TOWARDS A CYBERSECURITY FRAMEWORK FOR SOUTH AFRICAN E-RETAIL ORGANISATIONS

by

PAUL CHIMDIEBERE JIDEANI

Thesis submitted in fulfilment of the requirements for the degree

Master of Technology: Information Technology

in the Faculty of Informatics and Design

at the Cape Peninsula University of Technology

Supervisor: Prof Bennett Alexander

Co-supervisor: Dr Louise Leenen

Cape Town
November 2018

DECLARATION

I, Paul Chimdiebere Jideani, declare that the contents of this thesis represent my own unaided work and that the thesis has not previously been submitted for academic examination towards any qualification. Furthermore, it represents my own opinions and not necessarily those of the Cape Peninsula University of Technology.

Chimdiebere

Signed

11/11/2019

Date

ABSTRACT

With the current in technology and information communications technology devices cybersecurity amongst organisations to deal with a plethora of cyber-ills. Organisations and governments continue to seek ways to improve cybersecurity. This study seeks to understand the cybersecurity environment of e-retail in South Africa. This study is intended to offer and/or inform the creation of a framework for cyber-securing e-retail organisations in South Africa, and to set parameters through which current legislation on cybersecurity can be made relevant to e-retail. It looks into the basis for further research into the security of e-retailers and how it can be used to support the national cybersecurity plan of South Africa in its entirety.

The aim of the study is to identify cybersecurity challenges of e-retail organisations. The study adopted a multiple case study approach. Qualitative data collection methods using purposive sampling (i) direct and in-depth interviews with e-retail company managers and e-retail employees - directly linked to the use and security of critical infrastructure such as technology (ii) document analysis on cybersecurity legislation and frameworks currently in use, as well as other relevant government documents on e-retail in South Africa were used.

Data collected from interviews were analysed using content analysis. The findings, which were presented thematically, constructed the narrative of cybersecurity in South Africa, bringing together cybersecurity challenges. From an organisational point of view, cybersecurity is normally relegated to the background without any emphasis on how e-retailers stand to benefit from operational cybersecurity practices.

The study provides theoretical and practical contributions. A conceptual framework positioning e-retail in South Africa relating to cybersecurity challenges is presented. One new category has been suggested/added to the NIST framework (2014) used called compliance. The NIST framework of 2014 was the framework used as this was the current accepted version at the time of the study. Suggestions for further research were also suggested.

Keywords: Cybersecurity, e-retail, framework, organisations, cyber attacks, cybercrime, legislation, practices

ACKNOWLEDGMENTS

O si na Chim: I thank my Lord for his divine favor and plan for me. From the start of the journey to its conclusion, he has been good. He opens and leaves open and no one shuts it. Without YOU I am nothing.

I wish to thank:

- Prof Bennett Alexander, my supervisor, for his guidance and support. I thank him for being patient with me through this journey
- Dr. Louise Leenen, my supervisor, for her tender care and guidance. Thank you, thank you Louise. My deep sincere appreciation in all ways possible
- Mr Jay Barnes, for his deep insight and contribution to this work.
- The eight organisations, for opening your doors to me and sharing your knowledge with me on this sensitive topic
- The Deeper Life Bible Church (DLBC) Western cape family for their love, support and prayer
- My friends who prayed and supported me in this journey
- Special thanks to my colleagues and all that assisted one way or the other

DEDICATION

I dedicate this thesis to the Glory of God

I dedicate this thesis to my parents, Prof Afam Jideani and Prof Victoria Jideani

I dedicate this thesis to the Church of the living God, in particular the Deeper Christian Life Ministry, where I feed and mature spiritually

I dedicate this thesis to my brothers, Josiah and Timothy Jideani

PUBLICATIONS FROM THESIS

Emanating from this research are some publication outputs:

1. A conference presentation at the International conference on Advances in Big data, computing and data communication systems (icABCD), Durban 6-7th August 2018

2. Publication in IEEE Xplore, see link to view paper https://ieeexplore.ieee.org/xpl/mostRecentIssue.jsp?punumber=8453211

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

GLOSSARY

Acronym/Term/Abbreviation	Explanation/Definition
ABC	An abstract name
Amazon	An electronic commerce and cloud computing company
American Express	A multinational financial services corporation
ATLAS.ti	A software application for qualitative and quantitative data analysis
B2B	Business to business
CCB	Cybercrimes and Cybersecurity Bill
CEO	Chief Executive Officer
CERT	Computer Emergency Response Team
CIO	Chief Information Officer
COBIT	Control Objectives for Information and Related Technologies
CSIRP	Computer Security Incident Response Plan
CSIRT	Computer Security Incidence Response Team
CTO	Chief Technology Officer
CVV	Card Verification Value
CyberCIEGE	A security game designed to teach network concepts
DDOS	Distributed Denial of Service
DOS	Denial of Service
DS	Decision Support
E-commerce	Electronic Commerce
ECT	Electronic Communication and Transaction
EDI	Electronic Data Interchange
ENISA	European Union Agency for Network and Information Security
E-retail	Electronic Retail
Exclusive Books	A bookselling company in South Africa
HIDS	Host Instruction Detection System
HomeChoice	An online product catalog store
ICMP	Internet Control Message Protocol
ICT	Information Communication Technology

IDS	Intrusion Detection System
Incredible connection	A consumer electronic and IT retailer
IP	Internet Protocol
ISACA	Information Systems Audit and Control Association: an international organisation focused on information technology governance
ISO/IEC	International standard organisation/ International Electro-technical Commission
ISP	Internet Service Provider
IT	Information Technology
ITIL	Information Technology Infrastructure Library
ITU	International Telecommunications Union
MasterCard	A multinational financial services corporation
Mr Price	A clothing store chain
NCPF	National Cybersecurity Policy Framework
NGO	Non-Governmental Organisation
NIDS	Network Intrusion Detection System
NIST	National Institute of Standards and Technology of 2014
OSI	Open System Interconnection
P2P	Peer to Peer
PayFast	An online and electronic commerce payment gateway company
PayU	An online and electronic commerce payment gateway company
PCI DSS	Payment Card Industry Data Security System
Pick n Pay	A supermarket chain store
PIDS	Perimeter Intrusion Detection System
POPI	Protection of Personal Information of South Africa
SA	South Africa
Sarbanes-Oxley Act	An act for corporate and auditing accountability of the United Kingdom
SET	Secure Electronic Transaction
SLA	Service Level Agreement
SME	Small Medium Enterprises

SMME	Small Micro and Medium Enterprises
SPF	Sender Policy Framework
SPM	Spoofing Prevention Methods
Sportsmans warehouse	A sports equipment and sportswear store
SSL	Secure Sockets
StormShied	An organisation and product for network security
Takealot	An online store
US	United States
UTM	Unified Threat Management
WannaCry	A ransomware worm
Woolworths	A multinational retail company

CHAPTER ONE: INTRODUCTION

1.1 Introduction

Cybersecurity involves the protection of cyberspace and any assets that can be reached via the cyberspace while taking into consideration threats, vulnerabilities and assets (Reid & Van Niekerk, 2014). The National Cybersecurity Policy Framework (NCPF) describes the cyberspace as “any physical and non-physical terrain created by and/or composed of some or all of the following: computers, computers systems, networks, data, traffic data and users” (South African Government Gaszette, 2015). Cybersecurity is required in all areas that involve the internet and the cyberspace such as e-retail. E-retailing is a form of electronic commerce in which goods and services are obtained over the cyberspace (Mohanraj & Sakthivel, 2016). Deloitte's (2015) emphasizes that addressing cybersecurity in the retail sector has been a great challenge that many businesses and government bodies have been struggling with over the years. As a result, e-retail organisations especially small to medium businesses have increasingly become vulnerable targets of cybercrime. Von Solms (2015) suggests that amongst other factors, a lack of cybersecurity expertise and knowledge makes these businesses vulnerable.

However, having knowledge and expertise is not enough. A tool such as a framework is required, to guide the execution of the business activities against attacsks, towards protecting an organisation from cybercrime (Ghernaouti, 2013). The cybersecurity polices or frameworks need tailoring to the operational peculiarities of the industrial sector. Without an appropriate cybersecurity framework tailored to cater for organisational threats and vulnerabilities, business organisations will remain victims of these cybercrimes and other related activities. The consequence of cybercrime and attacks would ultimately result in unforeseen operational, financial, strategic and other challenges to the organisation and the country at large (Taylor et al., 2014). Evidence shows that these frameworks customized for e-retail exists are few and literature suggests a number of existing frameworks do not appropriately address cybersecurity concerns within the e-retail context. This observation and argument seem to be confirmed by practitioners and consultants, as detailed in the PricewaterhouseCoopers 2014 document (PriceWatersHousecoopers, 2014).

As a result of continuous cybercrimes, organisations, governments and countries have placed importance on implementing cybersecurity policies, legislation and frameworks in order to prevent or minimize the occurrence of cybercrimes (Bessette et al., 2015). According to PriceWaterhouseCoopers (2015), South African organisations experience a high rate of cybercrime. The evolution of internet technology has made cybercrime more prominent making it the 4th most reported type of economic crime. Amongst a number of polices that address cybersecurity currently available, there exists a South African National Cybersecurity Policy Framework (NCPF) which was published in December 2015 and addresses a broad perspective of national cybersecurity guidelines.

