradigm through qualitative research methods was used. The Electronic Communications and Transactions Act (ECT) of 2002 define cybercrime as the "unauthorized access to, interception or interference with data, computer-related extortion, fraud or forgery, attempt, aiding and abetting cybercrime". According to Swenson (2011), cybercrime includes a wide variety of illicit criminal activities and includes activities performed by individuals whereby the target or the tool used to perpetuate the crime is a computer system or sometimes both. According to this author, there are two categories of cybercrime. The first one includes a scenario whereby a computer network attacks other computer networks and the second one is whereby a computer network attacks a larger population. Examples of cybercriminal activities include identify theft, phishing, denial of service, hacking, piracy and Card Not Present (CNP). Thomas and Loader (2000:3) provides a commercially sound definition of cybercrime wherein the authors posits that cybercrimes are computer related activities which are illicit in nature and performed using computer mediated resources through global networks. This definition tends to indicate that cybercrime is performed in a virtual environment and the modus operandi introduces complexity in terms of how organisations manage cybercrime. The virtual environment is often referred to as cyberspace. The cyberspace includes the interconnection of computers in a world-wide networked architecture (Castells 2002:177).

In the past few years, statistics indicate that cybercrime is on the ascendency in South Africa and taking place using different mechanisms and channels (Spyridon, 2012). The focus of this study will therefore be limited to cybercrime in a South African bank. The existence of the internet has revolutionized the way we interact and the mechanisms that we employ to achieve certain desired outcomes in our daily lives. Through its use, one can practically perform multiple

activities such as shopping, banking and interacting using social media without having to physically leave a particular location (Newman & Clarke, 2003). When the internet was invented, the thought process was to make human life easier and much attention was not given to the possibility that it will soon be misused for purposes other than what it was intended (Newman & Clarke, 2003). The proliferation of the internet also presents challenges in the form of cybercriminal activities and other forms of illicit online activities which would not have easily existed. This is further exacerbated by the remote ability of these criminal acts to take place under disguise by concealing their identity. According to Wall (2007), there is a link between technology and crime. In the authors' critical exploration of the transformational activities that have taken place, he posits that cybercriminal activities are harmful activities that are global, networked and informational in nature. Knowledge about cybercrime is often misconstrued and various crimes are mistakenly categorized as cybercrime due to the lack of knowledge about the characteristics and features of cybercrime. This is opined by Levi (2001) in which he states "the normal disciplines by which we evaluate the plausibility of threat levels are absent".

1.2 Background to the Research Problem

Researchers have attempted to explain how changes in routine activities were linked to crime trends over time. To explain this, Cohen and Felson (1979) performed research in 1960 to explain why crime rate was on the high when economic activity had improved. The authors concluded that dispersion in human activity away from their homes caused the increase in crime in that as people moved away from their household, the concept of guardianship became less practical and subjected their homes to becoming suitable targets for crime to take place. Extending this theory to cybercrime, it can closely be associated with the virtuality of the internet and computer systems over which these crimes take place. Wilcox et al. (2004) argue that by virtue of the routine activities that an individual performs, they may be placed closer to the potential offender for a possible attack. Its applicability to online activities may pose a question as cybercrime takes place away from the offender. Whilst it can be argued that proximity is not a greater factor in cybercrime activity, the nature of the routine activity being performed places the individual at risk of victimization.

1.2.1 Cybercrime and South African Banks

According to the 2014 South African Banking Risk Information Centre (SABRIC) report, 75% of fraud that took place in South African banks was attributed to cybercrime schemes. Cybercrime makes use of the internet as a primary channel for fraud which is considered to be cybercrime because it is performed in the spatial realm. South African banks continue to be at the receiving end of cybercriminal activities and from the statistics above, the trend seems to be on the ascendency. Literature exists which attempts to shed light on criminal activities and they range from sociology, political and cultural studies, law, criminology and technological studies. The existence of literature from the viewpoints of the disperse disciplines does not however address the social aspects of cybercrime and how cybercrime has evolved and become pervasive in South African banks. Also, very few empirical studies exist to help South African banks curb the splurge of cybercrime activities. Where attempts have been made to draw linkages to cybercrime, conclusions made do not have depth and are not context specific. The attributes of a suitable target, absence of a capable guardian and knowledge of the person as a component of the Routine Activity Theory are characteristics linked to sociological dimensions and therefore generalizing outcomes of research of a study using the Routine Activity Theory weakens the depth and profound understanding of the findings. This study aimed to bridge that gap by providing depth and a profound understanding of cybercrime from the perspective of a South African bank.

Further, most criminologists and academic researchers place much emphasis on the socio-structural domains where cybercrime takes place. Through the use of the Routine Activity Theory as a theoretical lens, the study will demonstrate that an analysis of cybercrime goes beyond the fundamental scope of the socio-structural domains by exploring other plausible domains that account for the increasing spate of cybercrime in South African banks.

Another gap that has been identified and therefore aimed to be filled by this study is that research that relates to this phenomenon has not been conducted in the context of South Africa and more specifically to South African banks, which makes this case study unique. In conclusion, an extensive research on cybercriminal activity exists in a broader scale but very little empirical information exist on factors that lead to cybercriminal activity from the perspective of South African Banks through the theoretical lens of the Routine Activity Theory. It is also unclear as to whether researchers have sufficiently explored the underlying factors of the three elements of the Routine Activity Theory (i.e. absence of capable guardianship, the potential offender and a

suitable target) that lead to fraudulent crimes not performed in the physical time and space (Choo, 2011). In order to address gap in the body of knowledge, this paper explored and described cybercrime from the perspective of a South African bank using the Routine Activity Theory.

1.3 Study Location and Context

BetaBank (pseudonym) is a registered South African Financial Service Provider and offers banking products that range from personal, business, corporate to investment banking. They have presence in South Africa and other African countries. The nature and extent of the services they provide to its circa 9 million customers required that BetaBank identified innovative ways to ensure that customers are able to execute banking transactions without the need to have a face-to-face interaction with customer service agents or rely on a telephonic intervention. This resulted in the design and implementation of online portals to facilitate seamless and systematic processing of transactions. These portals include online banking, mobile and telephone banking.

In mid-2000, BetaBank embarked on a strategic journey to migrate all the traditional banking services to its online portals in order to provide a faster, effective and efficient customer service to its clients. In time, BetaBank began to realise the benefits of their innovation and soon turned this innovation into their customer value proposition. The rapid increase in customer migration onto these portals was indicative of their acceptance and preference for the use of these online portals. BetaBank realized that the proliferation of these online portals was closely and inherently associated with the need to improve security. Soon, BetaBank was inundated with civil and litigation claims for crimes committed using customer bank accounts which were not initiated by the customers.

In 2012, BetaBank senior management initiated and intensified security programs to educate its customers, procure and implement robust fraud detection systems to curb the increasing rate of crimes committed in the spatial realm. Although the result of these initiatives did see significant improvement in the rate of occurrence of cybercrime, these did not stop cybercrime as new forms were emerging. Due to the efficiencies and cost saving, which were imperative for the operational objective of BetaBank, senior management took a decision to continue the use of

these online portals but also implemented additional initiatives to ensure that whilst they adopt security controls to safeguard customer information, they also minimise the financial loss to its customers. In response to this, ex-gratia payments were introduced which meant that for financial losses incurred as a result of cybercriminal activity which were not initiated by the customer, the bank accepted partial or full liability for the loss. BetaBank management is slowly taking steps to adopt a reactive approach to cybercrime within the organisation as management cannot pre-empt the nature and extent of the next criminal activity. The current approach to cybercrime is tactical with the aim to move towards a more strategic solution as the cybercrime phenomenon matures within BetaBank. The cybercrime department comprises of a team of eight consisting of Head of e-Crime, two managers and five specialist support teams. The objective and mandate of this cybercrime business unit is to develop strategies that are aimed at combating cybercriminal activity. BetaBank is part of the South Africa bank-wide e-Crime fraud forum where cybercrime related events are discussed amongst all the major financial banks in South Africa.

1.4 Problem Statement

A number of theories exist in Information System's research, however these theories have not been applied extensively to cybercrime in the context of South African financial institutions. As a result of the lack of extensive empirical research in the field of cybercrime, organisations in South Africa have realised very little success in implementing processes to manage the risks associated with cybercrime. Also this gap in knowledge has resulted in senior management being ill-informed in their efforts to combat the ever increasing rate of cybercrime activity. There is inadequate literature or lack of studies addressing cybercriminal activity especially in the context of South African banks. This study sought to explore and describe the cybercrime phenomenon and conceptualise factors that lead to cybercriminal activity and provide measures South African banks can take to minimise their risk exposure to cybercrime. Having said this, cybercriminal activity in financial institutions is a growing and a real concern both globally and within the South African context making this study research relevant.

1.5 Goals and Objectives

The primary goal and objective of the research was to conceptualise a framework for factors which influence cybercriminal activity in a South African bank.

The secondary objectives of the research were:

- To analyse and describe cybercriminal activity through the lens of the Routine Activity Theory within a South African bank; and
- To recommend how South African banks can minimize cybercrime activity.

1.6 Research Questions

1.6.1 Primary Research Question

RQ1: What are South African banks' perceptions on the factors which influence cybercrime activity?

1.6.2 Secondary Research Questions

RQ2: How does the Routine Activity Theory help analyse and describe cybercrime activity in BetaBank?

RQ3: How can South African banks minimize cybercrime activity?

1.7 Delineation

The study focused on the social context of cybercrime activity and therefore the proposed solutions are merely recommendations South African banks may adopt. Further, the solutions provided in this study are not exhaustive and organisations should consider exploring complimentary solutions in addition to what has been proposed in this research report.

1.8 Research Contributions

A research outcome may contribute to the body of knowledge either in the practical or theoretical dimension. A theoretical contribution infers how the research output influences current thinking. A theoretical contribution may not necessarily imply the generation of a new theory (Corley et al. 2011). Practical contribution mostly implies the applicability of the research to industry and may not necessarily be limited to the Information Systems practice.

1.8.1 Theoretical Contribution

The introductory section of this research indicated that one of the motivations for this research was the minimal empirical study performed in the area of cybercriminal activity and especially in the context of South African banks. This study bridged that gap in knowledge as far as the cybercrime phenomenon is concerned. The use of the Routine Activity Theory also provided an opportunity to study the cybercrime phenomenon through a different theoretical lens. Based on existing literature, there is no other study that has applied this theory to cybercrime in the context of a South African bank. Further, the research output will provide a basis for future studies to be performed to unravel and provide an understanding of the full cycle of cybercrime which will include an attempt to explain individual and collective behaviors (Turner, 2016) that influence the occurrence of cybercrime attacks.

1.8.2 Practical Contribution

For practitioners, a holistic understanding of the trends and the behavioral attributes contributing to cybercriminal activity can help model practical solutions to proactively combat cybercrime activity. The challenge with cybercrime for a practitioner is the dynamic nature of human behavior which is not easily quantifiable in a way that one can easily predict a universal approach to address this gap. By applying the Routine Activity Theory in this research this gap may be bridged as the research outcome will explore and describe the characteristics of a cybercriminal.

1.9 Summary of the Chapter

The study sought to explore and describe factors that lead to cybercrime in a South African bank through the theoretical lens of the Routine Activity Theory and to provide recommendations on ways South African banks can minimise cybercrime activity. The chapter introduced the research report by providing background to the field of study and the landscape of cybercrime in South Africa. The goals and objectives, research questions, delineation and contributions of the field of study to the body of knowledge were also discussed. The next chapters are structured as follows:

- *Chapter 2* – provides a review of literature on cybercrime and the theoretical perspectives of cybercriminal activity in Information Systems literature. The chapter also discusses the Routine Activity Theory which forms the theoretical lens for a conceptual research framework that guides the research.
- *Chapter 3* – This chapter outlines the research design approach which encompasses the philosophical paradigm under which this study is conducted. It also includes aspects of the research strategy and techniques that were used in this study. Also included in this section is a conceptual framework based on Cohen and Felson (1979) Routine Activity Theory forms the theoretical basis for data collection and analysis.
- *Chapter 4* – This chapter provides a narration and interpretation of data analysis in the form of themes that emerged from the conceptual research framework.
- *Chapter 5* – Following from chapter 4, this chapter provides a synthesis of the research findings in relation to the research questions and literature that this study aimed to address.
- *Chapter 6* – This chapter provides the conclusion to the study, critical review of the findings noted in the study, the limitations of the study and recommendations for future studies regarding this phenomenon.

CHAPTER 2

SURVEY OF SCHOLARSHIP AND THE THEORETICAL FRAMEWORK

This chapter provides the theoretical background underpinning this phenomenon. The layout of this chapter is as follows. Section 2.1 provides an account of the survey of scholarship; Section 2.2 provides an overview of the theoretical framework. The chapter then revisits identified research gaps that this study aims to address and further provides a detailed review regarding these gaps; Section 2.3 provides an overview of the theory underpinning the study by discussing the different elements of the Routine Activity Theory and how this theory supports the conceptual framework and the results of this study and in Section 2.4, the conceptual research framework is formulated based on the theoretical underpinning. Section 2.5 provides a summary to this chapter.

2.1 Survey of Scholarship

This chapter examines the landscape of cybercrime globally and in South Africa. Historically, the life of an ordinary person began with newspaper reading in the morning and generally ended with activities such as bed time reading hard copy books or watching televised programs. In recent years, the first thing most people do when they wake up is to confront world affairs through social media. Information is therefore instantaneous. The internet has aided this real-time access to information. The sections below explore linkages between the internet and cybercrime and highlight the global and South African view of cybercrime.

2.1.1 Cybercrime

In the recent years, cybercrime has being viewed as computer crime by many and generally connotes cybercrime with crimes performed over a computer network. Over the years, the nature of cybercrime has changed significantly with the advancement in technology. The dynamic nature of this crime and the sophistication associated with it makes it increasingly difficult for policy makers and government institutions to implement laws and policies to combat cybercrime. International cooperation and efforts are weakened by the dynamic nature of this crime. Notwithstanding this, there is cooperation from many government agencies and law makers in an attempt to implement laws and policies to combat it (Holt et al., 2015). What is cybercrime?

Walden (2007) views cybercrime as a component of computer crime and argues that for a cybercrime to take place, a computer connection to cyberspace must exist. Hunton (2009) supports this definition of cybercrime and asserts that crime committed through the use of an electronic media involving the cyberspace may be classified as cybercrime. It is important to draw a distinction between computer-assisted and computer focused crimes discussed in section 2.1.4 of this chapter.

2.1.2 Types of Cybercrime

Wall (2001) further classifies cybercrime activity into four distinct categories discussed briefly below:

- *Cyber-trespass:* According to the author, cyber-trespassing involves the act of malicious damage to other people by moving from their territory into others and cites virus attacks and hacking as examples of cyber-trespassing;
- *Cyber-deception and theft:* This is whereby the cybercriminal masquerades the identity of the potential victim in order to conceal their identity. The aim is to steal and these acts of theft normally involve theft of property or money such as credit card fraud, piracy and many other forms of illicit crimes;
- *Cyber-pornography:* This relates to the breach of laws regarding obscenity and indecency. This may involve watching pornographic movies on the internet via various media; and
- *Cyber-violence:* This involves inciting violence in the form of psychological or physical harm to others. Examples include hate speech and cyber stalking.

The subject of cybercrime introduces discourse as it has been fully embedded into our society as a phenomenon that needs to be studied in all its dimensions. According to Wall (2007), a key driver for this discourse is the need to identify and classify what constitutes normal and abnormal behavior in a society that has almost fully embraced technology. This discourse is classified into four domains namely legislative and administrative, academic, expert and popular, emotional or laypersons' discourse. The presence of discourse therefore poses a challenge to evaluate the quality of information as it is subjective and dependent upon which lens we focus our attention on from the perspective of the discourse (Wall, 2007). A hurdle for many researchers attempting to explore or analyse the cybercrime concept is that there has not been a consistent definition of cybercrime and as such formulation studies around this subject matter is done with some level of difficulty (NHTCU/NOP 2002: 3). Wall (2001) echoes these sentiments when the author

comments that policy makers who are charged with tackling cybercrime have not been able to provide a term which has a specific reference to the characteristics of cybercrime.

The ability of cybercrime to happen in the spatial realm away from the target individuals is exacerbated by the inherent features of the computer mediated communication medium which is unconstrained by the normal barriers of physical distance. In the words of Yar (2013), the cyberspace technology acts as a "force multiplier" as it allows persons with little resources the ability to effect significant, often negative, change on a larger population. Complexities regarding cybercrime are further strengthened by the ability of the individual to conceal their identity which is generally far removed from their real world (Turkle, 2011) and thus makes it an increasingly difficult challenge for law enforcement agencies and interested parties seeking to track down offenders. The ability to maintain anonymity through disguise and masquerades permits the unscrupulous to easily engage in cybercrime activities (Joseph, 2003).

2.1.3 South Africa and the Global View on Cybercrime Activity

As a result of the attributes and pervasive nature of cybercrime, the concept is gaining the attention of governments of various countries, policy makers, private and public sector entities. In 2011, the UK government ranked cybercrime as one of the top priorities alongside terrorist attacks and natural disasters and committed £650m over a four year period to fight cybercrime. The UK government has intensified its efforts to fight cybercrime (Rosewarne, 2012). The same trend is seen in major economies such as the USA, China, Japan and several African countries. According to the author, cybercrime is transnational and permeates all domains on the business world. The landscape in South Africa is no different from what is been observed globally.

The South African cabinet enacted the Cyber Security Policy Framework which aimed to address national security threats in South Africa, encourage private and public sector participation in research and development, combat cybercrime and cyber warfare, raise cyber security awareness, review and update existing regulations relating to cyber security, encourage the participation in trusted forums to share information regarding cybercrime, build confidence and trust in the use of information and technology and to develop a cyber-security curriculum.

According to Rosewarne (2012), the proliferation of cybercrime is attributed to two factors which are underpinned by individuals responding to monetary and psychological gains. The

author postulates that the prevalent use of the internet and low penalty imposed on the cybercriminal once convicted are the key drivers for cybercrime proliferation in South Africa.

2.1.4 The Role of the Internet in Cybercriminal Activities

The internet has enabled interactions and interconnection between people and systems. Our daily lives are therefore significantly impacted by the cyberspace through the broadband networks that resides underneath, wireless signals that surrounds us in every aspect of our lives, power grids that light our nation, the artificial intelligence that protects all citizens and their assets and the World Wide Web that seamlessly opens platforms for people to interconnect with one another.

The presence and use of these cyberspace elements makes individual, corporate and countries vulnerable to cybercrime related attacks as the threats to the confidentiality, integrity and availability of information increases. These threats surface using the internet as an important tool to deny access to information, conceal or steal, alter information and the context of the information, change the outlook of the information. The complexities associated with this modus operandi makes cybercrime a difficult risk to manage across many organisations and countries. Organised criminals, syndicates and terrorists are constantly launching attacks against society to achieve their criminal intents.

At this point, it is important to highlight the two primary dimensions of cybercrime. These dimensions are classified into computer-assisted crimes and computer-focused crimes. Computer-assisted crimes are those crimes committed in the cyberspace using the internet as their primary tool. Examples of computer assisted crimes include money laundering, theft, fraud, pornography, hate speech to mention but a few. In brief, computer-assisted crimes use the internet and the IT systems as enablers to facilitate the crime. Computer-focused crimes on the other hand are attacks for which an IT system is the target and the crime will not exist aside from it. Examples of computer-focused crimes include hacking and virtual attack (Furnell, 2002). Having provided an explanation for these two dimensions of cybercrime , it is vivid that the distinction between these two types of crimes is the role that technology plays in the execution of the crime. Thus, technology plays a contingent (Computer-assisted) or a necessary (computer-focused) role in defining how a crime is committed (Yar, 2013).

2.2 Theoretical Framework

A theoretical framework gives direction to the research and helps to identify variables that are to be measured, the relationship between them and how these can be modelled to further support the phenomenon under scrutiny (Borgatti, 1999). Theoretical framework provides a foundation to evaluate a focused research area in order to come to a conclusion. Several theories exist and the researcher can apply their judgment in selecting the most suitable theory that compliments the research topic. Some theories that are most commonly applied in the Information Systems discipline are Structuration Theory, Agency Theory, Technology Acceptance Model (TAM), Social Cognitive Theory and the Theory of Planned Behavior amongst others. The ensuing paragraphs briefly explain these theories.

- Structuration Theory: The theory of structuration posits that social acts informs structure, however this structure is not through random individual acts but rather a repetition of these acts (Jones et al., 2008);
- Agency Theory: Agency Theory describes the relationships that exist between principals and agents and presupposes that the principal and the agent act in self-interest. In an organisational context, the Agency Theory explains how best one can organise work such that one party determines the work to be performed whilst the other executes the work (Zsidisin et al., 2003);
- Technology Acceptance Theory (TAM): This theory models how users perceive technology and come to accept its use thereof (Venkatesh et al., 2000);
- Social Cognitive Theory: This theory infers that knowledge can be acquired through observation within the social context (Bandura, 2011); and
- Theory of Planned Behaviour: This theory describes and links beliefs with behavior (Ajzen, 2011).

For the purpose of this research, the Routine Activity Theory (Cohen and Felson, 1979) was used to underpin the study.

2.3 Theory Underpinning the Study

2.3.1 Introduction

The theory underpinning the study is the Routine Activity Theory. This theory was used to analyse cybercrime from the perspective of a South African bank. The Routine Activity theory is an interpretive approach to research derived from the Activity Theory which posits that an activity is a set of general conceptual systems or principles which include the hierarchical structure of activity, internalization/externalization, object-orientedness, tool mediation and development (Kaptelinin et al. 2006)). The Routine Activity Theory assist researchers model how an analysis of the actions of people as they interact amongst themselves or with other objects can lead to a desired outcome. In other words, the theory attempts to explain human behavior when an interaction takes place between the subject and its world. The Routine Activity Theory does not attempt to explain the motivational factors that influence a person to commit crime but rather focuses on identifying series of events that are antecedents to a crime taking place (Spyridon, 2012). The Routine Activity Theory therefore is a theory about crime consisting of events. Kodellas et al. (2015) indicated that crime is a product of intersection of time and space of the potential criminal, suitable targets and the absence of capable guardians. According to the author, Routine Activity Theory permits the exploration of criminal events and allows for the critical examination of these three factors. Prior to the emergence of the Routine Activity Theory in the mid-1980's, many researchers and practitioners could not provide a concise and logical explanation for the disconnect between criminal events. The Routine Activity Theory therefore provides a deeper understanding of how the presence of the three components of this theory facilitates crime. Another aspect to this theory seems to suggest that an activity promotes crime. This is echoed by Schreck et al. (2002) who posit that generally, active members of a community are more susceptible to crime than those who stay at home or are unemployed and not actively engaged in any form of activity. A routine is an antecedent for an activity.

2.3.2 Application of the Routine Activity Theory

The Routine Activity Theory is underpinned by behavioral tendencies and posits that an individual attitude can be studied in-depth to understand their behavior. According to this theory, a researcher can rely on certain measures as long as these measures can be related to the unit of analysis (Spyridon, 2012). Ditsa (2003) summarizes this theory and posits that "The Routine Activity Theory allows the actions of people and the mediating influences on their productive activity to be openly examined. Based on this it can deduced that it is possible to examine a hybrid of traits from sociological and technological aspects of human life (Ditsa, 2003) .

In 1979, Cohen and Felson developed an approach based on the Activity Theory called the Routine Activity Approach and defined that as a social phenomenon which could be applied to understand criminal trends. It is modelled around the premise that a routine set of performing an activity can lead to successful predation. The authors concluded that certain conditions must exist for crime to be committed and named these conditions as comprising of three elements:

- a potential offender;
- a suitable target; and
- the absence of capable guardians.

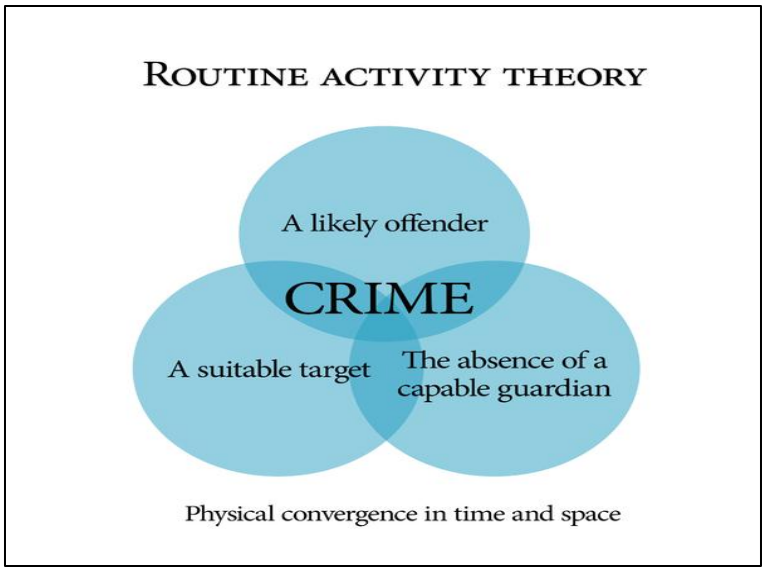


Figure 2.1: The Routine Activity Theory (Choo, 2011)

The authors considers these elements as enough premise for a crime to be committed and suggests that in the absence of these three conditions, crime will not exist, primarily based on the fact that "it is their spatial and temporal convergence that gives rise to opportunity for crime". In sociological terms, Cohen and Felson (1979) argued that crime rate was on the ascendency post

World War II due to societal migration from homes. This they believe led to a higher probability that offenders could converge in space and time to commit crime in the absence of suitable guardianships. Eck et al. (2015) further elaborates that an attempt to resolve crime in one area only shifts the problem to another location. The author argues that these locations are generally not protected. Because criminal activities are not infinite nor spread evenly in a society, the potential offender can only select a maximum number of target objects. The following discussion discusses the three elements of the Routine Activity Theory.

Guardianships

Guardianship is defined as the ability to prevent a perpetrator from causing malicious harm or injury to a person or object (Cohen & Felson, 1979). One can easily draw an analogy between safeguarding a home and safeguarding computer systems against malicious attacks. Studies have found that the propensity for a criminal to target a household with no physical security such as locks and burglar bars is higher than those with little or some degree of physical security (Grabosky & Smith, 2001). Metaphorically, cybercrime does occur due to the absence of physical measures such as antivirus software (Grabosky & Smith, 2001). Another form of guardianship that has been explored is social guardianship and refers to the deterring factors such as presence of a control or the perceived presence of an object with the innate capability to ward off the offender (Coupe & Blake, 2006). An example in the real context points to the idea that a criminal will most likely target a property with no occupant than one where there are people present.

The Potential Offender

In a study by Holt and Bossler (2009), it was established that the probability of being infected or predisposed to a potential offender is higher when one engages in computer deviance activities. In the same study the author concluded that using high speed computers increases a person's chance of being subjected to an online attack due the relative speeds at which remote users can connect, download or install malicious software on computer systems (Hinduja, 2001). According to Cornish et al. (2014), the propensity of an individual to commit crime is often influenced by experiences over time and involvement decisions such that the inclination to commit crime is shaped by positive reinforcement from criminal acts. This they say could lead to

a higher frequency of committing crime. In so saying, they suggest that new associations with peers can intensify continual involvement decisions. The Rational Choice Theory posits that potential offenders carry out risk assessment of the target prior to launching any form of attack. The risk assessment process includes an evaluation of the perceived benefits, costs and risks associated with the criminal activity (Willison and Backhouse, 2006).

A Suitable Target

The use of computer systems presents inherent risk exposures which may materialize in different forms. The suitable target is the object of an attack and can be a computer system, a person or a property (Cohen and Felson, 2001: 43). Research has established that when crime occurs, it is mainly because the perpetrators of the crime connote the wealth of the area with the value of the items within each individual household (Coupe & Blake, 2006). In contrary, all users of the internet are subject to an attack regardless of the geographical location, age, gender, race, economic and social standing (Newman & Clarke, 2003). Cohen and Felson (1979) infer that value, inertia, visibility and access are some qualities of a target and that suitability is a function of at least these qualities. In terms of value, the potential offender may associate a value or perceived value to the target. The relative weight of the target also plays a role in the making the target suitable for an attack in that it makes the attack possible. Also, what is visible is more likely to appeal to a potential offender for a possible attack than abstract or imaginary targets and the ease with which the target is accessible are contributing factors for a target to become suitable. Clarke (1999) applied Cohen and Felson's (1979) work on the principle of a suitable target in a different dimension and concluded that a large number of crimes were as result of a few products which he classified as "hot products" and the attributes are linked to products that are concealable, reliable, available, valuable, enjoyable and disposal.

2.3.3 Contrasting Routine Activity Theory with Existing Social Science Theories

Cybercrime also bears some relationship to the criminological specificity of the Routine Activity Theory by drawing a distinction between dispositional and situational explanation of crime and deviance (Sutherland, 1947). According to the author, Dispositional Theory attempts to shed more light on crime by soliciting causal inferences in a bid to account for why people generally have a desire to break the rule of law. Situational Theory on the other hand is able to reasonably

account for patterns and trends in the activities of the offender (Cohen and Felson, 1979). Through the Routine Activity Theory by Cohen and Felson (1979), explanations for committing law breaking acts are not short of plausible motivations for the crimes committed and cite that crime may be an attribute of social, economic and other structural factors beyond theoretical terrain of the Routine Activity Theory. According to Routine Activity theorists, organisational dynamics in social activities are best suited to account for patterns and trends in criminal activity in which case a study of online activities to establish how this translates into and helps people model their criminal inclination into action is warranted. This calls for an exploration and validation of Cohen and Felson (1979) postulate of the Routine Activity Theory as eccentric components of the criminogenic social situation. Through this, we are able to transpose this proposition to the cyber-spatial context given the clear disparities between the spatial realm and the real world settings. To provide a holistic account of the situational and dispositional attributes which will allow us to draw a clear distinction between the two, we explore emotive and affective disposition which cybercriminals experience when they engage in crime. Bhaskar (2014) describes emotive and affective dispositions as individual responses and commentaries that one makes when they interact with the real world. It is meaningful to highlight the affective disposition is not devoid of rationality. Affective and emotional responses such as fear, panic and excitement are natural reflex responses individuals exhibit when confronted with events in their environment.

The Routine Activity Theory is based on the premise and presupposition that the potential offender's choice on the course of action to take is not restricted and they do so underlined by the expected returns of their choice of action. This mirrors the Rational Choice Theory (Clarke and Felson, 1993) which has a limitation of not being able to accommodate crimes that originate from non-instrumental choices. Whilst the Routine Activity Theory provides a powerful explanation of crime related to property offences (i.e. those crimes linked to economic and material rewards and gain), it does very little in providing considerable explanatory power for expressive crimes such as interpersonal violence (Wilcox et al. 2004). The transposition into the cyber-spatial context is based on the premise of its powerful explanatory power for property offences.

2.4 Conceptual Research Framework

An organization's assets can be protected using different methods against any computer related crimes which are the primary channels used by potential offenders to perpetuate cybercrime. Samonas (2013) argue that in the hierarchy of defenses against cybercrime, people are the first lines of defence to combat cybercrime. The author then concludes in as much as people are the first lines of defence, they are also the main causes of security breaches which results in vulnerabilities that make cybercrime possible to manifest. In some instances these vulnerabilities are created in order to exploit these security weaknesses. Pironti (2013) pointed out that more often than not, organizations focus on implementing controls to combat external threats with little attention given to insider threats. Based on the above theory, a conceptual research framework has is illustrated in Figure 2.2, showing how South African Banks' perception on factors that lead to cybercriminal activity.