Cybersecurity involves the protection of cyberspace and any assets that can be reached via the cyberspace (Department of Justice and Constitutional Development, 2016; South African Government Gazette, 2015). As with many other definitions, scholars have argued and proposed similar or conflicting notions on what cybersecurity is. The NCPF describes cybersecurity as the "practice of making networks that constitute cyber-space secure against intrusions, maintaining confidentiality, availability and integrity of information, detecting intrusions and incidents that do occur, and responding to and recovering from them" (Craigen et al., 2014). The Information Systems Audit and Control Association (ISACA) took a more methodical approach in its definition by suggesting that to understand cybersecurity, cyber-risk must be understood first. Cyber-risk, (which may vary in technology, means or attack vector etc.) is a group of risks that have a potential of severe impact and once considered improbable. The International Telecommunications Union (ITU) in (Korff, 2015), also defined cybersecurity as "the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organisation and users assets" against cybercrime.

1.2 Background of the study

The evolution of the web/internet has transformed the e-commerce over the years and has brought about a need for security in e-retail due to persistent malicious threats and attacks (Smedley, 2014). With the evolution of the internet, cybercrime has become prevalent with small companies increasingly becoming major targets. Amongst many factors small to medium enterprise companies often lack adequate knowledge on how to deal with such cybercrimes (Von Solms, 2015). This rapid growth has brought about communications and transaction with real-time processing of information which could stem from a personal computer to cross-country geographical locations (Gubbi, Buyya, Marusic & Palaniswami, 2013). Besides speed and convenience, anonymity is an umbrella criminals use to perpetrate malicious activities and wide-scale attacks called cybercrimes. As a result of continuous cybercrimes organisations, governments and countries have placed importance on implementing cybersecurity policies, legislation and frameworks so as to prevent or minimize the occurrence of cybercrimes (Bessette, LeClair, Sylvertooth & Burton, 2015).

There has been difficulty in addressing cybersecurity in the retail sector (Deloitte, 2015). Over the past decade, there has been considerable developments in internet technology which has resulted in evolution and sophistication of the threats and risks for small businesses (Bhattacharya, 2015). Reliance on outsourced IT expertise, the emergence of cloud computing, the proliferation of mobile devices, smart devices, and other technological advances have led to recent cybersecurity risks and challenges. SME's remain challenged to survive and guarantee their businesses stay profitable whereas keeping a watchful eye on the potential harm from cybersecurity attacks. (Bhattacharya, 2015).

1.3 Problem statement

In the last decade, cybercrimes and attacks on organisations, specifically on small to medium enterprise that are within the e-retail business have increased. The increase in cyber attacks and organisations vulnerability are not a result of a lack of remedies or security tools, but the generic nature of the tools. Each organisation is unique, in areas such as setting, processes, activities and culture. Literature evidence suggests that existing cybersecurity policies and some frameworks are not addressing e-retail organisations needs. Customization of frameworks is needed for individual organisations specific needs and requirements. The problem is that the existing generic policies and frameworks are challenged with inappropriate addressing and mitigating against cybersecurity concerns within the small to medium enterprises within the e-retail context (PriceWatersHousecoopers, 2014). This problem manifests into consequences such as financial losses and information theft, which affects competitiveness and sustainability of many organisations. If this problem is not addressed, the damages and losses that are encountered through cyber attacks can only get worse.

1.4 Research Aims and Objectives

The aim of the research is:

- to understand the cybersecurity environment of e-retail in South Africa.
- to propose the elements that should be included in an e-retail cybersecurity policy.

1.5 Research Questions

1.5.1 Main Question 1

What are the specific cybersecurity challenges faced by e-retail organisations?

I. Sub-question 1

What are the peculiarities of the e-retail industry in terms of cybersecurity?

II. Sub-question 2

What measures have e-retail organisations taken to comply with current cybersecurity laws?

1.5.2 Main Question 2

How can South African e-retail organisations mitigate against the occurrence of cyber attacks?

I. Sub-question 1

How can South African e-retail organisations ensure cybersecurity practices?

II. Sub-question 2

What should characterize a cybersecurity e-retail framework?

1.6 Summary of Research Questions

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

Table 1.1: Research questions, methods and objectives

Research Question 1	*What are the specific cybersecurity challenges faced by e-retail organisations?*	
Research Sub-Question 1	**Method**	**Objectives**
What are the peculiarities of the e-retail industry in terms of cybersecurity?	Interview, Document analysis	To determine compliance measures taken by e-retail organisations.
What measures have e-retail organisations taken to comply with current cybersecurity laws?	Interviews, Literature study	To know what elements are required to ensure the cybersecurity of e-retail organisations.
Research Question 2	*How can South African e-retail organisations mitigate against the occurrence of cyber attacks?*	
Research Sub-Question 2	**Method**	**Objectives**
How can South African e-retail organisations ensure cybersecurity practices?	Document analysis, Multiple case study	To determine the degree to which cybersecurity frameworks are used to ensure cybersecurity
What should characterize a cybersecurity e-retail framework?	Interview, Literature Study	To determine the necessary elements for an e-retail framework

1.7 Key Concepts

Table 1.2: Clarification of terms

Term	Clarification
Cyberspace	Cyberspace is as “any physical and non-physical terrain created by and/or composed of some or all of the following: computers, computers systems, networks, data, traffic data and users” (South African Government Gazette, 2015).
Cybersecurity	Cybersecurity involves the protection of cyberspace, the elements that operate in the cyberspace and devices that can be reached via the cyberspace. It takes into consideration the threats, vulnerabilities and assets (Reid & Van Niekerk, 2014).
Cybercrime	Cybercrime is “any crime that is facilitated or committed using a computer, network or hardware device”(Sarah & Ford, 2006).
e-retail	E-retailing is a form of electronic commerce in which goods and services are

	obtained over cyberspace (Mohanraj & Sakthivel, 2016)
Policy Framework	Is a document written to facilitate protection of critical infrastructure and to safeguard personal identifiable information used by organisations for business purposes, so as to regulate how personal information is processed (South African Government Gazette, 2015).
Cybersecurity policy framework	A strategic document to guide cybersecurity in South Africa (South African Government Gazette, 2015).
E-commerce	E-commerce refers to the buying and selling of products over the internet, or any transaction completed via electronic means (Kumar & Bharati, 2016).

1.8 Outline of Thesis

The thesis is comprised of seven chapters in total followed by the list of references and appendices. All the chapters that make up the entire body of this study have been organised in a way that they inform and support each other in forming the entire argument for this study as shown in figure 1 below. The introduction, which is the current chapter introduces and provides the rational for the study to make the reader understand the subject of investigation. In this chapter, the problem statement, research aims, objectives and research questions inform the reader of how the argument of the thesis develops until the conclusion chapter of the study. The second chapter of this study is the literature review, which informs the reader about the issue of cybersecurity and e-retail business in South Africa. The main purpose of the second chapter is to intimate the reader about the current state of cybercrime in e-retail in South Africa, as well as steps and measures that undertaken to mitigate the issue of cybercrime. The literature review also goes further to point out some of the intiatives across the globe dealing cybercrime and cybersecurity. Chapter three informs the reader about the research methods and techniques that were undertaken to collect and gather data on cybersecurity across the e-retail business organisations in South Africa. It also provides a justification and reasons for the use philosophies, methodology and methods. Chapter five; is a presentation of findings obtained after carrying out the process stated in chapter three. Chapter six provides a discussion on those findings against literature and lastly Chapter 7 providing conclusion and recommendations of the entire study.

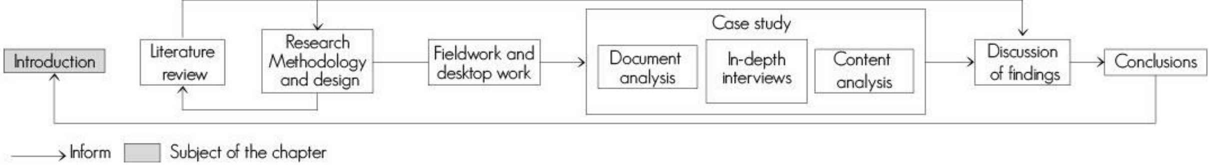


Figure 1.1: Organisation of chapters in thesis

1.9 Significance and Delineation of the Study

This study is seeking to propose a cybersecurity framework for e-retail organisations and not necessarily to make/create a policy or framework. Synthesis of South African cybersecurity policies and frameworks are interpreted and analysed. The rationale behind this is that evidence suggests consideration was given to international standards during the creation of these National policies.

1.10 Conclusion of Chapter 1

The current chapter provided a background to the research problem under study in this thesis. This chapter has highlighted the background of the research, research problem, the aims, and objectives, the research question, sub-questions guiding the research, the definition of terms, and delineation of the research. On the definition of key terms, key concepts about this research were stated for easy understanding of the reader. This chapter also gave a basic overview of thesis layout by clearly presenting what to expect in each section of the thesis. This chapter discussed the introduction and background to the challenges associated with lack of having a proper cybersecurity policy for small to medium enterprise businesses, the research question, the aim and objectives, the clarification of concepts as well as the limitations of the study. The purpose and motivation of this research is to understand the cybersecurity environment of e-retail in South Africa and to propose the elements that should be included in an e-retail cybersecurity policy. The next chapter is Chapter 2, based on literature that provides a background for this research.