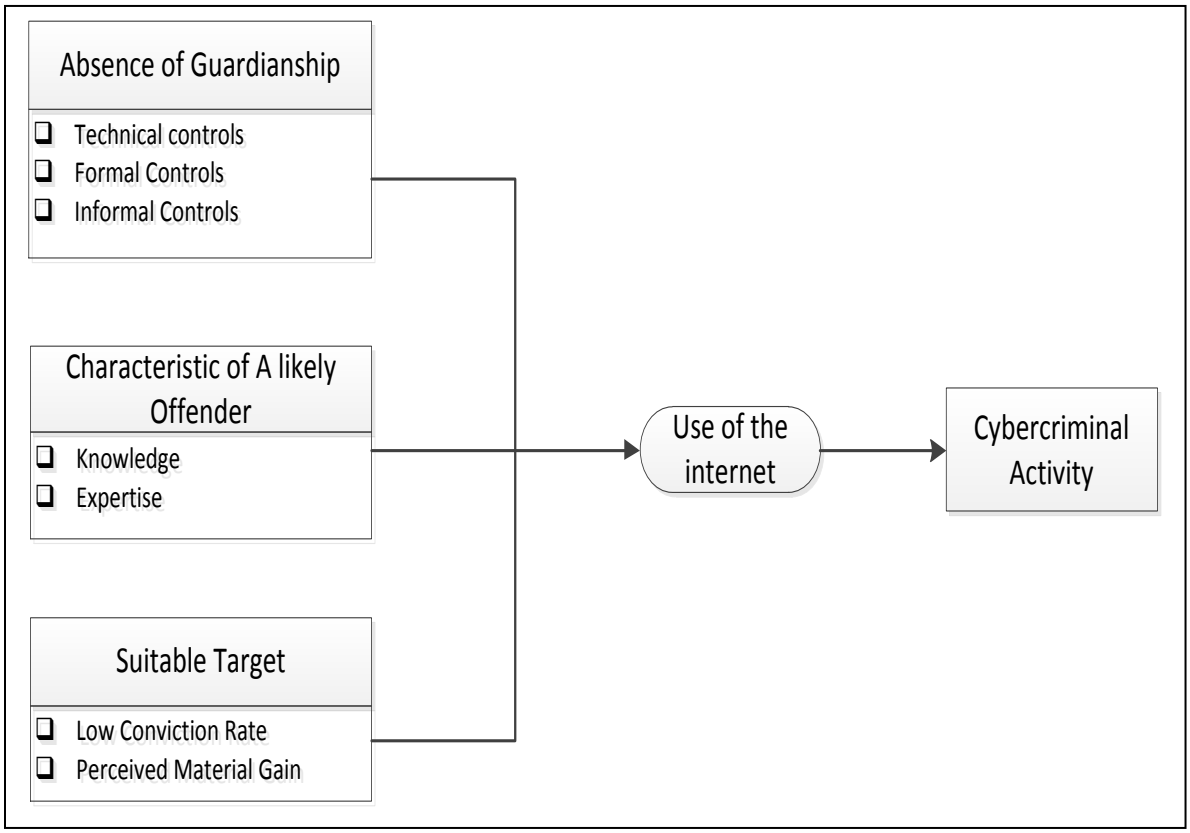


Figure 2.2: Conceptual Research Framework for the Analysis of Cybercrime: Perspective of South African Banks.

Absence of guardianship

Dhillon et al. (2001) draws on the different methods that can be used to protect an organization's assets. According to the author, an organization may opt to apply technical, formal and informal controls to circumvent fraud. Technical controls mainly address access control; formal controls involve the application of rules and are mostly modelled around adherence to corporate policies and procedures, compliance and regulatory requirements. Informal controls are centered on education and how that impacts the culture of an organization towards the implementation of controls to curb cybercrime (Furnell and Thomson, 2009). According to Samonas (2009), technical opportunities to commit cybercrime arise when the rules are relaxed or are applied inconsistently across the computerized systems in an organization.

Potential Offender

The propensity for a potential offender to commit cybercrime is often not only as a result of the standard access rights assigned to the individual but the knowledge/expertise of the potential offender to circumvent the target's access control mechanisms. In a related debate, Probst et al. (2009) argue that when log files have been analyzed for cyber-criminal activities performed, it was often linked to people who have been granted legitimate access. Whilst this may be true, some of these instances could relate to external attacks of perpetrators who have schemed and analyzed the access control gaps within the targets security systems and launched the attack. This argument leads to the question of motive and whether the intention of every criminal activity is preceded by a motive. Probst (2009) noted that motive is usually the leading question during the prosecuting of criminals and further argues that in cybercrime it is not the motive that is questioned but rather the issue of possibility which in most instances is difficult for prosecutors to unravel. Simply reviewing log files may not be sufficient to identify cybercriminal activity as it normally involves a network of other individuals working remotely and from many locations whose identity may not be identifiable by reviewing log files. Added to this complexity is the labor intense effort required to analyze huge amounts of log file data which might not produce meaningful results to detect patterns in behavior of the potential offender. The characteristics of the potential offender are therefore individuals who have knowledge and expertise of the targets asset or IT systems.

Suitable Target

According to Cohen and Felson (2001), a crime takes place when a suitable target has been identified. The choice of the target by the criminal is purely based on appeal, perceived value of the target or the potential returns. This brings to question who the targets are? According to Newman & Clarke (2003), all users of the internet are potential targets be it at the individual or organizational level. Based on the conceptual research framework, the selected unit of analysis is the cybercriminal activity as it the primary phenomenon under scrutiny which will be used to guide the research instrument and the interview schedule.

2.5 Summary of the Chapter

This chapter discussed the theoretical background underpinning the study and also projected a view on a global landscape of cybercrime with a specific focus on South Africa. It sheds light on existing literature regarding cybercrime activity and provided a detailed review regarding gaps identified which resulted in this study being performed.

CHAPTER 3

RESEARCH METHODOLOGY

3.1 Introduction

This chapter outlines the research design approach which encompasses the philosophical paradigm under which this study is conducted. It also includes aspects of the research strategy and techniques that were used in this study. The chapter is laid out as follows. Section 3.2 defines the research approach used, motivation for the selection and justification of why this was chosen over other alternative research strategies; Section 3.3 discusses the research paradigm by contrasting positivist and interpretivist research methods; Section 3.4 outlines the research strategy; Section 3.5 describes the research design approach and Section 3.6 provides a summary of the research methodology.

3.2 Research Approach

Academic research approaches place any research into either a qualitative or quantitative approach.

Qualitative approach to research does not break down an event into quanta for analysis but rather provides a holistic viewpoint of that phenomenon. This is because qualitative research approach aims to provide depth of understanding rather than a statistical analysis of the event or phenomenon (Ary et al, 2010). Based on this assertion, Krauss (2005) states that there is no objectivity reality as qualitative research is based on relative and constructive ontology. In qualitative study the researcher tends to become the primary data collection tool alongside other secondary sources. These primary sources may emanate from interviews, direct observations and stored documents (Brod et al, 2009). In most cases, the researcher is also primarily responsible for the data analysis and fieldwork. The outcome of qualitative research is not driven by statistics or data quantification as qualitative research outcomes may be supported by small samples of which the sample size can be a review of a single case (Creswell, 2013).

Quantitative research methods refer to scientific approach of research wherein the methods employed in the research are organized and are quantifiable (i.e. measurable). The concept is centered on the norms of reductionism which implies the ability to break complex structures into components that are easily understood and analyzed. The sample size in quantitative research is generally much bigger than qualitative studies and employs the use of statistical methods to analyse and synthesize the data obtained (Creswell, 2013). The approach to quantitative research is generally deductive and seeks to test theories, study causal inferences and relationships between concepts (Ary et al, 2010). Whilst qualitative studies takes into account the social and cultural constructs, quantitative studies correlates or factor out these influences (Brod et al, 2009).

3.3 Research Paradigm

For research purposes, there are more than two research paradigms in information systems research. The most prominent of these paradigms are broadly classified as interpretivism and positivism research paradigms. The epistemological and ontological position of these two research paradigms distinguishes one from the other. Whilst the interpretivist position infers that knowledge is interrelated and is subjectively derived, the positivistic view posits that knowledge should be based on scientifically observable facts and devoid of personal value judgments (Walsham, 2006). The following section provides an overview of these two types of research paradigms.

3.3.1 Positivist Research

Positivist research thrives on order and is underpinned by natural sciences which require objective, observable and quantifiable examination of a phenomenon. In positivist research, the researcher does not participate in the research topic and mainly relies on observations as a means of data collection (Livesey, 2006). Positivist research is therefore devoid of bias and influence. Positivists believe that reality is separate from the individual who observes it. The scientific approach is associated with positivist realm of research and attempts to discover and explain real life and social phenomenon, explain patterns and regularities using scientific method. Positivist research is characterized 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 explanations above places positivist research in the quantitative research paradigm. Quantitative research methods refer to scientific approach of research wherein the methods employed in the research are organized and are quantifiable (i.e. measurable). In light of the above definitions and concepts associated with the positivist realm of research, a philosophical dimension of a positivist research projects the view that factual knowledge gained through measurement and observation is considered trusted knowledge (Collins, 2010). Research in the positivist paradigm infers 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 (ibid). Crowther and Lancaster (2008) posits that research in the positivist realm normally follows a deductive approach and is underpinned by objectivity. The objectivity criteria imply that the researcher maintains minimal interaction with the participant throughout the research process (Wilson, 2010). Positivist research therefore relies on manipulative and experimental methods (Creswell et al. 2017).

3.3.2 Interpretive Research

Interpretive research is based on the underlying assumption that social reality is not singular but shaped by our human experiences and social contexts (Livesey, 2006). Interpretivists believe that the natural science approach used by positivist is inadequate to conclude on social phenomenon. In essence, the interpretivists hold the view that people and social constructs are different from the physical realities examined by natural sciences. Because interpretivist research aims to analyze human interactions and the interpretation of such interactions, it employs the use of methods which are not common in the positivist paradigm (Weber, 2004). Interviews and observations are the primary data collection methods in interpretivism research. Interprevitism research methods rely on relative ontology which perceives reality as inter-subjects underpinned by meanings and understandings on social and experimental levels. It also has elements of subjectivist epistemology which simply implies that people and the knowledge they have are inseparable (Bhattacherjee, 2012) and is underpinned by the principle that access to reality is only through social constructions (Myers, 2008). According to the author, interpretivist philosophy is based on the critique of positivism in social science context. As purported earlier, interpretivism is associated with idealism and distances itself from the objectivist notion that

meaning resides in the world independent of our human consciousness. In interpretivist approach, the researcher is the social actor and must be cognizance of the different human traits that exist. The existence of the varying human dynamics requires that research in the interpretivist paradigm employs multiple methods to evaluate the different aspects of the phenomenon under scrutiny.

3.3.3 Justification for Interpretive Research Selection

The aim of the study was to explore and describe factors that lead to cybercriminal activity from the perspective of a South African bank using the theoretical lens of the Routine Activity Theory and provide recommendations on how South African banks can minimise exposure to cybercrime. The study will be based on a single case study of one of the major South African banks. The justifications for selecting interpretivist research paradigm using qualitative research methods are as follows:

- Although the concept of cybercrime is well known in research and literature exists around this phenomenon, very little empirical research data is available on this phenomenon. The qualitative approach will help provide an in-depth and profound understanding on the factors that lead to cybercriminal activity from the perspective of a South African bank using the theoretical lens of the Routine Activity Theory. Research methods that provide deeper and profound understanding of a phenomenon follows the interpretivist research approach (Bowling, 2005);
- This study is context specific and limited to a bank in South Africa. Research in the interpretivist paradigm is appropriate for studying context-specific, unique or idiosyncratic events (Bhattacherjee, 2012);
- Primary data obtained in an interpretivism research tend to have a higher degree of validity as the data in such studies are generally obtained from trustworthy and honest sources (Myers, 2008). The case study was conducted with primary sources who manage the cybercrime activity in BetaBank who have extensive knowledge of the cybercrime activity in the organisation. The ability to corroborate the data obtained with secondary data sources enriched the credibility of the findings and validated the trustworthiness of the interviewees;
- The research approach will rely on a case study of one of the four major banks in South Africa achieved through conducting semi-structured interviews as the primary data

collection method. Qualitative research methods generally adopt a less structured format generally in the form of interviews and participant observations (Livesey, 2006). Using less structured approach provides contextual meaning to questions;

- The objective of the research is to explore and describe the cybercrime concept through the lens of the Routine Activity Theory perspective. Routine Activity Theory is grounded on qualitative methods and is known to be effectively employed in the interpretivist paradigm of research which is the theory of focus in this review (Dista, 2013);
- This goal of this study best suits a deductive study. The goal of a deductive research is to refine or extend a theory and to allow for the emergence of themes out of the data (Bhattacherjee, 2012) The goal of this study is to apply the Routine Activity Theory in a different context for the purposes of extending the Routine Activity Theory in a different context; and
- The shortcomings of a positivist approach in the context of the study objective positions interpretive studies as the best approach for this study in that positivist research is descriptive in nature and lacks insight into in-depth issues (Easterby-Smith et al, 2015). According to Bhattacherjee (2012), the empirical nature of positivist research hinders a researcher's ability to make reasonable inferences about a phenomenon due to the lack of logical reasoning. According to the author, positivist research seeks to test theory which is not generally suitable for interpretative studies which aims to build theories. Further, positivist research develops generalized patterns. This objective places interpretative studies as best suited for this study as it seeks subjective interpretation of social phenomenon.

3.4 Research Strategy

A number of research design approaches exist and include but not limited to experiments, case studies, surveys, ethnography and action research (Bhattacherjee, 2012). Selection of a particular type of research design is underpinned by the philosophical perspective and the nature of the research question one seeks to answer. The ensuing discussion describes case study research and a justification as to why this was selected as opposed to the other alternatives which are equally suitable for qualitative research studies.

3.4.1 Case Study

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). A case study uncovers a wider spectrum of cultural, social and political factors related to the object of study which will otherwise not have been known from the beginning and helps to obtain a deeper and richer contextualization of the phenomenon of interest. This is because the researcher is able to capture a richer array of contextualized information. Case study can be both or one of qualitative and quantitative depending on the research design. Although it can be used in a positivist realm of research, case study research generally conforms better to the rules of an interpretive research. Patton (2005) adds that a case study is best suited for studying complex organizational processes that involve multiple participants and interacting sequence of events. Such is the case with the cybercrime phenomenon.

A case study research may be conducted in order to explore, explain or describe a phenomenon. According to Bhattacherjee (2012), exploratory research seeks to explain an observed phenomenon with the aim of establishing causality. Case studies may be based on a single or multi-sites. The researcher may adopt an approach based upon the context and the objective of the study. A single case provides depth and yields a richer description and understanding of the phenomenon under scrutiny whereas a multi-site case study is best suited for research intended to account for a research area in diverse settings (Lawrence, 2011). The objective of this study was to explore and describe the perceptions of factors influencing cybercrime activity in a South Africa bank. According to (Yin, 2013, p. 47-50), a single case may be considered when the case is unique, revelatory or longitudinal. This is the case with cybercrime hence a case study was suitable.

3.4.2 Justification for Case Study Selection

Researchers collect data about a phenomenon using different techniques. Some of these techniques include participant and direct observations, interviews, protocols, tests and an examination of records. The choice of which method or technique to employ in a particular study is often shaped by the intended outcome of the research. In order to narrow down the options available to a researcher, Glaser (2017) posit that the researcher need to acknowledge and answer questions regarding the nature of the research, whether the phenomenon can be studied in its natural settings, has a well-grounded theoretical base, does the researcher have control and

whether the research is based on contemporary events. Based on the following responses to the questions above, the case study research strategy was adopted:

- Nature of the research: According to Bhattacherjee (2012), case studies are more suited for studying complex social phenomena which are not easily explained using quantitative methods and aims to answer questions such as "how" or "why. The objective of this research was to explore and describe the perceptions of factors influencing cybercrime activity in South Africa banks. Exploratory and descriptive studies are mostly suitable for case study research strategy as it allows for a richer and an in-depth empirical account of a research interest (Eisenhart & Graeber, 2007);
- Context – When research involves a phenomenon holistically and in its natural settings, a case study approach is most appropriate. In addition, case studies support research for which certain variables in the study are not known beforehand (Eisenhart & Graeber, 2007). Because of the qualitative nature of this research, certain variables are not known beforehand and they will emerge through themes during data synthesis. This supports the context above regarding case study research;
- Theoretical Base – A well-grounded theoretical base existed for this study upon which the conceptual framework was developed. The study is based on Cohen and Felson (1979) Routine Activity Theory as the theoretical base to delimit the study;
- Researcher Control – The design of case study research is best placed with studies where the researcher has no control over the phenomenon under scrutiny or aims to control the subjects of the study of how the perceptions of factors influencing cybercrime activity in South Africa banks, the researcher has no personal interest or gain from the outcome of the study and therefore may be viewed as an outsider to the phenomenon. This makes case study design the most suited for this study. Walsham (2006) however warns that because the researcher is seen as outsider to the process, it sometimes introduces some challenges when attempting to obtain data that is classified as sensitive or confidential. This was resolved by identifying alternative sources of data and complementing these with secondary data obtained; and
- Contemporary Events – An important aspect of a case study research is the degree of focus. Due to the evolving nature of cybercrime activity, the study is consistent with the view regarding contemporary events.

The choice of a case study as the preferred research strategy approach was informed by the ability to significantly alleviate most of the deficiencies associated with case study research as

opposed to other alternative research strategies such as action research and ethnographic studies which are also commonly used in qualitative research realms. Ethnographic research requires closer association with the research settings which exposes the researcher to a greater risk of not being totally independent of the opinions expressed (Walsham, 2006). Regarding action research, the objective is to provide quick responses to research problem which will aid a faster turnaround time for resolution. The objective of the research is not to provide solutions but to describe, explore and provide recommendations of the cybercrime phenomenon. These factors weighed in on the selection of case study as the preferred research strategy method.

3.4.3 Disadvantages of a Case Study Research

Case study research has its disadvantages although it is found to have been used extensively in Information Systems research. The first disadvantage is that case studies focus on a particular context and therefore it usually has no scientific basis for generalization (Woodside, 2010). However, the objective of this study is not to generalize the findings using quantitative research approach but rather its aim is to support theoretical propositions which are normally not achieved using statistical methods. Research outcomes aimed at supporting theoretical propositions are better achieved through the use of explicit mental models in a specified domain (Lee and Baskerville, 2003). Also, the dynamic landscape of cybercrime does not support a generalizable trend in that it is constantly shaped by technological advancements and evolution.

Another disadvantage of a case study research is that because it generally takes long to complete, the research output in some instances becomes obsolete at the time of completion (Yin 1994). This limitation was minmised or avoided by defining the boundaries at the start of the research to focus of a particular research and delimit the studies and findings to those boundaries. For this study, Cohen and Felson (1979) Routine Activity Theory was used as the theoretical lens to formulate the conceptual model. In so doing, the boundaries of the research which informed the data collection approach was defined to eliminate the limitations associated with prolonged research investigations. In addition, because the cybercrime phenomenon is an evolving trend in the context of financial institutions, the review was performed at a point in time which eliminates the need to consider multiple domains and dimensions to the phenomenon.

Lastly, case study research is known to result in a biased opinion (Lawrence, 2011). In order to remain objective and not provide any biased views, rigor was introduced into the study by

introducing data triangulation. This involved obtaining research data from multiple sources for analysis in order to strengthen the conclusions derived.

3.5 Research Design

This section provides an overview of the research design method used. The case study research was used to gather the data which was used for analysis and synthesis. The case study research enabled a multi-faceted investigation and thus allowed for an in-depth evaluation of the cybercrime phenomenon. The data collection employed the use of semi-structured face-to-face interviews, media reports on cybercrime and internal reports obtained from Senior Management at BetaBank.

3.5.1 Unit of Analysis

The unit of analysis was the cybercriminal activity as it the primary phenomenon under scrutiny which will be used to guide the research instrument and the interview schedule.

3.5.2 Population and Sampling

The location of this research was in Johannesburg, South Africa as it is the hardest hit city in South Africa for cyber-criminal activity. Statistics produced by SABRIC for 2014 indicate that Gauteng province accounted for 55.5% of cyber related fraud in the South African banking sector. In addition, the head office of the sampled bank for investigation is situated in Johannesburg and cybercrime strategy and its implementation are driven centrally from this location. The study focused primarily on this bank in South Africa as this bank has been one of the biggest victims of cybercriminal activity in the past five years in South Africa as indicated by the SABRIC report. Another criterion for selecting this bank is primarily based on its annual turnover and customer base. The case study focused on one bank as research in the interpretivist paradigm using qualitative research method is concerned with studying a phenomenon in depth within a specific context is aimed at providing a profound understanding of a phenomenon. Therefore selection of one bank was sufficient to provide and deeper and profound understanding of the phenomenon under scrutiny.

Case site selection is generally selected on a random basis. However, Eisenhardt (1989) disagrees with this stance and echoes that randomly selecting a case site is not necessary or preferred and sometimes not the best as in some instances, the researcher may miss an opportunity to select a case site that is best suitable for the research. As a result, a judgmental approach as opposed to a random selection was applied in selection the case site. In applying judgment, consideration was given to ease of access to the case site, participant and the willingness of participant to partake in the research.

The case site is a South African bank with a big footprint in the financial services sector both locally and within the African continent. They provide a range of banking solutions which include retail, business, corporate, investment and wealth management. These products are offered to a diverse range of its customer segment that belongs to different income, age, gender, race and social economic groups. The current customer base is circa 10 million as at 30 April 2015 with a market capitalization of approximately 140 billion. The need to retain its market share and competitive edge requires that BetaBank provides avenues for its customers to seamlessly access products and services and interact with the bank with ease. These sets of competitive edge and customer centric strategic has led BetaBank to use technology to reach these milestones.

Through these technological advancements, BetaBank has been able to provide online facilities in the form of internet banking, Automated Teller Machines (ATMs), mobile banking and various banking applications and tailored these features to suit the different customer segments. Through these channels, BetaBank has experienced a significant increase in revenue growth, introduced efficiencies in the way it serves its customers, greater flexibility to alternative banking solutions and increased market penetration to other markets outside of South Africa. The provision of these services inherently predisposes BetaBank to certain risks such as online fraud, hacking, cybercrime and theft of data which may include customer personal information.

3.5.3 Participants

The key participants interviewed were specialist employees of the Cybercrime division as well as other stakeholders within the bank who have a vested interest in the bank's effort to curb the surge of cybercrime exposure. Particularly, the Head of e-Crime and the Information Security Specialist were interviewed separately aside from the key participants. The table below is the

summary of the participants who partook in the interview and details their role in BetaBank as well as the years of accumulated experience relevant to cybercrime.

Pseudonym	Job Title	Years of Experience
Respondent A	Vice President - Information Security	20
Respondent B	Head: e-Crime	19
Respondent C	Head: Information Security	17
Respondent D	Cybercrime Specialist	9
Respondent E	e-Crime Fraud Specialist	10

Table 3.1 provides a summary of the demographics of the participants

3.5.4 Data Collection Techniques

By virtue of using a case study, there are numerous sources of data that can be collected for a case study. According to Yin (2013), typical sources of case study data collection include documentation, archived records, interviews, direct observation, participant observation and physical artifacts. According to Yin (2013), none of these sources have a relative advantage over the other and suggests that the sources should be used to complement each other.

3.5.4.1 Justification for Selecting Interviews as Data Collection Technique

For the purposes of this study, an interview was deemed appropriate. There are three types of interviews namely structured, semi-structured and unstructured interview. One of the key strengths of interviews is that it provides perceived causal inferences (Gillham, 2000). The study under review aimed to explore and describe a South African Banks' perspective on the factors that lead to cybercriminal activity. Consistent with this reason, interviews will be the primary data collection method for this study. Individual interviews will be conducted and will consist of an interview with the Head of e-Crime Fraud and other specialist teams in the bank under scrutiny. According to Bhattacherjee (2012), multiple methods of data collection should be used as inferences about the phenomenon of interest tend to be detailed and contextualized. Semi-structured interviews were used as it allows each participant the opportunity to elaborate on their views which may result in further probing. In addition, a semi-structured interview was used to respond to structured research questions and to create control. The type of questions posed to the

respondents was based on a priori themes derived from literature. Whilst the researcher stuck to the line of enquiry, the respondents were encouraged to provide context where necessary. Semi-structured interviews support such data collection techniques.

3.5.4.2 The shortfall of Interviews

Interviews present their own unique set of risks. Firstly, the interviewer is seen to be a part of the measurement instrument and sometimes becomes difficult to remove any elements of bias. Other weaknesses associated with interviews are that they are time consuming and resource intense (Bhattacherjee, 2012). To minimize the effect of these weaknesses, thematic analysis and data triangulation (comparing responses by interviewees) were employed.

3.5.5 Data Analysis

Analysing qualitative data may employ the use of hermeneutic analysis, thematic analysis and content analysis (Bhattacherjee, 2012). Hermeneutic analysis and content analysis are more concerned with interpreting subjective meaning of a given text within its socio-historic context. The themes emanating from the data gathering process will form the basis of drawing inferences about cybercrime and therefore thematic analysis will be used for this research as it is concerned with the systematic analysis of the content of the text. Thematic analysis is the most commonly used data analysis method for qualitative research. According to Braun and Clarke (2006), thematic analysis is concerned with recording patterns or themes within data. Themes are patterns across data sets that are important to the description of a phenomenon and are associated with a specific research question. The research design approach uses deductive approach which will be best supported using thematic analysis. Thematic analysis presents its own unique challenges in terms of how validity, credibility, conformability, transferability and dependability are achieved. The discussion that follows explains how these challenges were addressed.

3.5.6 Validity

Validity is concerned with the trustworthiness of the study and provides an assessment of the reliability and validity of the study. According to Golafshani (2003), qualitative study views reliability and validity as the same concepts. In order to achieve reliability and validity,

triangulation of the research was performed. Triangulation is commonly applied in qualitative research and establishes symmetry between different sources of data.

3.5.7 Conformability

Shenton (2004) defines conformability as the ability for other researchers to independently corroborate the results of the study. Conformability infers that the results of the research should be a reflection of the views and opinions of the participants as opposed to the researcher's preference. This relates to the principle of bias and in order to eliminate this aspect, data triangulation was used to relate the different sources of data. To achieve data triangulation case study was extended to multiple role players within BetaBank viz. Information Security Specialists, Fraud Experts, Information Technology Specialists and Ecrime Analysts. The varied data sources helped to achieve data triangulation.

3.5.8 Credibility

A key aspect of any research is the ability to establish credibility of the audience and the conclusions that were derived based on the data collected. In the interpretative research, the researcher must identify and demonstrate the use of evaluation criteria to confirm the credibility of the findings. In order to evaluate the credibility of the audience and the conclusions derived, Klein and Myers' (1999) set of principles for evaluating interpretative research was used as this evaluation criterion is better suited for research conducted in the interpretative paradigm. These principles include "hermeneutics, contextualization, interaction between subjects and researcher, abstraction and generalization, reasoning based on dialogue, suspicion and multiple interpretation. The authors' further states that these principles must be used as a guideline and not to be viewed as a set of mandatory research principles for evaluation of research outcomes. Researcher judgment is therefore required in applying these principles and they may be used at the discretion of the researcher. Klein and Myers' (1999) set of principles for evaluation interpretative research was used as the principles are not mechanistic and the flexibility it introduces allows the researcher to consider other evaluation criteria in conjunction with other proposed models. The figure below explains how these principles were applied in this study.

Klein & Myers (1999) principle for Evaluation	Application in this study
The hermeneutic circle In the context of an interpretivist research, the hermeneutic circle principle requires that the researcher should apply an iterative approach in understanding a phenomenon in parts and their relationships in order to understand the complex whole.	The researcher developed a narrative of the case and divided the research question into parts which formed a theme. These themes were analysed in parts which were then viewed collectively to understand the complex whole.
Contextualization The researcher must provide a historical account so that the reader can have a better understanding of how the current situation came about.	The researcher reviewed secondary data relating to past cybercrime events in order to obtain contextual and historical accounts of the cybercrime activity within the organisation. This was validated with industry data obtained from SABRIC.
Interaction between subjects and researcher The social construct of the data collection must be explained reflecting on the interaction between the participants and the researcher.	The design of the questionnaire was such that it minimized posing questions to the participant that would influence their responses. The questions were posed in a manner that it solicited objective responses from the participants. The researcher eliminated the possibility of channeling the participant's viewpoint into the perspective of the researcher. Secondary data was obtained to support the data obtained from the interviews. The researcher used secondary data and observation in order to complement the raw data from interview transcripts.

Abstraction and generalization This requires the researcher to demonstrate a link between the interpreted data and the underlying theory that describe the nature of human understanding and social action.	The case narrative and interpretation is based on themes developed from the conceptual framework based on the Cohen and Felson (1979) Routine Activity Theory in order to be able to achieve analytical generation and to expedite a theoretical exploration and description of the factors that lead to cybercriminal activity in a South African bank which will subsequently result in recommendations on ways South African banks can minimise exposure to cybercriminal activity.
Dialogical Reasoning The researcher must consider the possibility of contradictions between the conceptual framework and the findings derived from the data analysed.	The researcher took into account the relationship between the suitable target, the absence of suitable guardianship and the offender in order to draw a relationship between the data and the conceptual framework. This allows for an exploration of a possible contradiction between Cohen and Felson (1979) Routine Activity Theory and the findings.
Multiple Interpretations The researcher must take cognizance of how the logical flow of events expressed by the participants may vary.	The selection of the participants took into account the possibility of relaying events differently due to their vested interest and proximity to the cybercriminal concept.
Suspicion The researcher must consider individual bias and possible distortion of the events relayed due to the participants close association with the organisation.	The researcher also took into account the fact that the participants view point may be influenced by their positions in the organisations. To address this, the researcher interviewed people at different levels of management in the organisation.

Figure 3.2 explains the application and interpretation of Klein and Myers' (1999) principles of interpretivist research

3.5.9 Transferability

Transferability refers to the ability to extrapolate the findings of one research to a different setting (Shenton, 2004). In order to achieve this, the researcher needs to understand the context of interpretivist research findings in relation to where it is intended to be transferred to. In order to ensure transferability in this study, the researcher provided a detailed account of the research context by indicating the research location, units of analysis, participant demographics, and the organisation that was selected for the study.

3.5.10 Dependability

Dependability concerns itself with the dynamic context within which the study takes place (Shenton, 2004). In order to ensure dependability, the researcher sought peer reviews and also presented the initial proposal to a group of academics for initial commentary. Dependability was further achieved by performing detailed investigation of the cybercrime phenomenon which was supported by solid theoretical underpinnings, research methodology, data collection and analysis as well interpretation and evaluation of the research findings.

3.5.11 Research Ethics

The study was approved by the Wits University Research Ethics Committee (Non-Medical), Protocol Number: CINFO/1107. The study was done to respond to an academic question in order to bridge a gap in knowledge with no intention to benefit financially or to be incentivised. The study design was such that it does not result in a pre-empted outcome or direct a particular viewpoint with respect to the phenomenon under scrutiny. In order to adhere to confidentiality and anonymity, the name and details of the organization were not mentioned in this review. Where it was necessary to make a reference to the organization, a pseudonym was used.

Informed Consent

Another important principle which was considered as part of the study was the need for the participants to volunteer to participate and they must not have been coerced or pressured to participate. Once information has been provided, the onus lies on the researcher to ensure anonymity in its storage, analysis or reporting. Where confidential information is to be made public, consent should be formally obtained from the people involved (Beauchamp and Childress, 2001). To achieve this, the selected participants were asked to voluntarily participate in the interviews with background about the researcher and the objectives of the research being provided upfront. Those interested were asked to give consent to participate in the interview process. The selected participants were all adults and full-time employees of the organisation which they represent and therefore were not vulnerable in any way.

Right to Privacy

Deception is not always possible to avoid especially in circumstances where it is not possible to inform participants or in instances where knowledge of the research may influence the outcome of the research. However, knowledge of the principle of deception is important where the researcher purposefully set out to deceive the participants. Deception was eliminated from the studies by involving the participants in the development of the questionnaire to align to the research objective. The questionnaire development also ensured that there was no ambiguity in the questions posed and responses were played back to the participants to confirm accuracy. In order to ensure that the right to privacy requirement was applied, it was highlighted to the participants prior to the start of the interview that they have a right to withdraw from the research at any point in time without any recourse. Under this guideline, there were no circumstances where the participants were made to feel pressured to continue with the interview after they had shown intent to withdraw (Davis, 2001). In order to protect the privacy of the participants, each participant had the right not to declare who they are, in other words their responses remained anonymous for the purposes of confidentiality. The responses from the participants were only be used for the purposes of this research and at no stage did the researcher initiate contact to try and bias the responses.

Protection from harm

Commonly referred to as the principle of non-maleficence, the research should not cause discomfort to participant. In many instances, a researcher does not set out to cause harm intentionally to participants. It is more often the risk of harm that a researcher should aim to minimise (Beauchamp and Childress, 2001). Informed consent is underpinned by making sure that the participants understand the nature of the research they are taking part in and what is required of them during the research process (Davis, 2001). The study design was such that it did not cause harm to any of the participants either personally or professionally.

3.6 Summary of the Chapter

This chapter began by providing the choice of philosophical paradigm adopted to guide the research, the research strategy employed to ensure that the outcomes answered the research questions, the techniques used to achieve this and the justification for all these choices made. In the later sections, a discussion regarding the choice of research method, unit of analysis, participant selection, detailed analysis of the conceptual framework and the subsequent data collected and analysed was provided. The research evaluation section followed to explain how the data which supported the results of the research was analysed and evaluated. Lastly, considerations of the research design choices opted for was provided. The ensuing section provides a summarised view of this section.

Research Design Choice	Decision
Research Paradigm	Interpretivism using qualitative methods
Research Strategy	Case study
Unit of Analysis	Cybercrime activity
Participants	Head of e-Crime Strategy, Head of Information Security and their direct specialist teams
Site Selection	Pragmatic – Primarily based on the ease of access to the organisations and the people
Conceptual Framework	Based on Cohen and Felson (1979) Routine Activity Theory
Data Collection	Semi-structured interviews, SABRIC database and research articles
Data Analysis	Iterative model for qualitative data analysis using thematic analysis

Evaluation	Klein & Myers' (1999) principles of evaluating Interpretive research
Ethical Considerations	Ethical research considerations regarding informed consent, right to privacy and protection from harm were adhered to in this research at the start of each interview and were consistently applied across all participant groups

Figure 3.3: Summary of Research Methodology Approach

CHAPTER 4

DATA ANALYSIS AND DISCUSSION

4.1 Introduction

The previous chapters provided an account of the research methodology used for the study. This chapter provides an analysis of the data gathered during the data collection stage. Two separate semi-structured interviews were conducted. The first interview was conducted with the e-Crime department at BetaBank with the Head of e-Crime and Cybercrime Fraud Specialists from the e-Crime and Cybercrime divisions within BetaBank.