CHAPTER 2: LITERATURE REVIEW

2.1 E-Commerce

2.1.1 History of e-commerce

As far back as 1960, companies conducted electronic transactions using Electric Data interchange allowing primitive computer systems to share business documents such as invoices, quotation forms (Roos, 2008). In 1979 Michael Aldrich who is considered to be one of the pioneers of ecommerce successfully implemented the first online shopping system (Phillips et al., 2004). In 1982, the Transmission Control Protocol TCP was created which developed into the commonly well-known and used world wide web service. And in 1990 Tim Berners-Lee world wide web server and created the first web interface which presently is known as a browser (Phillips et al., 2004; Roos, 2008). In 1995, Jeff Bezos sold the first ever book over the internet on Amazon.com which opened up a terrain, which consequently became known as e-commerce. With rapid development in internet related services the launch of google in 1998 as a major frontier in internet based technology evolved. The early 2000 which saw a rise in the internet sector as a result of the world wide web known as the Dot-com bubble or digital revolution (Teeter & Sandberg, 2016). As a result of this increase in internet based activities in 2004 credit companies such as VISA, MasterCard, American Express saw the need to create the Payment Card Industry Data Security Standard (PCI DSS) as a compliance standard for card payment security (Gikas, 2010).

2.1.2 Scholarly definitions of e-Commerce

There is a lack of consensus on a formal definition of electronic Commerce, a subject of debate amongst authors with varying definition according to the premise in which it is used. Roger Clarke (1999) defines e-commerce broadly as the “conduct of business with the assistance of telecommunications, and telecommunications-based tools”. Roger Clarke explains that e-commerce goes beyond procurement of goods but also electronic services delivery. Coppel (2000) describes as the “selling goods and services which are delivered offline as well as products which can be ‘digitised’ and delivered online.” In addition Dan (2014) presents as “business, technology, society and skills of buying and selling of products and services with the aid of internet and computer or handheld devices which involves the process of ordering products or services to the time of delivery to the customer.” E-commerce is encompassing all the various electronic business activities within an organisation commonly called e-business: which is “transforming business process using internet technologies” such activities include e-payments, e-procuring etc. (Mirescu & Maiorescu, 2010). Secure trading of information, products and services by computer networks that involves the exchange of value online and support for business transactions over some digital infrastructure. Which is often from business to customer or in some cases business to business (Buhalis, 2016). From the variant definitions described above in a concise manner e-commerce can be defined as a process of conducting electronic transactions over the internet, an electronic medium (Henderson, 1999; Adeyeye, 2008; Dan, 2014).

2.1.3 Major types of e-Commerce

Due to increase in e-commerce technologies, transactions that take place during the exchange of goods and services could take different paths as they move from one entity to another. These paths form the types of e-commerce. 2 main types of e-commerce exists though authors and writers have suggested additions, for this study the major types of e-commerce put forward by Shim, Pendyala, Sundaram, and Gao (2000) will be taken as the major types of e-commerce as they are considered all-inclusive of any other types of e-commerce. The following is one the major types of e-commerce:

Business-to-Business

Business-to-Business abbreviated (B2B) has been conducted as early as in the early 90's with transactions between Dell and Cisco. B2B e-commerce has progressed in recent years (Kaplan & Sawhney, 2000). It involves businesses buying and selling amongst themselves, where both buyer and seller are business entities. The electronic support of business transactions to form electronic relationships with suppliers and distributors (Turban et al., 2009). A type of business where businesses depend on other businesses for several direct or indirect inputs to its end product. For example, a computer manufacturer depends on one or more companies to provide processor chips and other hardware devices. B2B automates and streamlines buying and selling intermediate products (Shim et al., 2000). Business- to-business ecommerce is a fast growing sector in the online trade space which is expected to generate revenues of $6.7 trillion by 2020, as manufactures and wholesalers move from legacy systems to open, online platforms Frost & Sullivan (2015). Online trading saves companies costs by removing overheads such as rentals and office spaces, all these enabled with technology and other interconnected devices to make transactions more efficient. The ubiquity, affordability and enabling technology of the web has made is possible for business organisations to automate and transact their B2B interactions (Sarah & Ford, 2006). This research takes a business-to-business approach, providing solutions to organisations on how to protect critical infrastructure.

2.2 E-Retail

Electronic retailing has over the years been given numerous names such as e-tailing, e-shopping an abbreviation for electronic shopping etc. E-retail will be used in this research to denote electronic retailing, is the sale of goods or provision of services through the internet or other electronic channels, for use by consumers (Dennis, Fenech, Pantano, Gerlach & Merrilees., 2004). From the definition, it involves all e-commerce activities that result in transactions with end consumers. It involves all activities involved in selling goods to the final consumer (Kamisli & Alegoz, 2017). To supplement the definition above e-retail is a branch of e-commerce that involves the selling goods or services to larger markets. All activities such as inquiries, ordering, purchase and goods or a service are conducted electronically until the good or service is delivered to the specified customer (Fernie et al., 2013). Within the e-retail as will be discussed in the course of the literature has a number of components it interacts with, therefore e-retail is not solely a goods providing but also could render a service as a product or as means to obtain a product. This is important and should not be overlooked.

2.2.1 Overview of E-Retail in South Africa

According to Goldstuk (2016) South Africa has continued to experience growth in online retail with an annual rate growth of 20%. Having a current market share of about R9billion of a total retail sector share of R900 billion, stakeholders have forecasted a double increase in the amount by 2020. However, the author raises an issue that online retail in South Africa is still in its infancy and its falling behind western developed markets. This is creating a market divide consisting of high performing set of e-retailers and a grappling majority.

In the continent, South Africa is marked with one of the countries to have a high internet penetration rate with a number of technology savvy users. However, the rate at which users adopt online retailing is not encouraging. This calls for the need for improvement in its innovative strategies for e-retailing (Durham, 2011; Goldstuk, 2016; Alexander et al., 2016). In addition, the penetration of e-commerce in South Africa is only about 1% of the entire retail market compared to 13% and 15% of the US and China, who are major pioneers of e-commerce (Gernon, 2017). The e-commerce penetration rate will continue to rise as more avenues and users are brought on board. Some of the evident key propellants of online retailing is South Africa highlighted by research conducted by (Mybroadband, 2015) are: (i) lower product costs (ii) faster delivery (iii) flexible delivery options (iv) secure methods of payment. Concerns have been raised about payment methods such as security and privacy. Also, reluctance of users to give away their personal information has been a major hindrance to participation in e-retail in South Africa (Alexander et al., 2016). However, with the proliferation of mobile devices and the resultant shift from using desktop devices will further drive online retail in South Africa (Mybroadband, 2015). In South Africa, the table below shows top 12 online retail stores based on market share in South Africa

Table 2.1: Top 10 e-retail stores in South Africa by Market share

Top e-retail stores in South Africa	
Shop	Market Share (%)
Takealot	12.5
Apple App Store	5.5
Pick n Pay	5.1
Woolworths	2.7
Sportsmans warehouse	2.2
Incredible connection	2.0
Exclusive Books	1.8
HomeChoice	1.6
Amazon	1.5
Mr Price	1.5

Source : (Bratt, 2018)

2.2.2 E-Retail ecosystem/landscape

According to literature and a deep examination of e-retail below is a conceptualisation of the elements that orbits around an e-retail organisation. The e-retail organisation at the core. Secondly, physical connected environment at the next orbital level: these are considered as the actors or areas which service the e-retail organisation. The actors include: (i) banking which facilitates payments and financial transactions. (ii) Service providers: these are third parties that provide resources to the e-retailer, such as web development houses, data storage facilities or any other form of third-party amenity. (iii) Supplier: these provide products to the e-retail, there exists situations where the supplier is fully integrated into the system of the e-retail organisation where a dedicated system is made available to the supplier to manage, a very important aspect worthy of note. However, in some cases the supplier is a separate entity, not having any rights to systems. For the purpose of the research, the delivery service was intentionally omitted, as it does not directly influence ecosystem which will be presented in this study. The legislative framework at the outer orbital, which governs the operations of the e-retailer. The legislative framework recognises salient global, regional and national legal imperatives that support cybersecurity for e-commerce. The legislative framework will evolve using desktop research.

2.3 Cyberspace

An electronic environment created by interconnected networks of ICT, a realm of communication and interaction between computers facilitated by data exchange via the internet (Newbould & Collingridge, 2003). The South African Government Gazette (2015) defines as “physical and non-physical terrain created by and/or composed of some or all of the following: computers, computer systems, networks and their computer programs, computer data, content data, traffic data and users". The US Cyber Command (2008) defines the cyberspace as "a domain characterized by the use of electronics and electromagnetic spectrum to store, modify and exchange data via networked systems and associated physical infrastructure". The cyberspace is a major technology-enabled medium providing locus of internet traffic and exchange data. It is the housing block of all ICT and networks with the technology and the internet being a significant enabler (Goodman, 2008).

2.4 Cybercrime

There has been varying descriptions and definitions given to cybercrime, differing based on the perception of the observer and investigation at hand. Ascribable to the intricate nature of cybercrime there has been no official definition of cybercrime, however different scholars, governments and agencies provide subjected definitions based on what they seek to address (Tsakalidis & Vergidis, 2017). Sarah and Ford (2006) defines cybercrime as "any crime that is facilitated or committed using a computer, network or hardware device". Similarly it is any criminal offence committed via the internet, computer network. From the earlier definitions, the European commission on EU law issued a publication and proposed to define cybercrime in 3 aspects:

1. Traditional crimes committed through electronic communication networks and information systems
2. Any distribution of illegal content over electronic media and,
3. Crimes unique to electronic networks (Anderson, Barton, Bhöme, et al., 2013).

Taking a closer look at the definitions above a few aspects can be deduced:

- In the case of cybercrimes, the computer or electronic device could be the agent of the crime
- The facilitator of the crime or the target of the crime

A more concise and encompassing attempt to the definition of cybercrime was proposed by the Council of Europe's Convention on Cybercrime (2001) as: "crimes committed via the internet and other computer networks, dealing with particularly with infringement of copyright, computer related fraud, child pornography, and violations of network security." Of salient note is an additional definition which refers to cybercrime as "cyber-space offences" that are "either committed against integrity, availability and confidentiality of computer systems and telecommunication networks or consist of the use of such networks of their services to commit traditional offences. (Committee of Experts on Crime in Cyber-Space (PC-CY), 2001; Tsakalidis & Vergidis, 2017)"

In summary of the above deduced points it takes place using or targeting computer networks and devices. This research proposes to follow the definition: “any crime that is facilitated or committed using a computer, network or hardware device” suggested by Sarah & Ford, (2006) as it satisfies the dual nature that the computer, network or hardware device could be the means to commit or the target entity. Cybercrime envelopes a broad scope of activities associated with the use of IT for criminal motives. There is an increasing streamline between traditional crimes perpetrated through the use of ICT (Kraemer-Mbula et al., 2013). This increase presents a significant threat to businesses in particular SMME’s, organisations and to national economies at large. The current global financial damage caused by cybercriminals is estimated to be $225 billion (Anderson, Barton, Bhöme, et al., 2013). In addition, cybercrime poses a significant threat to safety, and well-being of society. PriceWaterhouseCoopers, (2015b) propounds that cybercrimes are not only numerically increasing but also are becoming progressively destructive and target a wide assemblage of information and attack vectors. Due to the global nature of the internet illegal activities are perpetuated by criminals all over the world. More so, the internet knows no boundaries making it a challenge to contain illegal activity over the internet, networks and hardware. Therefore, it is essential countries make cybersecurity a priority (Parodi, 2013). Cybercrime a newly coined term has been practiced as early as the inception of the internet and in recent years has experience progression in the manner and scale to which cybercrime is carried out.

Cybercrimes have become issues of global issue of concern. This has prompted countries to strategically developed goals to counteract cybercrimes from affecting the society and economy. A number of countries have successfully developed and implemented policies while other countries are still in the early stage of developing policies related to cybercrime. Some nations are yet to understand the severity of the surge of cybercrimes (Wegener et al., 2004; Stewart et al., 2017). Majority of these countries are in the continent of Africa and other developing nations across the globe. South Africa as a nation has experienced a rise in cybercrime since 2003. However, South Africa has recognised cybercrime as a challenge to its national security, as a result has placed structures in place to curb its expansion. With collaboration with government, private sector and organisations: cybersecurity hubs have been established as Computer emergency response team to serve as to-go places in the event of a cyber attack. It has also improved the ICT infrastructure of the Virtual cybersecurity hub by reconfiguring and hardening its perimeter (Department of Government Communication and Information System, 2016).

2.4.1 The evolution of cybercrime

The advancement and dissemination of the internet and computer technology has brought about an increase in sophistication of cybercrime (Silva, 2017). The internet has unravelled an abundance of benefits to society in an age heavily reliant on information. Though there are positive benefits the internet provides when used for licit purposes, there are also illicit activities carried out using the internet and these have escalated in recent years giving birth to 'cybercrime'. Today, cybercrime has emerged as one biggest threats to our information and internet-dependent society (Dashora & Patel, 2011; Riek et al., 2016; e Silva, 2017). From the first computer virus created in 1988 called the Morris worm to the early 2000s were information stealing on infected computers and fast-forward to today widespread attacks that aim to cripple critical infrastructure, internet based terror attacks and major threats to national security (Silva, 2017).

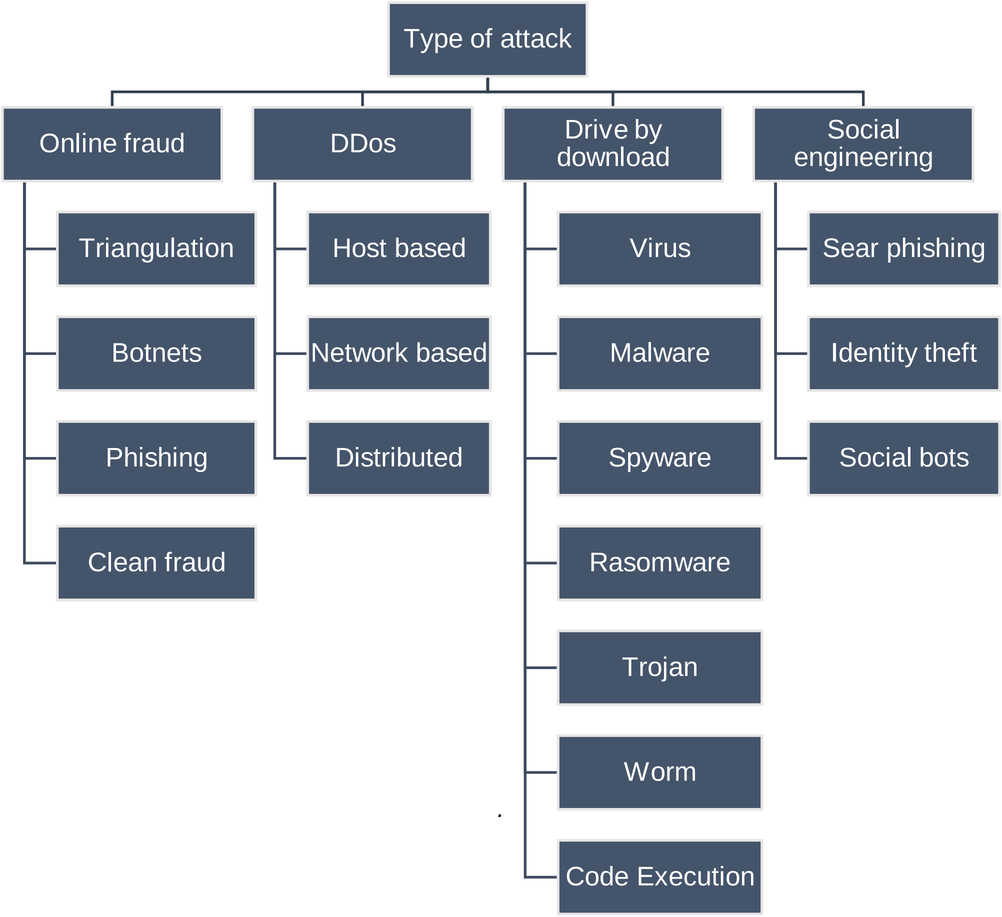
Cybercrime has shown a substantial rise in recent years, its effect of cybercrime on businesses has shown a considerable effect in later years from viruses, hacks, ransomware to steal confidential information. With the development of innovatory security devices and protocols which are arguably more reactive than proactive to security continue to fall short of restraining cybercrimes. Given the wide array of cyber-attacks that businesses such as (hacks, denial of service, malware etc.) with the anonymity the internet provides, makes it immensely difficult to trail and pinpoint cyber-criminals.

2.5 Cyberattacks

Closely linked to cybercrime are cyber attacks. Cyber attacks specific attempts to gain access or control over information stored on computer networks (Kiggins, 2014). They are deliberately targeted events to alter, disrupt or destroy computer systems, networks or information (Gonzalez, 2015).

2.5.1 Types of cyber attacks

In order to extensively identify as much cyberattacks prevalent today a taxonomy of cyberattacks is presented. A taxonomy is an orderly classification of objects, people or other phenomena according to a predefined natural relationship with each other (Burton et al., 2004). The purpose of a taxonomy is to simplify identification of different individual elements in a complicated universe (Miller, 1967). In order words, taxonomies can be adopted to reduce the complexity of a knowledge domain. Cyberattacks being the knowledge domain in this context.



Source: (Shabut, Lwin and Hossain, 2017)

Figure 2 above presents a taxonomy of cyberattacks that organisations and the ICT community have to deal with. Note that this is not an exhaustible list of cyberattacks notwithstanding it gives a clear representation of general cyberattacks. It is also important to note that these may not all be targeted at the commerce industry. Online or internet fraud is described by Cross & Kelly (2016) as the use of the internet to make a request, dishonest invitation or offer by providing personal information or money that leads to financial or non-financial impact of some kind. A dubious deceitful business transaction carried out electronically with an intention to defraud. Online fraud has become a major challenge to e-commerce. Online fraud involving e-commerce could be from using stolen credit card details to purchase goods online to more sophisticated schemes using email addresses or impersonating a buyer to transact business. They are in most times very complex and appear to be legitimate (Nandy, 2010).

2.6 Cybersecurity

Cybercrime is an ill cybersecurity seeks to address, as an approach to handle crime that occurs within the cyberspace. As with many other definitions scholars have argued and proposed similar or conflicting notions of what cybersecurity. The National Cybersecurity Policy Framework of 2014 describes cybersecurity as the “practice of making networks that constitute cyberspace secure against intrusions, maintaining confidentiality, availability and integrity of information, detecting intrusions and incidents that do occur, and responding to and recovering from them.” “The organisation and collection of resources, processes and structures used to protect cyberspace and cyberspace-enabled systems from occurrences that misalign de jure from de facto property rights” (Craigen, Diakun-Thibault, & Purse., 2014). The Information Systems Audit and Control Association (ISACA) took a more methodical approach in its definition by suggesting that to understand cybersecurity, cyber-risk must be understood first. Cyber-risk (which may vary in technology, means, attack vector etc.) are a group of risks that have a potential of great impact and once considered improbable. In view of that Cybersecurity is the sum of efforts invested in addressing cyber-risks. Kissel (2013) says the ability to protect the cyberspace from cyberattacks. The International Telecommunications Union (ITU) defines cybersecurity as “the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organisation and users assets” (Korff, 2015).