4.2 Analysis of Qualitative Data Used

The data was analysed in accordance with the themes and sub-themes. The themes identified in the data analysis mainly related to causes of cybercrime which subsequently informed recommendations on how South African banks can minimise cybercrime activity. The analysis was performed by linking each of these themes to the research objective as follows:

- Theme A explores and describes factors that lead to cybercrime activity in BetaBank – Objective 1 (What are the perceptions of factors influencing cybercrime fraud activity in BetaBank?);
- Theme B analyses the cybercrime activity through the lens of the Routine Activity Theory - Objective 2 (How does the Routine Activity Theory help describe cybercrime activity in BetaBank?); and
- Theme C explores approaches South African banks can adopt to minimise cybercrime attack – Objective 3 (How can South African banks minimize cybercriminal activity?)

In order to relate the themes to the theoretical constructs and the conceptual research model, the data was transcribed and coded. The ensuing discussion details the researcher enquiries and the participants' responses and the researchers deductions based on the responses received.

Theme A: Cybercrime causes – Objective 1 (What are the perceptions of factors influencing cybercrime fraud activity in BetaBank?)

Theme A describes how the question posed to the respondents related to objective 1. The structure of this chapter is such that for each question, the responses from the participants are italised to indicate how their answers influence the question being posed and the researcher's opinion on the responses received.

A_Q1 related to the company profile which did not require further synthesis and analysis.

A_Q2. What is the approach to crime in your company, particularly the approach to cybercrime in your organisation?

"On a real-time basis, we receive alerts for all suspicious online activity performed. We have a functional Operations Team that reacts immediately to these alerts through investigation. Depending on the risk grade of the alert, a time is allotted within which the alert must be closed. We are somewhat between preventative and reactive, but more reactive if I may say so" - Cybercrime Specialist (D).

"We have access to the complaints dashboard and we heavily rely on customer complaints to establish cybercrime related incidents. We sometimes call these customers to follow up on their query. The complaints dashboard assists us in establishing trends that inform our next set of actions to undertake" - Head: e-Crime (B).

BetaBank's approach to cybercrime encompasses ongoing reviews of cybercrime alerts generated through a fraud system. The approach has been rather tactical instead of strategic as it is reliant on the ability of the fraud detection system to identify cybercrime alerts. BetaBank also relies on customer complaints as a means of analyzing cybercrime patterns within the organisation. Based on the analysis and trends established, measures are put in place to mitigate the risks identified. The approach is therefore more detective as opposed to preventative and it is primarily as a result of the dynamic nature of cybercrime and its rapid pace of evolution.

A_Q2 (a). Who defines cybercrime strategy?

"Because the business ultimately owns the risks associated with cybercrime, they are primarily responsible for approving any proposal on cybercrime strategy. Cybercrime strategy is defined by the e-Crime management team in close consultation with specialist support functions such as fraud, digital channels, technology and information security" – Head: e-Crime (B).

The setting of cybercrime strategy is performed internally by accountable business units in collaboration with specialist functions. Although the cybercrime strategy is defined internally, based on historic events and cybercrime risk exposures, the definition of the strategy takes into account external factors such as industry trends peculiar within the market within which BetaBank operates. The Head of e-Crime Strategy manages the process of defining the cybercrime strategy. However, responses from the participants indicate that the cybercrime strategy is discussed and challenged at various forums before approval. These forums include the e-Crime forum, Digital Channels Risk Forum and Control Review Committee.

A_Q2(b). How is the cybercrime strategy implemented once approved?

"The number of business rules built into our fraud detection IT systems is what drives the strategy implementation. These are automated rule sets that kick-in when user activity takes place. These user activities allow us to profiles our customers such that we are able to predict certain behaviours and generate an alert if an activity is outside the normal behavioral pattern of the user. The rules are implemented at a transaction level and are invoked when a customer performs any online transaction"- Vice President – Information Security (A).

According to the respondents, the ability of a functional cybercrime fraud system to detect and/or prevent fraud is directly associated with effectiveness of the fraud detection rules built into these systems. In the context of BetaBank, cybercrime strategies implemented on the fraud systems are designed based on business rules. The business rules are driven by customer behavioral patterns which are then used to predict user activity when they perform online transactions.

A_Q2(c). Is there any monitoring and reporting on cybercrime activities?

Digital channels perform monthly trending of all cybercrime events which include near misses, actual events where the cybercrime has materialised, potential and actual loss incurred as of the cybercrime taking place. In our monthly e-Crime Forum meeting, these stats are discussed to identify possible root causes. Root cause analysis significantly impacts the cybercrime strategy formulation and implementation" – Cybercrime Specialist (D).

"……We also report on our fraud events which include cybercrime events on an ad hoc basis to SABRIC. This is seen as added layer of reporting on our fraud (cybercrime) statistics in order to benchmark against industry occurrence rates. – Head: e-Crime (B)"

According to the respondents, central cybercrime reporting takes daily but these aggregate into monthly reporting which are discussed at the monthly e-Crime forum meeting and also to SABRIC on a periodic basis. This indicates active monitoring of cybercrime activity in BetaBank.

A_Q2(d). Are there any oversight committees to monitor and assess the effectiveness of the cybercrime interventions in the organization?

"We hold monthly e-Crime forum meetings where we discuss the strategy and potential revisions to it based on market trends and cybercrime risk events. The meeting looks at holistic trends in the market and potential impact on BetaBank. There is also the digital and fraud meeting which takes place monthly and has a representation from each of the cybercrime impacted business units. On a monthly and quarterly basis, we have the Digital Risk Forum and Control Review meetings - Head: e-Crime (B)".

Internally, BetaBank has a well vexed oversight committee that monitors and challenges cybercrime activities within the bank. These meetings also reflect on the cybercrime strategy and whether there is the need to revise the strategy taking into account internal and external cybercrime events. This is echoed by another respondent who added that:

".....BetaBank is a member of SABRIC and we meet on a frequent basis. In this meeting, representatives from all the major banks in South Africa are present to discuss the cybercrime

landscape within their respective organisations, report of any cybercrime risk exposures and share learnings with each other" - Cybercrime Specialist (D).

A_Q3. Does your company have tools and systems to detect cybercriminal activity? If so, how does it detect cybercrime?

"BetaBank has a fraud detection system that is rules based. These rules are designed to analyse abnormal customer online behavior in order to detect cybercrime. The design of this system is detective in nature as the rules built into it are not robust to proactively identify and stop a cybercriminal from perpetuating fraud. The internal fraud systems do not really play a role in stopping cybercrime. One thing I can really say is definitely efficiencies you can gain in terms of call centres that may have some impact in stopping cybercrime" Vice President – Information Security (A).

"Our IT architecture is not easily permeable and requires complex scripts and high tech knowledge of network security in order to gain access. Unless the crime is performed by an internal staff member, it is generally difficult for external agents to gain access to these networks - Fraud Specialist – (E)"

"The number of business rules built into our IT systems are aimed at detecting and in some instances preventing cybercrime" - Vice President – Information Security (A).

In addition to the above, the respondents indicated that they have a dedicated Operations Team that responds to alerts (including cybercrime alerts) that are of a suspicious nature. Although the IT architecture and systems are strong enough to prevent a cybercriminal from easily gaining access, they use avenues that do not require access via BetaBank' s network access as they often resort to illegally obtaining other users information to gain access to the online profile. This invalidates the efficacy of the IT network.

"The end result of all cybercriminal attack is to gain access to a customer profile to perform an illicit activity. However, the process is initiated through a compromise of the customer personal information as the criminals find it much easier to attack individuals than IT systems" – Fraud Specialist – (E)

Another respondent agrees with these views and added that internal controls are not easily compromised due to the multiple layers of security introduced into the network.

"Our formal controls are intrinsic and applicable to internal staff members to ensure that they do not circumvent internal controls which might render our IT systems susceptible to cybercriminal attacks. Due to the complex nature of the banking network security, it is not easy for cybercriminals to attack our systems. They mostly go for soft targets being our customers. Our fraud policies, IT policies and procedures, compliance and other regulatory requirements are internal and do not inform our defensive approach to cybercrime. Our defenses are aimed at external forces we do not have a control over" – Cybercrime Specialist (D)

A_Q4. What is the general level of understanding of cybercrime in your organization and with your customers?

"Technical and support staff have a deeper understanding and knowledge of the security risks associated with the use of online transactions. However, the general public do not have the same level of education and awareness regarding cybercriminal activity" – Head - Information Security (C).

"Users' lack of education and awareness is the biggest root cause of cybercriminal activity as people are still clinking on anonymous links and posting their personal information on social media such as Facebook" - Head: e-Crime (B).

"South Africans are susceptible to this kind of fraud like phishing and credit card cloning because generally speaking, people are ignorant about the risks associated with the use of these online facilities. Recent survey indicated that a vast number of customers responded to bogus emails which resulted in their personal information been fraudulently obtained"- Vice President: Information Security (A).

Due to the low levels of user education and awareness, BetaBank is implementing strategies to combat cybercrime which will minimise the need to stringently enforce user education and awareness. In a related response from one the interviewees, he emphasized that the security controls being deployed onto the online platforms are focusing on preventative controls rather than detective.

"We analyse volumes and spikes and have noted that cybercrime is on the high for instances where the customer compromised their personal information and was not aware of what steps should have been taken to prevent the cyber- attack. Our stats also indicate that a high number

of our users have been attacked more than once. This definitely drives our strategic focus in implementing security controls that are preventative" – Cybercrime Specialist (D)

A_Q5. Briefly describe the nature of cybercriminal activities that are pertinent to your organization?

"In the South African context, it is organized cybercrime syndicates and these are syndicates that are actually involved in physical crime like hijackings, theft, ATM bombings who branch out into cybercrime using IT specialist"- Vice President: Information Security (A).

"These criminals are normal guys who know how to defeat our controls. They are thugs who threaten employees from the banks to solicit customer information. In other instances, they rely on syndicates located in Russia who phish our customer information and sell it back to our South African syndicates who in turn use these information to commit cybercrime. Our South African syndicates are not always the brains behind the soliciting of customer information through phishing which is used to perpetuate cybercrimes" – Head: e-Crime (B).

In one instance, we traced the IP (Internet Protocol) address to a prison cell" – Head: e-Crime (B).

From the responses provided, it is apparent that the nature of cybercrime takes place through syndicate groups who operate in different locations around the globe. The landscape of cybercrime is therefore not limited to one geographical domain. It is networked and multi-faceted with different role players involved.

A_Q6. What are the types of crimes performed, by whom, how and when do these crimes take place?

"Besides phishing which is our biggest concern, we also see incidences of online identity theft which is quite prevalent. It is whereby someone purports to be someone else with the intention to commit fraud or benefit financially. We rarely see other forms of cybercrime such as ransomware, DDoS attacks which is used to make the online service available by bombarding it with traffic or ransomware which is a malware-based attack" – Vice President: Information Security (A).

"These criminals are normal guys who know how to defeat our controls. They are thugs who threaten employees from the banks to solicit customer information. In other instances, they rely on syndicates located in Russia who phish our customer information and sell it back to our South African syndicates who in turn use these information to commit cybercrime. Our South African syndicates are not the brains behind the soliciting of customer information through phishing which is used to perpetuate cybercrimes" – Head: e-Crime (B).

"In the south African context, it is organized cybercrime syndicates and these are syndicates that are actually involved in physical crime like hijackings, theft, ATM bombings that branch out into cybercrime using IT specialist - Vice President – Information Security (A).

The respondents all agreed that phishing is their biggest concern as the controls to mitigate against this risk lies with the customer whom the bank can influence to a certain extent through ongoing customer education. Additionally, the respondents indicated that cybercrime is not performed by technical individuals but normal people who solicit information from different sources to commit these crimes. In short, cybercriminals are just criminals who look for loopholes in online banking processes and exploit that to their advantage.

"Statistically, the highest incidence of cybercrime attacks take place during the holiday seasons as most people become less security conscious. For instance, some couples switch off their phones whilst on holidays and therefore are unaware of online notifications informing them of activity on their online account" - Head - Information Security (C).

The responses above and similar from other respondents indicate that cybercrime occurrence rate is highest between December and January of each year followed by other intermittent public holidays. According to one respondent, this trend is the same across all the major banks as they are centrally reported to SABRIC.

A_Q7. What are the most common mechanisms cybercriminals use to perpetuate cybercrime?

"A significant proportion of cybercrime activities take place via phishing. Phishing accounts for a significant proportion of cybercrime activities and involves fraudulently obtaining confidential information from a person such as online username and passwords, banking details and credit

card information. Perpetuators often disguise themselves as a trustworthy source by sending a fake link to a user who unknowingly clicks on the link where their security credentials are compromised" - Cybercrime Specialist (D)

"In our analysis of cybercrime and the trends, phishing remains the biggest concern for senior management. 80% of our budget geared towards cybercrime management is allocated to controls to combat phishing and this approach is systemic across all the major banks in the country. We know this because we are part of an industry cybercrime forum called SABRIC": e-Crime Fraud Specialist (E).

From the responses provided, it is apparent that phishing is the biggest form of cybercrime and it is used as the primary means to illegally solicit customer online information which is used to perform cybercrime. Cybercrime does not generally take place by gaining access to the bank's network but through information provided by customers.

A_Q8. Is cybercrime management a proactive, preventative or detection approach?

"……The design of this system is detective in nature as the rules built into it are not robust to proactively identify and stop a cybercriminal from perpetuating fraud" - Vice President: Information Security (A).

Cybercrime is an evolutionary activity and as a result, the shape and form of the crime is difficult to proactively detect in order to inform a defense approach. Consequently, the approach to combating cybercrime in the banking industry is detective and reactive rather than preventive.

A_Q9. In your view, does your firm size, management support and IT experience influence cyber-criminal activity?

"No – The size of the IT team and management support in addition to the existence of a robust IT system does not proactively combat cybercrime. These assist in executing fraud strategies to minimise cybercrime exposure. We need these people to formulate fraud strategies. This includes cybercrime by the way" – Head: e-Crime (B).

In addition to this other participants agreed with this statement and additionally echoed that the senior management support and the size of the firm do not result in a decline of cybercrime activity. They merely drive the implementation of strategies aimed at combating cybercrime.

A_Q10. Based on the trends on cybercriminal activity, what are management perceptions on the root cause of cybercriminal activity?

"The end result of all cybercriminal attack is to gain access to a customer banking profile to perform fraud. However, the process is initiated through a compromise of the customer personal information as the criminals find it much easier to attack individuals than IT systems. This places security as our number one root cause of cybercrime in the organisation" – Fraud Specialist – (E)

"In our analysis of cybercrime and the trends, phishing remains the biggest concern for senior management. 80% of our budget geared towards cybercrime prevention is allocated to controls to combat phishing and this approach is systemic across all the major banks in the country. Protection of customer information through system enforced controls remains paramount to us": e-Crime Fraud Specialist (E).

Based on the responses from the participant, it can be deduced that security and access controls are a key factor that influences cybercrime activity in BetaBank.

"Lack of user education and awareness is the biggest root cause of cybercriminal activity as people are still clicking on anonymous links and posting their personal information on social media such as Facebook" - Head: e-Crime (B).

We cannot stress enough the importance of user education on the use of the online portals. We try our best to provide public security awareness programs but users only become aware of them once an attack has been launched on their account. With the increase in use of our online portals, user education is pertinent as a success metric against cybercrime" - Head: e-Crime (B).

Lack of user awareness is considered as a further factor that influences cybercriminal activity.

"These criminals are normal guys who know how to defeat our controls. They are thugs who threaten employees from the banks to solicit customer information. In other instances, they rely on syndicates located in Russia who phish our customer information and sell it back to our South

African syndicates who in turn use these information to commit cybercrime. Our South African syndicates are not always the brains behind the soliciting of customer information through phishing which is used to perpetuate cybercrimes" – Head: e-Crime (B).

"The design of this system is detective in nature as the rules built into it are not robust to proactively identify and stop a cybercriminal from perpetuating fraud" - Vice President: Information Security (A).

In analyzing the responses from the above, ineffective internal controls and processes result in cybercrime attack.

"In mid-2000, BetaBank embarked on a strategic journey to migrate all the traditional banking services to its online portals in order to provider faster, effective and efficient customer service to its clients. In time, we began to realise the benefits of this innovation and soon turned this innovation into a customer value proposition. The rapid increase in customer migration onto these portals was indicative of their acceptance and preference for the use of these online portals" – Head of Information Security (C)

According this statement and other contributions from the respondents, it is apparent that whilst there is prevalence in the use of the internet to perform online transactions, the unintended consequence is the proliferation of cybercriminal activity on its customer. Prevalent use of the internet is therefore seen as a root cause as to why cybercrime is on the increase in BetaBank.

"....In all of these crimes, the motive is to perform fraud either by way of stealing customer personal details in order derived some economic benefit or reward. They do this for money!" - Head: e-Crime (B).

".....I believe if there was no material gain, the crime will not be performed in the first place": e-Crime Fraud Specialist (E).

Besides the low conviction rate, BetaBank has been a target of cybercrime due to the perceived monetary gains the cybercriminal projects they will benefit from cybercrime activity in BetaBank. BetaBank has a healthy balance sheet with a customer base of circa 9 million customers. This makes BetaBank a suitable target for cybercriminal activity. Therefore perceived material gain is a factor that leads to cybercriminal activity in BetaBank.

Theme B: Cybercrime and the Routine Activity Theory - Objective 2 (How does the Routine Activity Theory help describe cybercrime activity in BetaBank?)

Based on the analysis above, the Routine Activity Theory proved to be a useful tool and a sound theoretical base to explore the cybercrime phenomenon. By using the conditions necessary for crime to take, it became clear the variables to consider in order formulating the research question to inform the research outcomes discussed above.

Theme C: How to minimise cybercrime attack – Objective 3 (How can South African banks minimize cybercrime fraud activity?)

C_Q11. What are the conviction rates for cybercriminal activity in your organisation?

"These cybercrime syndicates are known but it takes time to arrest them due to the multiple role players involved in one attack and worse is their geographical spread" – Cybercrime Specialist (D)

"The conviction rate is less than one percent. Across the banking industry in South Africa, there has been no conviction. The low rate of conviction promotes cybercrime" - Head: e-Crime (B).

With lower rate of convictions, the propensity to commit crime is high as there are no consequences or legal recourse against the perpetuators of these crimes.

C_Q12. Are there convictions for these crimes when they have been identified?

"The conviction rate is less than one percent. Across the banking industry in South Africa, there has been no conviction. The low rate of conviction promotes cybercrime" - Head: e-Crime (B).

Although there have been some arrests, these have not resulted in any convictions partly due to the fewer arrests made and the lack of evidence to convict these criminals.

"Also, law enforcement agencies do not arrest all parties concerned which results in broken pieces of evidence which is not strong enough to inform a successful conviction" - Head: e-Crime (B).

C_Q13. Does the organization have a view of the profile of these criminals?

"These criminals are normal guys who know how to defeat our controls. They are thugs who threaten employees from the banks to solicit customer information. In other instances, they rely on syndicates located in Russia who phish our customer information and sell it back to our South African criminals who use these information to commit cybercrime. They are not always the brains behind the soliciting of customer information through phishing which is used to perpetuate cybercrimes" – Head: e-Crime (B).

"Although cybercrime requires expert knowledge of IT control breakdowns, the person performing the cybercrime does not need to be an expert in cybercrime as the information required to engage in cybercrime can be purchased from many sources"- Head of Information Security (C).

According to the respondents although cybercriminal activity involves the use of and knowledge of IT systems, the main syndicates are generally not IT experts or a technically inclined individuals. They are merely individuals who solicit the help of an IT specialist to assist them in committing these crimes. This makes cybercrime an activity that requires more than one person to execute. It is multi-faceted.

C_Q14. What actions is the organization currently taking against cybercrime?

"First and foremost, we need to ensure that we ring-fence our customer information such that it is not easily hacked by cybercriminals. Security remains a core focus for us in our fight against cybercrime" - Head - Information Security (C).

"Access and security is something that we continue to prioritise. For us to minimise our risk exposure to cybercrime, we need to ensure that our security controls are robust to deter entry both internally and externally"- e-Crime Fraud Specialist (E)

Based on the above responses, improving security of the online portals and protecting customer data are core aspects that BetaBank needs to achieve in order to minimise exposure to cybercrime.

"We cannot stress enough the importance of user education on the use of the online portals. We try our best to provide public security awareness programs but users only become aware of them once an attack has been launched on their account. With the increase in use of our online portals, user education is pertinent as a success metric against cybercrime" - Head: e-Crime (B).

"Our customers cannot protect themselves when they do not have the knowledge about the security features. Educating our users is a key step in our strategy to combat cybercrime" - Head - Information Security (C).

The respondents all agreed that user education and security controls are perhaps the most key management focus as they aim to minimise cybercrime attacks. This points to the fact that whilst management are putting concerted efforts to secure online portals, the controls will be deemed weak if the users do not apply stringent measures on their part to ensure that the banks' efforts are commensurate with knowledge of the do's and the don'ts of using online portals.

"We cannot be ahead of the fight against cybercrime if we only focus our attention on cybercrime attacks within our organisation. We need to be in sync with other industry players to ensure that whilst we analyse our cybercrime attack patterns, we also review attacks on our competitors to inform a better proactive approach to cybercrime management. Our participation in the period SABRIC meetings is therefore a good start - Head: e-Crime (B).

Other proponents of this view echoed that the fight against cybercrime in the banks is a collaborative effort and one that needs the participation of other organisations whose organizational setup is also prone to cybercrime attack.

"We need to also design and implement effective internal systems and processes with minimal manual interventions. The fast pace of cybercrime requires that we respond quickly to any new or emerging attack on any of our platforms or against any of our customer portals" – Head: Information Security (C).

These systems and processes that management designs and implements should provide adequate support for the cybercrime processes and should have the human capital to execute and manage these systems.

C_Q15. Are the steps being undertaken effective? If not, why?

"Yes, these steps are effective. We generally see a decline in the number of incidences when we consistently apply these set of rules. In most cases, there is a sudden spike when a new form of attack emerges which we cannot entirely be prepared for"- Head: e-Crime (B).

"These controls work but sometimes we have staff attrition which ends up opening ourselves up to loss of IP (Intellectual Property) to continue executing these activities. Otherwise we do pretty well when these controls are performed consistently"– Cybercrime Specialist (D)

It is clear that these controls are sustainable and effective when performed consistently. Although it does not eliminate the cybercrime risk entirely, it provides a solid defense mechanism to fight cybercrime.

C_Q16. Are there any other factors that lead to cybercriminal activity in BetaBank?

There were no additional responses from the participants to include other than what has been discussed and deliberated upon in this section.

4.3 Summary of the Chapter

It is evident from the narratives and the responses from the participants that cybercrime is evolutionary and in the context of BetaBank, it is mainly caused through the absence of preventative controls coupled with IT systems that are not robust to proactively detect and prevent cybercriminal activity. Another key driver for cybercrime attacks in the South African banking environment is the poor level of user education or lack thereof to ensure that users are able to perform online activities with the full knowledge of the security considerations to undertake. It is also evident that BetaBank has a cybercrime strategy which is supported by an effective governance process to ensure that the strategy is adapted to align to changes in the cybercrime landscape. Whilst the internal IT architecture responds to the security requirements which makes it not easily accessible to cybercriminals, the same cannot be said for enforced security measures on the part of the customer due to the lack of understanding of the security implications. The most common type of cybercrime which affects BetaBank is phishing attacks and accounts for a significant proportion of their cybercrime events. In order to minimise the exposure to cybercriminal, the respondents indicate that management should consider

implementing security controls to protect customer information, educate their users, implement internal systems and processes and participate in industry wide cybercrime programs.

CHAPTER 5

INTERPRETATION OF RESULTS AND THE CONCEPTUAL FRAMEWORK

5.1 Introduction

This chapter interprets and links the results from the research to the literature which was explored in the beginning chapters of this study. The introductory chapter aimed to identify factors that lead to cybercriminal activity from the perspective of a South African bank and subsequently provide recommendations on ways South African banks can minimise cybercriminal attack. This chapter provides a narrative of the case, the interpretation thereof and how themes emerged which were underpinned by the initial conceptual framework based on the Routine Activity Theory. The narrations are used to answer the research questions posed to the respondents during the interview process.

5.2 Causes of Cybercrime Construct

The analysis of this theme is underpinned by Cohen and Felson (1979) Routine Activity Theory. The authors posit that one of the conditions that must exist for crime to take place is the absence of capable guardianship, the characteristic of the criminal and a suitable target. Based on this premise, a conceptual research framework was identified which posits that technical, formal, informal controls, the presence of the internet and low conviction rate were factors that lead to cybercriminal activity in BetaBank. Based on the data analysis and interpretation thereof, the following were identified as causes of cybercrime from the perspective of BetaBank:

- Poor security and access controls linked to technical controls;
- Lack of awareness and user education linked to informal controls;
- Prevalent use of the internet linked to the use of the internet;
- Ineffective systems and processes linked to formal controls;
- Low rate of conviction linked to suitable target; and
- Perceived material gain on the part of the cybercriminal linked to suitable target.

The ensuing discussion links these themes above to literature and the conceptual framework.

(a) Poor Security and Access Controls (Technical Controls)

Access to customer information which is used to commit the crimes are generally not fraudulently obtained but through social engineering mechanisms wherein a customer unknowingly responds to a fake email or logs onto a fake site. The term used to describe this concept is called Phishing. Phishing is a homophone for fishing which simply means an act of deception to catch a fish. In the context of cybercrime, phishing infers using tactics to cunningly obtain sensitive information from a person. This agrees with literature as purported by Jagatic et al. (2007) who posit that cybercrime takes place through fraudulently obtaining confidential information from a person such as online username and passwords, banking details and credit card information. According to the authors, the perpetuators often disguise themselves as a trustworthy source by sending a fake link to a user who unknowingly clicks on the link where their security credentials are compromised. Phishing has become an increasing avenue used to fraudulently obtain confidential information from clients as it is easier to solicit this information than attempting to gain unauthorised access to the same information through a computer system (Dhamija et al., 2006). The perpetuators of these crimes embellish emails and websites with logos to mimic the original entity or person which is then used to falsely obtain sensitive information from the victims. It was deduced from the interview that although phishing is performed on the South African bank customer, the perpetuators of this activity are not based in South Africa. They remotely obtain this information which is sold to an ordinary person on the street which is then used to commit cybercrime. Effective execution of cybercrime activity is dependent on the accuracy of the customer information at hand.

In some instances, these syndicates use social media information to gather some of the customer information they use in these crimes. The expertise required is not geared towards the ability to gain direct access to customer information but rather the knowledge to mimic genuine websites or emails and presenting these to the customer as though it was original.

With reference to Dhillon et al. (2001), technical controls mainly address access control. Based on the discussion above, it can be deduced that technical controls in the form of access rights has a direct impact on cybercriminal activity as the information used to perpetuate cybercrime is obtained through unauthorized access to customer personal information. According to Samonas (2009), access rights create opportunities to commit cybercrime. Phishing as explored above is

the primary access control mechanism used by cybercriminals to commit cybercrime. This in effect is the biggest cause of cybercrime and is the primary focus for senior management when they define strategies to combat cybercrime.

"In our analysis of cybercrime and the trends, phishing remains the biggest concern for senior management. 80% of our budget geared towards cybercrime prevention is allocated to controls to combat phishing and this approach is systemic across all the major banks in the country": e-Crime Fraud Specialist (E.)

(b) User Awareness and Education (Informal Controls)

Informal controls are centered on education and how that impacts the culture of an organization towards the implementation of controls to curb cybercrime (Furnell and Thomson, 2009). Due to the prevalent use of online banking facilities, there is the need to focus on user education. From the interview performed, all the respondents agree that aside phishing, user education and awareness is the next biggest root cause of cybercrime activity.

"Users Lack of education and awareness is the biggest root cause of cybercriminal activity as people are still clicking on anonymous links and posting their personal information on social media such as Facebook" - Head: e-Crime (B).

"South Africans are susceptible to this kind of fraud like phishing and credit card cloning because generally speaking, people are ignorant about the risks associated with the use of these online facilities. Recent survey indicated that a vast number of customers responded to bogus emails which resulted in their personal information being fraudulently obtained Vice President – Information Security (A).

"Technical and support staff have a deeper understanding and knowledge of the security risks associated with the use of online transactions. However, the general public does not have the same level of education and awareness regarding cybercriminal activity" - Head of Information Security (C).

Due to the low levels of user education and awareness, the banks in South Africa are implementing strategies to combat cybercrime. In a related response from one of the respondents, he emphasized that the security protocols are being deployed onto online platforms are focusing on preventative controls rather than detective.

"We analyse volumes and spikes and have noted that cybercrime is on the high for instances where the customer compromised their personal information and was not aware of what steps should have been taken to prevent the cyber- attack. Our stats also indicate that a high number of our users have been attacked more than once. This definitely drives our strategic focus which is geared at implementing security controls that are preventative" – Cybercrime Specialist (D).

(c) Prevalent Use of Technology Construct (Internet)

The conceptual framework projects that as a result of cybercrime taking place in the spatial realm, it inherently requires technology as an enabler. The framework suggests that the internet is a core resource that enables cybercrime to take place. Consequently, the internet shapes the choice of an organisations defense mechanism against cybercrime. The respondents agree with this assertion and also indicate that the prevalent use of technology by South African bank customers to perform online activities places an onus on these banks to enhance its online defense mechanisms. The prevalence is as a result of the low cost and the ease of access to multiple internet domains.

The link to cybercrime is echoed by Schreck et al. (2002) who posit that generally, active members of a community are more susceptible to crime than those who stay at home or are unemployed and not actively engaged in any form of activity. A routine is an antecedent to cybercrime.

……The rapid increase in customer migration onto these portals was indicative of their acceptance and preference for the use of these online portals" – Head of Information Security (C)

This agrees with literature as according to Rosewarne (2012), the prevalent use of the internet and low penalty imposed on the cybercriminal once convicted are the key drivers for cybercrime proliferation in South Africa. The author again suggests that increasing the use of online services increases the chances of a user being susceptible to cybercriminal attack. The data analysis suggests that in the absence of the internet, cybercrime will cease to exist, thus the internet is an antecedents to cybercrime. Wilcox et al. (2004) argue that by virtue of the routine activities that an individual performs, they may be placed closer to the potential offender for a possible attack. Its applicability to online activities may pose a question as cybercrime takes place away from the offender. Whilst it can be argued that proximity is not a greater factor in

cybercrime activity, the nature of the routine activity being performed places the individual at risk of victimization.

(d) Internal Systems and Processes Construct (Formal Controls)

According to Dhillon et al. (2001), formal controls involve the application of rules and are mostly modelled around adherence to corporate policies and procedures, compliance and regulatory requirements. Based on the discussion, the respondents are of the opinion that corporate policies and procedures, compliance and regulatory requirements and adherence thereof do not have a significant effect on cybercrime activity or have an impact on the way the bank determines and implements its defenses. In their opinion, compliance or existence of policies and procedures does not influence the proliferation of cybercrime within the South African banking industry.

"Our formal controls are intrinsic and applicable to internal staff members to ensure that they do not circumvent internal controls which might render our IT systems susceptible to cybercriminal attacks. Due to the complex nature of the banking network security, it is not easy for cybercriminals to attack our systems. They mostly go for soft targets being our customers. Our fraud policies, IT policies and procedures, compliance and other regulatory requirements are internal and do not inform our defensive approach to cybercrime. Our defenses are aimed at external forces we do not have control over" – Cybercrime Specialist (D)

(e) Low Conviction Rate Construct (Suitable Target)

BetaBank is a member of SABRIC (South African Banking Risk Information Centre) where all the banks in South African report on cybercrime related activities. SABRIC's primary objective is to combat bank related crimes. BetaBank reported six cybercrime cases to SABRIC in 2015 which resulted in six arrests; however none of these cases resulted in a successful conviction. Across the industry, there has been no conviction since the proliferation of cybercrime in the South African banking industry. According to this respondent, the multi-faceted approach to cybercrime makes it an increasingly difficult task to make an arrest and a conviction.

"Syndicates are known but it takes time to arrest due to the multiple role players involved in one attack" – Cybercrime Specialist (D)

"The conviction rate is less than one percent. Across the banking industry in South Africa, there has been no conviction. The low rate of conviction promotes cybercrime" - Head: e-Crime (B).

Further, because the criminals masquerade the customers online profiles as their own, it is extremely difficult to trace these crimes to an individual. The multi-layered approach to cybercriminal and the fact that it involves more than one person makes it an increasing difficult crime to curb.

"In our last arrest, the IP (Internet Protocol) address was traced to a mobile number in the prison cell. The mobile number was registered to a different user whose mobile number had been sim-swopped earlier" - Head: e-Crime (B).