2.6.1 The need for cybersecurity in e-retail

Cybersecurity is not optional; it is a necessity given the world transition from traditional marketing to selling and buying of goods and services over the cyberspace. Thus, protecting technological infrastructure commonly known as critical infrastructure (technology, application, hardware, network and data) requires security as these are the fundamental building blocks for an ICT driven society. Several reasons justify the need for cybersecurity in e-retail as a priority. Among these reasons, include the need to encourage wide range of acceptability of e-commerce.

Statistics reveal that cybercrime is growing faster in Africa than in any other continent, as 80 per cent of PCs on the continent are reported to be infected with malicious software (United Nations Economic Commission for Africa, 2014). In many developing countries, there seems to be a reluctance by individuals to e-retail or online purchase. A survey conducted by MasterCard in Kenya indicated that 38% of the respondents were not that the online transaction was secure. As is the case in many African countries this fear is not unfounded given that Kenya loses about 2 billion annually on cybercrime (Mastercard, 2014; Kigen et al., 2014). This discourages the growth of e-retail due to dissatisfaction with the security of transaction. As internet penetration expands, so also is the rate of cybercrime. As some authors have suggested that cybercrime is internet penetration driven (Park et al., 2017). Cybersecurity is an old new plague affecting organisations, industrial sectors and countries. Cybersecurity will instill trust in e-retail, trust will stimulate customers expectation of a secure transaction as well as eliminate uncertainty and perceived risk. When adequate security is put in place there will be no reluctance from customers to adopt e-retail (Kim et al., 2009; Yıldırım, 2013).

In the event of a cyberattack the financial loss could be severe, cyber-insecurity could incur large amount of financial loss. In 2014 there was a reported $2.7 million financial loss annual attributed to cybersecurity incidents. The absence of cybersecurity could lead to financial loss and could incur remediation costs within or external to the organisation (PriceWaterhouseCoopers, 2015a). In addition to these losses, recovering from a breach can be costly as systems have to be investigated, cleaned and repaired, and new operations are implemented to prevent future attacks. Due to the uncertainty, as to where the attack could originate from could be from within the organisation or external, the consequence could be catastrophic and if not contained could negatively tarnish the organisations image resulting in harm to reputation, erode customer relationship and potentially eat into revenue. The ever-present muster of threats emphasizes the growing necessity for organisations to develop cybersecurity programs that weaves preventative measures into business operations and processes (Kpmg, 2000).

The intricacy and sophistication of cyberattacks calls for the need for proactive cyber-defense measures. Also, the cybercriminals carrying out the small or wide scale attacks are becoming more skilled and adapt to circumvent protection that have been placed. SME’s face challenges due to limited resources such as expertise, information, finance. Thus, need cybersecurity to protect their cyberspace containing intellectual property, trade secrets are sensitive information (Von Solms, 2015). There are multiple reasons for conducting cyber-attacks against the e-commerce sector. With the dependence of trading on the sector, an attack could be used to affect trade in general, or even target a specific commodity. As a result of the interconnection and interdependence of the various e-commerce infrastructures, there are a variety of targets to impact the trade: service providers could be targeted to prevent transaction from going through. Customer information could be stolen to commit phishing and impersonation.

2.7 Cybersecurity legislation and frameworks

With the nearly 40% growth in hacking and other cyber incidents every year, various governments the world over have taken a prominent role in defining new requirements for corporate information security. This is being achieved by passing new legislation and revising or adoption new regulations. They also collaborate with the private sector and NGO’s in the development of policies, standards and best practices to achieve stronger cybersecurity protection and safeguard confidential information from loss and theft. Governments have responded to various ways due to the complexity and diversity of cybersecurity risk and their evolving nature (CREATe, 2016).

Some governments have taken it further by taking up direct actions by requiring the cybersecurity of various public and private networks and systems. Other actions include the encouragement of the development of frameworks, standards and best practices that industries can adopt. Some have drafted new requirements that are general and high level, with protective and prescriptive measures. Some of these requirements are mandated by specific government legislation, while others are implemented by regulatory bodies (Passman, 2016). In addition, focusing on some of the various legislation, frameworks and standards designed to help organisations protect information more effectively against cyber breaches at various levels.

2.7.1 International legislation

In this section, we discuss and report on International legislation around which e-retail is based on. Well-developed countries have made major strides in trying to deal cybercrime. Hence, attention to strategies developed by advanced nations in order to curb the cybercrime.

National Institute of Standards and Technology (NIST) Version 1.1 2014

A common cybersecurity framework developed at an international level is NIST, a well comprehensive, risk-based tool for managing information security among different types of businesses and organisations. The framework was developed through a series of workshops, research and data gathering from the public and private sectors. Developed by NIST the framework was titled "Framework for Improving Critical Infrastructure Cybersecurity" is a risk-based collection of guidelines that aid organisations to identify, implement and improve cybersecurity practices (Shen, 2014). The framework provides an evaluation mechanism that enables organisations to determine current cybersecurity capabilities, set specific goals and implement a plan for improving and maintaining cybersecurity initiatives (Shoemaker et al., 2016). The framework is composed of 3 primary components namely: Profile, Implementation tiers and Core. The profile component enables organisations to align cybersecurity practices based on peculiar business needs, tolerance for risks and available resources. It contains practical guidelines on how to secure critical infrastructure called framework cores and provides a array of tasks to achieve specific cybersecurity outcomes which include key functions such identify, protect, detect, respond and recover. Core activities can be used to align an organisations cybersecurity activities or initiatives with business requirements (Shen, 2014). Scofield (2016) suggests the NIST framework provides a common language platform on how organisations can keep and secure online information. Further, Perakslis & Stanley (2016) indicate that the NIST cybersecurity framework in conjunction with the NIST Risk management framework provide model approaches for assessing cyber risks and determining a budget for protecting IT systems and data which can be used as tools for development of further suitable frameworks for organisational specifics. To start with, organisations create a profile of their existing cybersecurity efforts against the recommended practices in the framework. Which include: process, procedures, technologies etc. (PriceWaterhouseCoopers, 2015a; Sigler & Rainey, 2016).

Implementation tiers as main functions within an organisations labelled as Identify, Protect, Detect, Respond and Recover and goes further to break into 22 categories and a further 98 sub-categories of activities and outcomes relevant to the development of an effective cybersecurity profile and implementation plan (NIST, 2014). It also adds to it a wide spectrum of risk assessment and management functions, specific IT and physical (hardware) security protections. In addition, it takes cognisance of the 'people and process factor' such as management oversight, third-party and supplier responsibilities, training and communication, response planning and ongoing improvement (CREATe, 2016).

PriceWaterhouseCoopers (2015) in its publication titled "managing risks in an interconnected world" warns that there is no one-size-fits-all solution for cybersecurity, going further to say that it is not possible to provide a comprehensive, prescriptive guideline for all entities across industries. Therefore, it calls for organisations to identity unique threats and attacks specific to their business. An effective cybersecurity program requires that organisations are aware, identify and understand specific threats and apply commensurate safeguards. Organisations have some statutory, contractual and regulatory obligations which are not addressed in the NIST framework. Ultimately, the framework provides for adaptability to cater across industry, providing an effective way to establish baseline, set targets for improvement and continuously evaluate progress (Drolet, 2017).

European Union Agency for Network and Information Security

The ENISA was set up in 2004 to contribute to the overall goal of ensuring a high level of network and information security within Europe. ENISA helps the member states and business community to address and respond to network and information security issues (Mitrakas, 2007; Levi-Faur, 2011). The main activities run by ENISA include:

- Monitoring security incidents and emerging risks in Europe.
- Encourage risk assessment and management methods to intensify capacity to deal with information security threats.

- Facilitating of pan-European cyber exercises
- Assisting CERTs cooperation in the member states
- Raising awareness in the information security field between different actors.

It main tasks is to advise the EU commission on salient issues to the safety of networks, hardware and software. It fosters EU security by aggregating electronic information and identifying risks before they occur through data assessment and management (Entrust Datacard, 2012; Skopik et al., 2016; ENISA, 2017).

2.1.1 National legislation

In this section, we discuss and report on South African legislation around which e-retail is based on. Earlier sections have established the landscape of e-retail and all its consists of. These are legislations that should govern any form of e-commerce activity within South Africa. E-retail which falls under e-commerce as previously examined relies heavily on ICT. Therefore, what governs the use of ICT in terms of legislation are the information technology laws/acts.

National Cybersecurity Policy Framework

The NCPF is a 95-page document that itemises roles to be played by government, private and civil society sectors in an attempt to ensure a safer cyberspace in South Africa. In addition, it also established reporting bodies known as CSIRTS responsible for receiving and handling cyber related matters, acting as a point of contact for coordination for Cybersecurity. The first draft of the NCPF was written in 2010, approved by government in 2012, and published in December 2015. The intention of the NCPF is to create a cyber-secure environment that facilitates protection of critical information infrastructure by:

a) Measuring nation-wide security in terms of cyberspace.
b) Measuring strategies to combat cyber warfare, cybercrime and other cyber ills.
c) Development, review and change existing substantive and procedural laws to confirm alignment.
d) Measuring confidence and trust in the secure use of ICT.

Besides its purpose the NCPF highlights some key objectives which the framework seeks to achieve. The NCPF will:

a) Centralize coordination of cybersecurity activities
b) Forster cooperation and coordination between all role players.
c) Promote international collaboration.
d) Develop required skills, research and development capacity.
e) Encourage a cybersecurity culture

f) Promote compliance to cybersecurity standards.

Amongst a number of areas, the NCPF seeks to address is to ensure safe and secure cyberspace environment enabling the growth of e-commerce and an all-inclusive information society (South African Government Gazette, 2015). The NCPF intends to identity role players which are the (state, public private sector, society and special interest groups) seeking for measures to promote their involvement in relation to cybersecurity threats. This is necessary to ensure a focused and all-encompassing security response within the cybersecurity environment (Burmeister, Phahlamohlaka & Al-Saggaf, 2014). The NCPF is considered a national approach for a single comprehensive strategy that guides cybersecurity in South Africa. However, Mohideen, (2016) in a critical review of the NCPF describes it as a being too vague and general with no practical specific implementation strategies in place which was earlier echoed by (Jansen van Vuuren et al., 2013) also describing the framework as very high level. Hence, there is a need for appropriate frameworks which would practically address cybersecurity concerns at various levels, which one of the objectives of the NCPF to encourage compliance with appropriate technical and operational cybersecurity standards. This policy provides a national strategy to aspects of cybersecurity which can be used as a blueprint to take on a cybersecurity plan by respective sectors of society whether in public or private capacity.

Protection of Personal Information Act (POPI)

Provides the protection of the right to privacy of individuals. Companies are obligated to apply reasonable security to protect personal information. In the case of this act personal information relates to demographics (age, gender, race), history (medical financial, criminal), biometric information, personal opinions etc. One major component within the e-retail ecosystem or landscape as discussed earlier is the finance (payment) element which often requires the financial records of an individual. This is an element covered by the POPI act which to be adhered to by e-retail organisations.

There are 8 information processing principles which form the core of POPI, though principles are important the 7th principle is relevant to this study which is the security safeguards it states that responsible party must secure the integrity of personal information, by taking organisational measure to prevent loss, damage, destruction and unlawful access to or processing of personal information. Furthermore, the responsible party must give due regard to accepted information security practices and procedures which may apply to it generally or be required in terms of specific industry or professional rules and regulations (South African Government Gazette, 2013).

Electronic Commission and Transactions Act

The Electronic communication and Transaction Act is another information technology law passed in 2002 with a purpose set out to facilitate and regulate electronic communications and transactions, develop national e-strategy, promote universal access to electronic communication and transactions and the use of electronic transaction by SMMEs(Government Gazette, 2002).

Cybercrimes and Cybersecurity Bill

The Cybercrimes and cybersecurity bill was published in December 2016 under the ministry of justices and correctional services. The aim of this bill impose penalties on crimes related to cybercrime, it grants the state powers to investigate cases of cybercrime and impose obligations on electronic communication service providers and financial institutions to assist in the investigation of cybercrimes (The Department of Justice and Constitutional Development, 2016). This bill is the latest information technology bill published for review and public comment with an aim set out to describe types of cybercrime and offences, creation of a government and private sector CSIRTs, cybersecurity structures, and identification, regulation and compliance of national Information Infrastructure (Department of Justice, 2015; Mohideen, 2016).

The primary goal of the bill is to properly handle cybercrimes and enforce security. The bill highlights how the bill will achieve national cybersecurity, a few are mentioned below

- Provides assistance to deal with cross-border investigation of cybercrime
- Providing establishment structures such as cybersecurity hubs, CERTS to promote cybersecurity capability building
- Provides measures to protect critical infrastructure
- Establishment of a 24/7 cybersecurity reporting centre to facilitate mutual assistance for cybercrime events
- Imposing of cybersecurity obligations on electronic service providers and financial institutions.

This bill has been criticized for its overly broad mandate and stating it gives the government full rights to control the internet of the country (Turianskyi, 2018).

2.8 Summary of cybersecurity policies and frameworks

At this point, it is important to clearly differentiate with a legislation, policy, policy framework and framework. A policy can be defined as "a course of action, guiding principle, or procedure considered expedient" (Von Solms & Von Solms, 2004). A framework is a generic solution to a generalised problem that provides common applicable ideas (Ford et al., 2014). Policies are high-level broad aspect addressing certain areas while frameworks specially address a need from the cybersecurity legislation and frameworks discussed above, the table below categorises the

Table 2.2: Categorisation of policies and frameworks

Document	Policy	Framework
National Institute of Standards and Technology (NIST) Version 1.1 2014		✓
European Union Agency for Network and Information Security (ENISA)	✓	
National Cybersecurity Policy Framework	✓	
Electronic Communication and Transaction Act	✓	
Cybercrimes and Cybersecurity Bill	✓	
Protection of Personal Information Act	✓	
Information Technology Infrastructure Library (ITIL)		✓
Control Objectives for Information and Related Technologies framework (COBIT)		✓

2.9 Technological aspect to Cybersecurity

Policies and frameworks are important but it will not prevent cybercrimes from occurring. From the statement, there seems to be an element of truth to this, however, it does play a vital role in the fight against cybercrimes. Therefore, not having legislation as a guide will certainly stand as a hindrance to security implementations. As defined earlier in this chapter, cybercrimes involve or make use of ICT, technology is one of the main driving forces of cybercrime, and therefore it is intuitive to seek technological solutions to technological problems.

2.10 Technologies for Cybersecurity implementation

Cybersecurity focuses on addressing the confidentiality, integrity and availability of IT systems. Cybersecurity takes a holistic end-to-end viewpoint of protecting enterprise computing resources, through identification, detection and recovering of assets, risks and malicious behaviour. Some cybersecurity technologies to support identification, detection and recovery include, role-based authentication, encryption, firewalls, intrusion detection systems and vulnerability assessment tools (Leszczyna, 2018). Cybersecurity is necessary but not sufficient for cyberspace operations. Cyberspace operations require its own set of technologies such as reconnaissance tools, software development tools, passive scanning and decision support. Some cybersecurity technologies do overlap with cyberspace technologies but the level and privilege to access will differ (Lathrop et al., 2016). There are a plethora of old and emerging cybersecurity technologies, each implemented based on the required objective. The following section addresses some cybersecurity technologies.

2.10.1 Encryption

Encryption involves presenting data in an unreadable form. Encryption ensures confidentiality, making sure that only authorized entity can read the data (Ankita & Lavisha, 2012). Encryption is a technique of securing data (plain text) to ciphertext, with the aim of restricting unauthorized access or persons. Encryption to date plays an important role in cybersecurity and in particular data security (Singh & Soni, 2018). Encryption is beneficial to e-commerce and e-retail, as transaction continues to grow there is a need to encrypt customer data which are personal identifiable information. Organisations are responsible for customer data and the security of data; therefore, encryption is necessary a technological tool to achieve this. In U.S organisations must ensure proper security systems are installed to protect customer data from all fraudulent activities. In addition, organisations are encouraged to explore the feasibility of encryption of data (B & Little, 2001). Encryption has provided a secure pathway to protect credit card numbers in transmit from consumer to merchant from being stolen. Not only can it be used to secure data in transit, it can also be used to secure data at rest i.e. data stored in storage devices (Shrivastava, 2014).

Everyone using the internet for buying and selling needs to be concerned about the security of their personal information.

Encryption protocols have been widely adopted by organisations that handle data and payment information. Secure Sockets Layer (SSL) and Secure Electronic Transaction (SET) are commonly used encryption protocols (Liao & Cheung, 2003). SSL an encryption protocol introduced by Netscape and today has become essential for secure online transactions used to protect sensitive data (passwords, credit card number etc.) and applications. It works by establishing a secure link between the web server and browser to ensure private and confidential data transmission. To obtain a secure internet transaction, a web server requires an SSL certificate to establish a secure connection. What makes the method secure is that encryption happens above the transport layer, making use of the asymmetric mechanism of public and private key (Byron & Green, 2007; Modi, 2016). Another encryption protocol is SET, introduced by Visa International and MasterCard to protect e-commerce payment transactions. It operates by using digital certificates to authenticate the customer, payment gateway and the merchant. SET provides a high level of security requiring special encryption software on both client and server side, as a result it is not widely used (Byron & Green, 2007). These encryption protocols accepted and used globally, SSL is cost effective and the recommended protocol to be used for securing data and transaction.

2.10.2 Access control technologies

Access control is "a process by which use of system resources is regulated according to a security policy and is permitted only authorised entities (users, programs, processes, or other systems) according to that policy" (Shirey, 2007). From the definition, it involves allocation of user rights and permissions to access resources; it is primarily focused on assets and resources. Within every organisation that makes use of ICT, a well-defined access control mechanism is crucial to provide authorised access to ensure asset security and business operation (Chaisiri & Ko, 2016). There are technologies solutions to ensure access control at various levels and for different needs, the sub-section below discuss a few.