According to Cohen and Felson's (1979) Routine Activity Theory, a condition necessary for a cybercrime to take place is an attribute of the characteristics of the potential offender. These characteristics include the acumen of the cybercriminal which revolves around their knowledge of the potential victim and the level of access the cybercriminal has which has been discussed in Theme 1. According to the respondents although cybercriminal activity involve the use of and knowledge of IT systems, the main syndicates are generally not IT experts or a technically inclined individual. They are merely individuals who solicit the help of IT specialist to assist them in committing this crime. This makes cybercrime an activity that requires more than one person to execute.

"These criminals are normal guys who know how to defeat our controls. They are thugs who threaten employees from the banks to solicit customer information. In other instances, they rely on syndicates located in Russia who phish our customer information and sell it back to our South African criminals who use these information to commit cybercrime. They are not the brains behind the soliciting of customer information through phishing which is used to perpetuate cybercrimes" – Head: e-Crime (B).

"Although cybercrime requires expert knowledge of IT control breakdowns, the person performing the cybercrime does not need to be an expert in cybercrime as the information required to engage in cybercrime can be purchased from many sources"- Head of Information Security (C).

"We analyse volumes and spikes and have noted that cybercrime is on the high for instances where the customer compromised their personal information and was not aware of what steps should have been taken to prevent the cyber- attack. Our stats also indicate that a high number

of our users have been attacked more than once. This definitely drives our strategic focus which is geared at implementing security controls that are preventative" – Cybercrime Specialist (D).

(f) Perceived Material Gain Construct (Suitable Target)

The concept of perceived material gains mirrors the Rational Choice Theory (Clarke and Felson, 1993) which posits that individuals always makes choices that results in the best benefit and satisfaction. Relating this theory to the theme, the respondents had this to say:

"....In all of these crimes, the motive is to perform fraud by way of stealing customer personal details in order derived some economic benefit or reward. They do this for money! - Head: e-Crime (B).

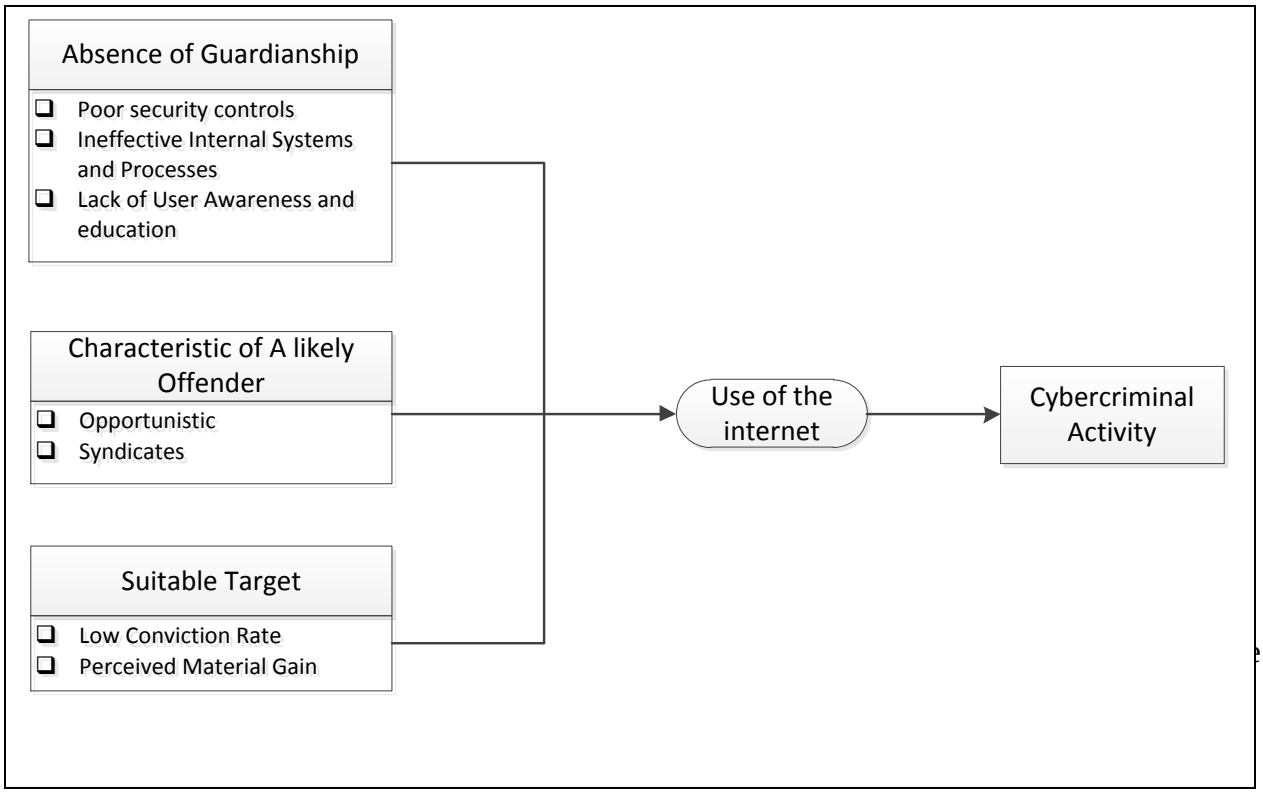
".....I believe if there was no material gain, the crime will not be performed in the first place": e-Crime Fraud Specialist (E).

This confirms that the Rational Choice Theory and the theme suggest that perpetuators of cybercrime do so with the intention to derive some benefit. Perceived material gain is therefore a factor that leads to cybercriminal activity. According to Willison and Backhouse (2006), criminals perform risk assessment on their targets and the process includes an evaluation of the perceived benefits, costs and risks associated with the criminal activity. These conclusions are also supported by Rosewarne (2012) who indicates that the proliferation of cybercrime is attributed to two factors which are underpinned by individuals responding to monetary and psychological gains.

Evidently, literature and themes are aligned to this view and conclusively project that the factors that were identified in the data analysis is supported by literature. Based on these, the initial conceptual framework was revised.

5.3 Revised Conceptual Framework

Based on the above, the initial conceptual research framework provided in Chapter 2 was revised to illustrate the factors that BetaBank perceives as causes of cybercrime through the theoretical lens of the Routine Activity Theory (Cohen and Felson, 1979).



5.4 Summary of the Chapter

This chapter aimed to explore and describe the case narrative of the factors that influence cybercriminal activity in a South African bank using the themes identified in the conceptual framework which was based on Cohen and Felson (1979) Routine Activity Theory. In the analysis of these factors, the aim was to validate the conceptual framework to assert through the Routine Activity Theory that the absence of capable guardianship (i.e. technical, informal and formal controls), the characteristics of the cybercriminal (i.e. knowledge and expertise), a suitable target and use of the internet are factors that influence cybercriminal activity and subsequently informs the defense mechanism that South African banks adopt to curb this phenomenon. From the data analysis performed and the ensuing discussions, it is clear that access controls and lack of awareness and user education about the risks associated with the use of online systems result in the highest number of cybercrime activity. This is the primary factor

that forms the basis of a bank's definition and execution of its defense mechanisms. The following other conclusions were drawn with reference to the conceptual framework.

- Technical controls relate mainly to access rights in the form of phishing. Phishing is the biggest form of cybercriminal wherein the cybercriminal will use social engineering techniques using mechanisms such as fake websites and emails to fraudulently obtain customer sensitive information which is used to perpetuate the cybercriminal act. This is the primary factor that leads to cybercriminal activity in BetaBank;

- Informal controls in the form of user education and awareness is the second most important factor that results in cybercriminal attacks. The rate of evolution of technology and cyber-related activities does not commensurate the level of education users have about the risks associated with cybercrime. South African banks need to define, design and implement preventative controls which will minimise the extent of user education required to use these online systems that results in customers becoming victims of cybercriminal attacks;

- Formal controls such as the existence and compliance to policies and procedures have minimal impact on the occurrence rate of cybercrime and thus have an insignificant impact on how it influences the banks approach in defining strategies to defend itself against any possible cybercriminal activity. However, defining and implementing a robust and stringent internal processes and systems to manage cybercriminal activity is deemed to be key as it regulates and guides the execution of activities aimed at combating cybercrime;

- The prevalent use of the internet inherently results in the cybercriminal activity taking place. The existence and use of the internet is an antecedent to cybercriminal activity. The internet therefore poses a security risk as far as access to and abuse of customer information to perpetuate cybercrime is concerned. In an attempt to curb the proliferation of cybercrime, BetaBank banks considers the use of the internet as an intrinsic area of focus in the design and implementation of cybercriminal strategies;

- Cybercrime takes place due to the perceived material gains which are usually monetary in nature.

- Cybercriminals are not all cybercrime experts but ordinary people who use the resources and information easily obtained through IT experts to perform cybercriminal activities. Cybercrime is a multi-faceted approach which involves the soliciting of customer information using technological means, churning the stolen information to circumvent customer's online profiles and executing unauthorised activities on a customer's behalf; and

- Expertise of IT is required in order to perform cybercriminal activity although it was also deduced that the cybercriminal may not be the person possessing the IT knowledge due to dependency on IT specialist to sell customer information obtained through social engineering that is required to commit these crimes. As the research is in the context of a South African bank, it is imperative to comment that although the cybercrime activity is performed within South Africa, the information used may have been obtained from other remote sources as deduced from the themes above.

CHAPTER 6

VALUATION OF THE RESEARCH AND CONCLUSION

6.1 Introduction

Through literature review, it was identified that there is a scourge of cybercrime activity in proportions that is rapidly becoming a global concern. Within the banking sector in South Africa, there is even a bigger threat of cybercrime due to the increasing attacks on the bank's network and customers' online profile with a significantly bigger proportion been attacks on customer information. Secondly, there has been very little research performed in cybercrime and in particular within the context of South Africa. This study focused on an analysis of cybercrime from the perspective of BetaBank and how these perceptions inform the defense approach for BetaBank. The concluding chapter provides a summary of the findings, research contribution, limitations and suggestions for future studies which involve this phenomenon. Section 6.1 provides a summary of the research and the associated findings; Section 6.2 provides commentary on the contribution of this research; Section 6.3 discusses the key limitations of the research; Section 6.4 concludes by highlighting areas where there exist opportunities for future research regarding cybercrime.

6.2 Overview of Chapters

Chapter 1

Chapter 1 provided an introduction to the research elaborating on the research problem statement, goals and objectives and an overview of the research strategy and design.

Chapter 2

Chapter 2 provided an overview of the survey of scholarship, the theoretical framework which underpinned the study. The chapter also explored existing literature regarding the cybercrime phenomenon in order to gain a holistic understanding to inform the data collection and analysis. Based on these theoretical underpinnings, a conceptual research framework was proposed which

was evaluated in subsequent chapters. The research was guided by Cohen and Felson (1979) Routine Activity Theory. Semi structured interviews and secondary data were the techniques used to obtain data.

C**hapter 3**

Chapter 3 explored existing research methodologies and provided a justification for the research method used in this study by contrasting these research methodology approaches. Thereafter, a critical exploration of the research approaches, research strategy and design was discussed with the limitations of the methodology also provided.

C**hapter 4**

This chapter focused on the data collected, the method adopted to analyse the data and the demographics of the participants that took part in the interview.

C**hapter 5**

Chapter 5 reviews the findings of the study and relates the findings to the literature review provided at the beginning of the study. The chapter also provided detailed analysis of themes identified in the data collected which was achieved through interviews and the interpretation of these themes.

6.3 Research Questions

Literature reviews suggested that crime takes place when certain conditions persist and classifies these conditions into three domains namely; absence of a capable guardian, the characteristics of the potential offender and a suitable target (Cohen and Felson, 1979). The aim of this research was thus to examine using an interpretive research approach, an analysis of cybercrime from the perspective of BetaBank. The ensuing discussions reflect on how the research questions formulated at the beginning of this report were addressed through this case study.

RQ1: What are the perceptions of factors influencing cybercrime activity in BetaBank?

From the case study analysed above, it can be seen that cybercriminal activity is influenced by many factors. However, from the perspective of the banks, cybercriminal activity is influenced by the following factors:

- Weak access controls which culminates in phishing attacks using social engineering techniques (section 4.2.1);
- Inability of BetaBank to adequately educate its users on the dangers associated with the use of technology to perform online activities thus users are ignorant on the security controls to be mindful of when performing online activities. The mass exodus of users migrating onto mobile/digital platforms has placed a limitation on BetaBank to effectively educate its users (Section 4.2.1);
- The prevalent use of the internet is a key factor that influences cybercriminal activity (Section 4.2.1);
- Ineffective systems and processes is a factor that influence cybercriminal attacks as a significant portion of controls have been placed on the customer. This is because the bank does not want to accept liability for the cybercrime attack on their customers account (Section 4.2.1).
- Low conviction rate as a result of criminals masquerading the customers' online profile as their own, traceability becomes difficult. The multi-layered approach to cybercrime and the fact that it involves more than one person makes it difficult to arrest and convict perpetrators (Section 4.2.1).
- Perceived material gain from the output of the cybercriminal act which are usually monetary (Section 4.2.1).

RQ2: How does the Routine Activity Theory help explore and describe cybercrime activity in BetaBank?

Based on the analysis above, the Routine Activity Theory proved to be a useful tool and a sound theoretical base to explore and describe the cybercrime phenomenon. By using the conditions necessary for crime to take place, it became clear that the variables to consider in order to formulate the research question to inform the research outcomes discussed above (Section 4.2.2).

RQ3: How can South African banks minimize cybercrime activity?

This question was not explicitly explored in the data analysis and thematic reviews section as the nature of the research question aimed to solicit the respondents opinion on ways that banks can implement processes to minimise their exposure to cybercrime. The ensuing discussion recommends ways South African banks can minimise cybercriminal attack primarily based on literature and some responses received from the respondents. In answering this question, the following recommendations are informed by empirical evidence and literature on how South African banks can minimise cybercrime activity (Section 4.2.3).

(a) Security of Customer Information

Based on the themes identified the biggest risk posed to BetaBank as far as cybercrime is concerned is access rights and the ability to obtain unauthorized access to customer data. Protection of customer data is therefore of utmost importance in the strategic focus for BetaBank towards combating cybercrime. South African banks should therefore aim to implement pervasive security controls across their networks and more so security over the databases, servers and other infrastructural support that stores customer information. In addition, banks need to implement and enforce access controls over their internal staff members who have elevated access rights to customer information. Access should be granted on the principle of least privilege which require that employees are granted access based on their roles and responsibilities.

(b) Creating Awareness and User Education

User education is a key aspect requiring management focus if they are to make inroads in the fight against cybercrime. Implementing awareness and user education programs and disseminating them periodically will minimise the occurrence rate of cybercrime attacks as users become more aware of the dangers of performing activities in cyber space. The mass exodus of users onto the online platforms creates an opportunity for the banks to utilize the same channel to reach its customers to provide continuous education.

(c) Implementation of Effective Internal Systems

The nature of cybercrime activity requires BetaBank to design and implement robust and proactive fraud detection systems to provide real time identification and resolution of potential fraud events. These systems should provide adequate support for the cybercrime processes and should have the human capital to execute and manage these systems. Processes and systems design should be such that they are able to prevent rather than detect cybercrime events.

(d) Active Participation in Industry-Wide Cybercrime Programs

Being a part of an industry wide forum will also assist to share ideas, analyse common cybercrime threats and trends faced by other banks which will help to shape the defensive approach adopted to mitigate the risks associated with cybercrime.

(e) Enactment of Government Policies and Regulations

The government needs to enact and enforce stricter polices within which harsher sentences are imposed on cybercriminals once convicted. In order to achieve this, the issues of cybercrime need to feature as a top priority in the Information, Communication and Technology (ICT) agenda.

6.4 Study Limitations

The case study research design approach followed an interpretive research approach which tends to lose reliability due to the wide variety of interpretations and that may arise from the themes. Because interpretive research is subjective and often based on a different set of ontological and epistemological assumptions, findings are generally not as reliable and representative as those derived in the positivist paradigm (Bhattacherjee, 2012) as the data is somewhat impacted by the researcher's personal view point, values and beliefs. To improve reliability, the themes in this study were closely monitored and data analysis was used to apply coding throughout the process. Additionally, a detailed account of the phenomenon and its social context was provided so allow a reader to independently authenticate their inferences. Another disadvantage of interpretivist research is the subjective nature of this research approach which tends to give room for

researcher bias. A further limitation of this study approach is the credibility of findings and how it is easily conveyed to the reader as believable. In order to improve the credibility of the findings, data triangulation and robust data management approach was adopted to ensure that a reader can independently audit the data collection and analysis (Bhattacherjee, 2012).

6.5 Recommendations for Future Research

A comparative study using the theory applied in this research can be performed on cybercriminal activities across other industries and geographical domains to establish the universality of this phenomenon. In addition, further research can be performed in the same context using alternative theories to establish commonalities in outcomes and to complement weaknesses in the application of the Routine Activity Theory. Further, it recommended that further research look into how banking institutions can collaborate with the government, public and private sectors to legislate and implement law enforcement within the ICT sector.