2.10.3 Intrusion detection systems

Intrusion detection systems are a set of software applications installed to regulate and monitor inbound and outbound traffic from a system (Donaldson et al., 2015). IDS helps to block malicious traffic travelling through the network. The use of IDS are closely linked and work together with the firewall, to restrict access to assets and system resources. The aim is to prevent denial of service attacks (DOS) from taking place. There are four commonly known categories of IDS, briefly described below:

Network intrusion detection system (NIDS)

NIDS operates within the network by monitoring network traffic by comparing traffic with a signature file that details a list of likely malicious activities with an aim of detecting malicious activity such as spams, DOS attacks (Banday & Mir, 2012). NIDS is an IDS that monitors network traffic into and out of the network. It operates by reconciling the packet flow with a known signature. There are advantages and disadvantages to IDS. The advantage of signature detection is that already known attacks can be detected and escalated. The disadvantage is that the signature will need to all known and new attacks, attacks that are not in the signature are known as zero-day attacks (Sherif & Ayers, 2003; Patcha & Park, 2007). Zero-day attacks are attacks that are not known to the signature within the IDS.

Host-based intrusion detection system (HIDS)

It recommended that small organisations adopt a blend of host and network-based IDS to identify ongoing attacks. This would aid in reducing business risks from possible security breaches that could outwit the implemented preventative measures (Raghavan et al., 2017). NIDS and HIDS are able to detect unsuitable or abnormal activities that likely affect a systems confidentiality, integrity and availability status (Banday & Mir, 2012). However, there have been noticeable to intrusion detection systems

Perimeter Intrusion Detection System (PIDS)

From the word ‘perimeter’ depicting a physical boundary of an area, the role of perimeter security systems is to function as the first level of area protection. Area boundaries are defined and an alert occurs at any intrusion attempts. This type of IDS adheres to the security rules that include: define, deter, detect, delay and detain any intrusions into the protected area (Hakim et al., 2016). This system provides the capability to notice and locate the location of intrusion attempts on the perimeter barrier of critical infrastructure. Using some electronic cabling technology fitted to the perimeter barrier, the PIDS notices anomalies on the barrier and in the event an intrusion is noticed an alert is triggered (Yadav, 2018). PIDS seeks to protect physical devices and areas, using various forms of RFID, sensors and smart mechanism to restrict and authorise access to a particular area. It is used to identify activity critical infrastructure (Adamsky et al., 2018). Another important aspect linked to perimeter security which organisation are advised to practice is a physical separation between network and critical systems. In the disaster, there is no destruction to the entire infrastructure of the organisations.

Biometric identification

Biometric security is an authentication technique which relies on physical characteristics to authenticate a user. The use of biometric security and biometrics is a cybersecurity technology in use today. Biometrics is one of the many methods to provide security to e-commerce. Individuals have unique biometric characteristics as a result there is less chance for an attack. There are several biometric identification schemes such as fingerprint, retina, voice, facial recognition (Kumari et al., 2016). E-retail organisations can incorporate biometric identification into their websites and applications. The use of fingerprint identification can be used during checkout on smartphones and smart devices; this is to provide additional level of security.

CHAPTER THREE: RESEARCH APPROACH AND METHODOLOGY

3.1 Introduction

The scope of this chapter is to provide foundational guidelines and order of steps that narrates how the researcher collected and analysed the data in this study. The underlying research problem underpinning this study is that there is little evidence of existing frameworks customized for e-Retail businesses. Evidence also points out that the majority of these small to medium e-Retail business organisations are unaware of the cybersecurity frameworks to reduce cybercrime (PriceWatersHousecoopers, 2014). A number of these policies do not appropriately address cyber-security concerns within the e-Retail context. With this lack of clarity, and inappropriate application of cyber-security frameworks in their daily operatives, small to medium e-Retail business organisations will remain victims of cybercrimes and other cyber-related activities ultimately resulting in unforeseen operational, financial, strategic and other challenges to the organisation and the country at large (Taylor , Fritsch & Liederbach, 2014).

The rest of this chapter is presented as follows: section 3.2 presents an outline of the key elements derived from the NCPF Policy Framework that will be used to develop a cyber-security framework for small to medium e-Retail businesses in South Africa so as to address the issue of cyber-security. In this regard, the link between the e-Retail ecosystem (Figure 3.2) and the research tool in detailed section below. This is then followed by the research paradigm and philosophy that was undertaken for this study in section 3.3. Justifications for the research paradigm and the epistemology are also provided in this section. A discussion on methodology, data collection procedures and data analysis procedures that were used to analyse the collected data is also presented in section 3.4 to 3.6. Finally, this chapter culminates with ethical considerations and a chapter conclusion from section 3.7 to 3.10. This section opens with a brief discussion on the e-Retail ecosystem followed by the research paradigm adopted for the current study.

3.2 Research design

A research design is useful to ensure that the proof obtained permits the investigator to answer the research questions as clear as possible (De Vaus, 2001). There are approaches to a qualitative inquiry, a research study could be set off to explain (explanatory), explore (exploratory) or describe (descriptive) (Creswell & Poth, 2017).

3.3 Research Philosophy and paradigms

The research paradigm is also a representation of ontology and epistemological points of view on the nature of existence, knowledge, and ways of knowing (O'Leary, 2007). Conferring to (Burke, 2007; Creswell, 2013), a research paradigm or philosophy can be defined as an investigation of foundational concepts and the requirement to understand a particular field through established knowledge claims. A paradigm presents a rational and motivation for conducting a scientific study. A research paradigm is also formed around fundamental array of philosophical supposition: ontology and epistemology. Ontology refers to our premise about how the world is viewed, e.g., is the world seen as a social order or continual change (Bhattacherjee, 2012a; Bhattacherjee, 2012b). Epistemology refers to our premise about the ideal way to study the world, for instance, the trade-off between undertaking a objective or subjective approach to study social reality. In information systems field, the two major conflicting research paradigms namely the positivist (Burrell and Morgan's functionalist paradigm) and the interpretivist. Within these paradigms lie the other schools of thought. Each paradigm boasts their own value and restriction (Burke, 2007).

3.3.1 Ontology

According to Burrell and Morgan (1979), ontology refers to our premise about how we view the world, for instance does the world composed of social order or constant change (Bhattacherjee, 2012a; Bhattacherjee, 2012b). Ontology is also concerned with the nature of reality and how it exists to the assumptions individuals have about the world, the entities within the world and how they operate(Saunders, Lewis & Thornhill, 2009).

Objectivism and subjectivism are two features of ontology, the view of entities regardless of social actors and the view of entities from the perception and consequence of social actors. Since the aim of this study is to understand e-Retail challenges pertaining to cybersecurity and to understand the peculiarities of the e-retail sector, the subjective ontology standpoint would be applied to this study. The current ontological landscape of e-Retail consists of various elements such as customer, data, networks, databases and legislation that should govern the e-Retail environment. This research seeks to understand legislation that governs e-Retail in South Africa. E-Retail falls under Business-to-Customer type of commerce and the aim is to build a cyber-security framework based on this type of legislation.

3.3.2 Epistemology

According to Burrell and Morgan(1979), an epistemological stance to any qualitative inquiry or investigation is informed by the phenomenon being investigated by the researcher which relates to the ontological presuppositions. This will determine the research paradigm to be taken, including positivism, interpretivism, critical realism. However, for the purpose of this research, the functionalist paradigm was adopted. According to Burrell and Morgan (1979), the functionalist paradigm seeks to provide meaning to social affairs.

From the researches view, if the world consists of social orders (ontology) and thus seeks to study patters of ordered events or behaviours. In addition, believes the ideal manner to study such a world is through an objective approach (epistemology) which is independent of the researcher conducting the investigation (Bhattacherjee, 2012a). However, if the researcher perceives that the best manner in which to study social order is by the subjective interpretation of participants involved such as conducting interview and interpreting differences amongst responses using the researcher own subjective perspective, then it means an interpretivism paradigm is being employed. If the researcher seeks to introduce radical change and seeks to understand change objectively, then the radical structuralism paradigm is employed. Lastly, if the researcher seeks to introduce radical change and seeks to understand change subjectively, then the radical humanism paradigm (Bhattacherjee, 2012b).

Functionalist paradigm

According to Burrell and Morgan (1979), the functionalist paradigm seeks to provide meaning to social affairs. A functionalist paradigm is a problem-oriented approach to research providing solutions to problems. It also seeks to provide an understanding to the status quo, the status quo in this research is an understanding on the current legislation that governs e-Retail in South Africa so as to build a cyber-security framework based on this legislation to prevent cybercrime. On these grounds, a functionalist approach is important to understand the problems e-retail organisations face and understand how they come about, this will, in turn, speak to a solution on the development of guidelines to reduce the occurrence and impact of this social problem. To date, a lion share of social science research has mimicked the natural science and functionalist paradigm. Functionalists are of the view that social order or events can be perceived in terms of their functional components, and as a result try to break down a problem into smaller components, then further study components in detail objectively (Bhattacherjee, 2012a; Bhattacherjee, 2012b). Since this study is not seeking to understand why e-retail organisations experience cybercrime; this research assumes the fact that there are cyber attacks and seeks to provide defense strategies to small and medium e-retail organisations on how to remain cyber secure.

In addition, a functionalist paradigm also provides explanations to social happenings and to generate regulative sociology (Ardalan, 2008). Thapa and Harnesk (2014), explains that the implementation of practices to protect information assets from attacks falls within the functionalist paradigm with the supposition that risks are controllable & predictable and that solutions exist out there. To minimise cybercrimes in organisations it is important to understand the problems e-retail organisations face and understand how they come about, this will in turn speak to a solution on the development of guidelines to reduce the occurrence and impact of this social problem.