REFERENCES

Ary, D., Jacobs, L.C., Razavieh, A., Sorensen, C., 2010, *Introduction to Research in Education 8th edition*, Wadsworth Publishers, Belmont.

Ajzen, I. (2011). The theory of planned behaviour: reactions and reflections.

Bandura, A. (2011). Social cognitive theory. *Handbook of social psychological theories, 2012*, 349-373.

Bechor, T., Neumann, S., Zviran, M., & Glezer, C. (2010). A contingency model for estimating success of strategic information systems planning. *Information & Management*, 47(1), 17-29.

Beauchamp, T. L., & Childress, J. F. (2001). Principles of biomedical ethics. *Oxford university press.*

Bhaskar, R. (2014). *The possibility of naturalism: A philosophical critique of the contemporary human sciences*. Routledge

Bowling, A., & Ebrahim, S. (2005). Handbook of health research methods: investigation, measurement and analysis. *McGraw-Hill Education* (UK).

Borgatti S. P. (1990). Theoretical Framework, Elements of Research. Available on http://www.analytictech.com/mb313/elements.htm accesses 2013-05-2013

Bhattacherjee, A. (2012). Social science research: principles, methods, and practices.

Bowling, A., & Ebrahim, S. (2005). Handbook of health research methods: investigation, measurement and analysis. *McGraw-Hill Education* (UK).

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

Brod, M., Tesler, L.E. & Christensen, T.L., 2009, 'Qualitative research and content validity: developing best practices based on science and experience', *Qual Life Res*, 18, 1263–1278

Castells, M. (2002). The internet galaxy: Reflections on the internet, business, and society. Oxford: Oxford University Press.

Choo, K.K. R. (2011). The cyber threat landscape: Challenges and future research directions, Computers & Security, 30, 8, pp. 719-731.

Clarke, R. V. (1999). Hot products: Understanding, anticipating and reducing demand for stolen goods (Paper 112, B. Webb Ed.). *London: Home Office, Research Development and Statistics Directorate.*

Cohen, L. E. and Felson, M. (1979) Social Change and Crime Rate Trends: A Routine Activity Approach, *American Sociological Review*, 44, 4, pp. 588-608.

Collins, H. (2010). Creative Research: The Theory and Practice of Research for the Creative Industries. *AVA Publications*, p.38

Corley, K. G., & Gioia, D. A. (2011). Building theory about theory building: what constitutes a theoretical contribution?. *Academy of management review*, *36*(1), 12-32.

Cornish, D. B., & Clarke, R. V. (Eds.). (2014). *The reasoning criminal: Rational choice perspectives on offending*. Transaction Publishers.

Coupe, T., & Blake, L. (2006). Daylight and darkness targeting strategies and the risks of being seen at residential burglaries. *Criminology*, 44, 431-464.

Creswell, J. W. (2013). *Research design: Qualitative, quantitative, and mixed methods approaches*. Sage publications.

Creswell, John W., and Cheryl N. Poth. (2017). *Qualitative inquiry and research design: Choosing among five approaches*. Sage publications.

Crowther, D. & Lancaster, G. (2008). Research Methods: A Concise Introduction to Research in Management and Business Consultancy. *Butterworth-Heinemann*

Davis, M. (2001) 'Introduction', in Conflict of Interest in the Professions, eds M. Davis, and A. Stark, *Oxford University Press*, New York pp. 3–22.

Ditsa, G. (2003). Activity Theory as a Theoretical Foundation for Information Systems Research. [Online] Available from: http://www.igi-global.com/chapter/activity-theory-theoretical-foundation-information/22960 [Last Accessed: 2015-05-10]

Dhamija, R., Tygar, J. D., & Hearst, M. (2006). Why phishing works. *In Proceedings of the SIGCHI conference on Human Factors in computing systems* (pp. 581-590). ACM.

Easterby-Smith, M., Thorpe, R., & Jackson, P. R. (2015). *Management and business research*. Sage.

Eck, J. E., & Weisburd, D. L. (2015). Crime places in crime theory.

Eisenhardt, K.M. (1989), Building theories from case study research, *Academy of management review*, Vol. 14 No. 4, pp. 532–550.

Eisenhardt, K.M. and Graebner, M.E. (2007), Theory building from cases: Opportunities and challenges. *Academy of management journal*, Vol. 50 No. 1, pp. 25–32.

Electronic Communications and Transactions Bill (2012). [Online] Available from: http://www.cybercrime.org.za/definition [Last Accessed: 2015-05-10]

Engeström, Y. (1990). Learning, working and imagining: *Twelve studies in activity theory*. Helsinki: Orienta-Konsultit Oy.

Engeström, Y., Miettinen, R., & Punamäki, R. L. (1999). Perspectives on activity theory. Cambridge University Press.

Furnell, S. (2002). Cybercrime: Vandalizing the information society. *London: Addison Wesley*.

Furnell, S. and Thomson, K.-L. (2009). From culture to disobedience: Recognizing the varying user acceptance of IT security, *Computer Fraud & Security*, 2, 5-10.

Gillham, B. (2000). Case study research methods. *Bloomsbury Publishing*.

Glaser, B. (2017). *Discovery of grounded theory: Strategies for qualitative research*. Routledge.

Golafshani, N., 2003, 'Understanding Reliability and Validity in Qualitative Research', The Qualitative Report 8(4), 597-607, 10 November 2014, from http://www.nova.edu/ssss/QR/QR8-4/golafshani.pdf

Grabosky, P., & Smith, R. (2001). Telecommunication fraud in the digital age: The convergence of technologies. *Crime and the Internet*, 29-43.

Gregor, S. (2006). The nature of theory in information systems. *MIS quarterly*, 611-642.

Hartel, P. H., Junger, M. and Wieringa, R. J. (2010). Cybercrime Science = Crime Science + Information Security, Technical Report TR-CTIT-10-34, Centre for Telematics and Information Technology University of Twente, Enschede. [Online] Available from: http://eprints.eemcs.utwente.nl/18500/03/0_19_CCS.pdf [Last Accessed: 2015-04-28]

Hinduja, S. & Patchin, J. W. (2008). Cyberbullying: An exploratory analysis of factors related to offending and victimization. *Deviant Behavior*, 29, 129-156.

Holt, T. J., & Bossler, A. M. (2009). Examining the applicability of lifestyle-routine activities theory for cybercrime victimization. *Deviant Behavior*, 30, 1-25.

Holt, T. J., Bossler, A. M., & Seigfried-Spellar, K. C. (2015). *Cybercrime and digital forensics: An introduction*. Routledge.

Hunton, P. (2009). The growing phenomenon of crime and the internet: A cybercrime execution and analysis model. *Computer Law & Security Review*, *25*(6), 528-535

Jagatic, T.N., Johnson, N.A., Jakobsson, M. and Menczer, F. (2007). Social phishing. Communications of the ACM, 50(10), pp.94-100.

Jones, M. R., & Karsten, H. (2008). Giddens's structuration theory and information systems research. *MIS quarterly*, 32(1), 127-157.

Joseph, J. (2003). Cyberstalking: An international perspective. In Y. Jewkes (ed.) Dot.cons: Crime, deviance and identity on the internet. *Cullompton: Willan Press.*

Kaptelinin, V., & Nardi, B. A. (2006). *Acting with technology: Activity theory and interaction design*. MIT press.

Klein, H.K. and Myers, M.D. (1999). A set of principles for conducting and evaluating interpretive field studies in information systems. *MIS Quarterly*. pp. 67–93.

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), 321-342.

Krauss, S.E, 2005, 'Research Paradigms and Meaning Making: A Primer', The Qualitative Report 10(4), 758-770, viewed 5 August 2013, from http://www.nova.edu/ssss/QR/QR10-4/krauss.pdf

Lawrence, J. (2011). The Factors that Influence Adoption and Usage Decision in SMEs: Evaluating Interpretive Case Study Research in Information Systems. *Leading Issues in Business Research Methods, 1*, 141.

Lee, A.S. and Baskerville, R.L. (2003), Generalizing generalizability in information systems research, *Information systems research,* Vol. 14 No. 3, pp. 221–243.

Levi, M. (2001). Between the Risk and the Reality Falls the Shadow": Evidence and Urban Legends in Computer Fraud (With Apologies to TS Eliot) (From Crime and the Internet, P 44-58, 2001, David S. Wall, ed.--See NCJ-213504).

Livesey, C, (2006). The Relationship between Positivism, Interpretivism and sociological research methods. *AS Sociology*. http://www.sociology.org.uk

Madero-Hernandez, A., & Fisher, B. S. (2012). Routine Activity Theory.

Mell, P., Kent, K., & Nusbaum, J. (2005). Guide to malware incident prevention and handling: Recommendations of the National Institute of Standards and Technology. *Washington DC: National Institute of Standards and Technology*.

Myers, M.D. (2008). Qualitative Research in Business & Management. *SAGE Publications*

Newman, G., & Clarke, R. (2003). Superhighway Robbery: Preventing e-commerce crime. Cullompton: *Willan Press*.

NHTCU/NOP (2002). Hi-tech crime: *The impact on UK business. London: NHTCU.*

Patton, M. Q. (2005). Qualitative research. *John Wiley & Sons*, Ltd.

Pizam, A., & Mansfeld, Y. (2000). Consumer behavior in travel and tourism. Routledge.

Pironti, J. (2013). The Changing Role of Security Professionals. [Online] Available from: http://www.infosecurity-magazine.com/view/30212/the-changingrole-of-securityprofessionals/?goback=%2Egde_1368287_member_212195880 [Last Accessed: 2015-05-31]

Probst, C. W., & Hansen, R. R. (2009). Analysing access control specifications. In Systematic Approaches to Digital Forensic Engineering. SADFE'09. *Fourth International IEEE Workshop* on (pp. 22-33). IEEE.

Rosewarne, C. (2012). The 2012/3 SA Cyber Threat Barometer [Online] Available from: http://www.bic-trust.eu/files/2012/10/SA-2012-Cyber-Threat-Barometer_Medium_res.pdf [Last Accessed: 2017-01-21]

Saunders, M., Lewis, P. & Thornhill, A. (2012). Research Methods for Business Students. *6th edition, Pearson Education Limited*

SABRIC. (2014). Card Fraud 2014. [Online] Available from: https://www.sabric.co.za/media/1141/final-card-booklet.pdf [Last accessed: 2015-11-02]

Samonas, S (2013). Insider fraud and routine activity theory. [Online] Available from: http://eprints.lse.ac.uk/50344/1/Samonas_Insider_fraud_routine_2013.pdf [Last Accessed: 2015-04-12]

Shenton, A.K, 2004, 'Strategies for ensuring trustworthiness in qualitative research projects', *Education for Information* 22, 63-75.

Schreck, C. J., Wright, R. A., & Miller, J. M. (2002). A study of individual and situational antecedents of violent victimization. *Justice Quarterly*, *19*(1), 159-180.

Sutherland, E. (1947). Principles of Criminology. *Philadelphia*: Lippincott.

Thomas, D. and Loader, B. (2000). Introduction – Cybercrime: Law enforcement, security and surveillance in the information age. In D. Thomas and B. Loader (eds) Cybercrime: Law enforcement, security and surveillance in the information age. London: Routledge.

Turner, P. (2016). Mediated Cognition. In *HCI Redux* (pp. 27-40). Springer International Publishing

Svensson, P. (2011). Nasdaq hackers target service for corporate boards. [Online] Available from: http://news.yahoo.com/s/ap/20110205/ap_on_hi_te/us_nasdaq_hackers [Last Accessed: 2015-04-25]

Spyridon, S (2012). Insider fraud and routine activity theory [Online] Available from: http://eprints.lse.ac.uk/50344/1/Samonas_Insider_fraud_routine_2013.pdf [Last Accessed: 2015-04-12]

Turkle, S. (2011). *Life on the Screen*. Simon and Schuster.

Venkatesh, V., & Davis, F. D. (2000). A theoretical extension of the technology acceptance model: Four longitudinal field studies. *Management science*, *46*(2), 186-204.

Walden, I. (2007). *Computer crimes and digital investigations*. Oxford University Press, Inc..

Wall, D. (2001). Cybercrimes and the internet. In D. Wall (ed.) Crime and the internet. London: Routledge.

Wall, D. (2007). Cybercrime: The transformation of crime in the information age (Vol. 4). Polity

Walsham, G. (2006). Doing interpretive research. *European journal of information systems*, *15*(3), 320-330. Wilcox, P., Land, K., & Hunt, S. A. (2004). Criminal circumstance: a multicontextual criminal opportunity theory. *Symbolic Interaction*, *27*(1).

Weber, R. (2004). The Rhetoric of Positivism Versus Interpretivism: A Personal View. *MIS Quarterly* Vol. 28 No. 1, pp. iii-xii/

Willison, R. and Backhouse, J. (2006). Opportunities for computer crime: considering systems risk from a criminological perspective, *European Journal of Information Systems*, 15, 4, pp. 403-414.

Wilson, J. (2010). Essentials of Business Research: A Guide to Doing Your Research Project. SAGE Publications

Woodside, A. G. (2010). Case study research: Theory, methods and practice: Theory, methods, practice. *Emerald Group Publishing.*

Yar, M. (2013). Cybercrime and society. Sage.Yin, R. K. (2011). Applications of case study research. Sage.

Yin, R. K. (2013). Case study research: Design and methods. *Sage publications*.

Zsidisin, G. A., & Ellram, L. M. (2003). An Agency Theory Investigation of Supply Risk Management. *Journal of supply chain management*, 39(2), 15-27.

APPENDIX A: Ethics Clearance

Faculty of Commerce, Law and Management
University of the Witwatersrand, Johannesburg

School of Economic and Business Sciences
Private Bag X3, WITS, 2050, South Africa • Telephone: +27 11 717 8004 •
email: Siyabonga.Molaba@wits.ac.za

CLEARANCE CERTIFICATE **PROTOCOL NUMBER: CINFO/1107**

PROJECT: **ANALYSIS OF CYBERCRIME ACTIVITY: PERCEPTION FROM SOUTH AFRICAN FINANCIAL BANKS**

INVESTIGATOR: Akwasi Obeng-Adjei

STUDENT NUMBER: **0202802J**

SCHOOL: SEBS

DATE CONSIDERED: 30 June 2016

DECISION OF THE ETHICS COMMITTEE: Approved

NOTE

Unless otherwise specified this ethics clearance is valid for 1 year and may be renewed upon application. Please remember to include the protocol number above to your participation letter.

DATE: 14/07/2016 **CHAIRPERSON: Jean-Marie Bancilhon**

cc: Supervisor:

Prof Ray Kekwaletswe

SCHOOL OF ECONOMIC & BUSINESS SCIENCES

APPENDIX B: Interview Questions

Company Profile

1. Briefly tell me about your company relating your responses to the following:
   a. Type of industry it operates in
   b. The clientele and the services provided;
   c. How business is conducted;
   d. What are the types of channels utilized for conducting business;
   e. How are the services mostly accessed by your clients?
   f. Which points of access or doing business are most vulnerable to crime;
   g. Annual turnover
   h. Number of years in business including the size of your fraud department
   i. Structure and mandate of your business unit in relation to e-Crime.

Perception on factors influencing cybercriminal activity in BetaBank

2. What is the approach to crime in your company, particularly the approach to cybercrime within your organization?
   a. Who defines the cybercrime strategy?
   b. How is the cybercrime strategy implemented once approved?
   c. Is there monitoring and reporting on cybercrime activities
   d. Are there any oversight committees to monitor and assess the effectiveness of the interventions in the organization?
3. Does your company have tools and systems to detect cybercriminal activity? If so, how does it detect cybercrime?
4. What is the general level of understanding of cybercrime in your organization and with your customers?
5. Briefly describe the nature of cybercriminal activities that are pertinent to your organization?
6. What are the types of crimes performed, by whom, how and when do these crimes take place?
7. What are the most common mechanisms cybercriminals use to perpetuate cybercrime?
8. Is cybercrime management a proactive, preventative or detection approach?

9. In your view, does your firm size, management support and IT experience influence cyber-criminal activity?
10. Based on the trends on cybercriminal activity, what are management perceptions on the root cause of cybercriminal activity?

Ways to minimize cybercrime activity within South African banks

11. What are the conviction rates for cybercriminal activity in your organisation?
12. Are there convictions for these crimes when they have been identified?
13. Does the organization have a view of the profile of these criminals?
14. What actions is the organization currently taking against cybercrime?
15. Are the steps being undertaken effective? If not, why?
16. Are there any other factors that lead to cybercriminal activity in BetaBank?

Conclusion *Is there any point discussed previously that you would like to elaborate further on or any other thing you would like to mention?*