3.4 Research approach

Research approach can be defined as a “systematic, rigorous investigation of a situation or problem in order to generate new knowledge or validate knowledge” (Majid et al., 2012). In this line of argument, a systematic concept follows a prescribed process, this implies vigorous, coherent and replicable steps and guidelines for undertaking an inquiry. Again, coherent assumption suggests that it follows a methodical, logical and consistent set of scientific methods (Amaratunga et al., 2002). In addition to the coherent and methodical concept, it also involves selecting the most appropriate methods and techniques to carry out the process of inquiry (Pope & Mays, 1995; Kitzinger, 1995; Creswell, 2003; Creswell, 2013). Therefore, a research design can be explained as a framework that specifically details regarding the required procedure that needs to be in conducting the research (Sreejesh et al., 2014). A detailed research approach is based on relevant paradigms that indicate a direction in which knowledge can be seen and analysed (Burke, 2007). According to O’Leary (2007), a typical research approach incorporates paradigms, conceptual and theoretical frameworks, as well as appropriate methods and techniques for designing research, collecting, analysing and interpreting data.

3.4.1 Qualitative research

Qualitative research approach refers to a set of methods and techniques of collecting and analysing data through explanations and context interpretations (Creswell 2003). Qualitative research focuses on investigating the phenomenon and its context. Qualitative research techniques also allow a richer insight into an observation. In this study, the qualitative research approach was based on developing a multiple case study on how cyber attacks could affect e-Retail businesses in South Africa and how to defend against such attacks. In qualitative research approach the researcher postulates knowledge claims based on constructivist perspectives (this means various interpretation of individual experiences, meanings socially and historically constructed, with an intention of developing a theory or pattern) (Creswell, 2003). Qualitative research approach also utilises other strategies of inquiry such as narratives, phenomenologies, ethnographies and grounded theory studies (Creswell, 2003). This research made use of multiple case studies where the researcher collects open-ended, emerging data with a main purpose of developing themes from the data on the cyber attacks that affect e-Retail businesses and how to defend against such attacks.

3.5 Research Strategy

Research strategy provides a clear direction of the research as it helps the researcher to conduct research systematically (Kilani & Kobziev, 2016). In addition, research strategy is an approach to capturing engaging practitioners to acquire knowledge and develop appropriate theories (Benbasat et al., 1987). A research strategy is also a methodological process through which research objectives can be questioned appropriately (Emhemed & Pandey, 2017). In this line of argument, it is methodological because the researcher follows some certain regime of methods, often referred to as scientific methods. To conduct research in qualitative manner and in particular in information systems, there are several research strategies which could be employed such as ethnography, grounded theory, phenomenological research and case studies. Each one of these methods is briefly explained in the following sections below:

3.5.1 Case Study

According to (Creswell, 2003), a case study is a qualitative research strategy in which the researcher explores in considerable detail a program, an event, an activity, a process, or one or more individuals. Case studies are activity and time-bound, where researchers gather comprehensive information using a variation of data collection procedures over a prolonged period of time (Stake, 1995). In this research, multiple case study is used as the research strategy. A multiple case study approach is essential as it enables an investigation of contrasts within and between cases as will be explained in detail in the following sub-section.

3.5.2 Multiple case study

A multiple case study is a thorough enquiry into a unit which is aimed to generalize over several units (Gustafsson, 2017). It also involves in-depth analysis of particular units for example. place, thing, organisation to make an inference across populations. On the other hand, a multiple case study helps to better and fully understand the phenomenon under investigation (ibid). It focuses on replicating findings from different cases through which comparisons can be drawn (Baxter & Jack, 2008). A multiple case study as a qualitative research strategy also includes an investigation which involves empirical understanding of a specific phenomenon within its real context using diverse sources of evidence (Rostam et al., 2017). Using multiple case study is beneficial as it strengthens research findings similar to how multiple or repeated experiments strengthen validity of experimental research findings. In addition, bias of collection and analysis of case data can be minimised by using multiple cases and could reveal aspects unknown to the researcher (Darke et al., 1998; Dubois & Gadde, 2002; Yin, 2013). The e-Retail organisations are considered as the case for this research. The amalgamation of synthesis of legislation, data collected from e-retail organisations presents and fulfils the case for a multiple case study.

According to Bhattacherjee (2012a), when conducting a multiple case study where evidence is obtained from several sites; one needs to systematically analyse and synthesis the data to allow ideas and patterns to emerge for the aim of building new theories or increasing existing ones. To do this, there is usually a set outline of procedures normally followed by researchers when collection or gathering multiple-case studies data (Bhattacherjee, 2012a). Such procedures that were followed by the researcher are as follows:

Define research questions. This stage similar to other scientific enquiries, compelled the researcher to start the case research by providing research questions that are theoretically and practically compelling, and identifying some possible answers to those research questions (Bhattacherjee, 2012a). The second stage was the **Selection of case sites.** In this stage the researcher used a process of *"theoretical sampling"* to identify case sites. In this approach, case sites were chosen on theoretical, rather than numerical considerations. Maximum detail and attention was undertaken to ensure that the selected sites suit the context of research questions (Bhattacherjee, 2012a).

During initial contact with case sites, the researcher described the purpose and attention of the research investigation, the manner in which data will be used. The researcher also assured confidentiality, privacy, and anonymity of both the individual and the respective organisation they represent.

The third stage also known as the **Creation of instruments and protocols** is one whereby the researcher came up with an interview protocol. An interview protocol was necessary to act as a guide during the interview process (Bhattacherjee, 2012b). The interview protocol normally details a series of questions to be asked, ranging from open-ended (unstructured), closed-ended (structured). There was strict adherence to the interview protocol, and the interviewer did not alter the order of questions, although some deviations were necessary inorder to probe further into pertinent respondent's comments that are unclear and require more clarification. The interviewer also maintained a neutral position, not trying to bias the respondents towards a specific answer or response (Bhattacherjee, 2012a).

Additionally, the researcher also had to **select respondents** at different organisational levels, this is in order to obtain divergent and different perspectives on the phenomenon of investigation. In this selection process, interviewees were selected based on their personal involvement with the phenomenon under investigation and their ability and willingness to answer the researcher's questions accurately and adequately, and not based on convenience or access. This research took up a multiple case study strategy as unit of analysis were taken from a wide range of pool of cybersecurity experts. The final stage was **commencement of data collection.** This will be discussed in section 3.7

3.6 Procedures and techniques

3.6.1 Unit of analysis and observation

The unit of analysis, as stated by Graneheim and Lundman (2004), are the variety of objects of study. The unit of analysis in this study was identified as small to medium sized e-Retail organisations that engaged in a form of electronic commerce in South Africa, which is a secondary source of data used in this research. The e-Retail organisations are considered as the case for this research. The unit of observation are the specific entities that data was sourced from. Non-random, purposive and convenient methods were used to identity observation units. For this study, information security officers or personnel bearing the role of information and security managers were the unit of observation. Once the researcher was able to determine that the research question is best answered using a qualitative case study and the case and its boundaries have been determined, then the researcher had to consider what type of case study will be conducted. The selection of a specific type of case study design had to be guided by the overall study purpose. Since the main objective was to explore the issue of cyber-security with in e-Retail business organisations across South Africa, the researcher ended up adopting a multiple case study as explained above

In summary, the unit of analysis is the entity (what or who) is being studied or investigated (Elo et al., 2014). The unit of analysis for this research will be the e-Retail organisations in South Africa where primary data will be collected from. The unit of observation will be the specific personnel or role/office bearers in the e-Retail organisations such as information security managers.

3.6.2 Sampling technique

Sampling can be described as a process of selecting a representative size of subjects from an entire population to further examine, using what is learnt to gain insight into a phenomenon in a larger context (Neuman, 2011). Each subject in the sample size is referred to as the unit of analysis. It involves the selection of a segment of the population or a subset of a population for an investigation. The complexities in collecting data from an entire research population which will be practically impossible creates the need for sampling. Another important consideration to sampling is the size, the size is determined by the ideal number necessary to permit valid inferences to be made of the general population (Marshall, 1996). There are certain approaches to selecting samples, this method of selection is based on a probability or non-probability approach Bryman (2015).

Probability Sampling

Probability sampling is a sampling technique used where the population size and location are known, with an accurate chance of selecting the sample at least once (Neuman, 2011). According to Bhattacherjee (2012), all probability samples have two attributes. Firstly, every entity in the population has a non-zero chance of being chosen. Secondly, it involves a random selection. Each entity in the population has an equal opportunity of being selected (Bradley, 1999). There are different types of probability sampling techniques such: as simple random sampling, systematic sampling, stratified sampling and cluster sampling. Due to time, contact and resource constraints it will be impossible to access the entire e-retail population in South Africa, thus an alternative sampling method was adopted for this study. This is discussed in the next section below.

Non-Probability Sampling

Non-probability sampling is a sampling technique where the chance of selection cannot be accurately determined. Selection is based on a non-random criteria (Bhattacherjee, 2012b). In non-probability sampling, the researcher has control over the selection process which is based on the discretion of the researcher as a result of that it is subject to bias (Tansay, 2007). Selection is also based on certain characteristics that will yield the desired data. Non-probability sampling is often used as it provides the necessary data to understand the phenomenon of interest (Parahoo, 2014). In this study, the research population fits the description of selecting a non-probabilistic sample because the number of information security personnel, as well as the e-retail organisations are widely dispersed in so much that they cannot have equal chances of being selected as a research sample. Furthermore, types of probability sampling technique include: quota sampling, convenience sampling, purposive sampling, snowball sampling (Bhattacherjee, 2012b). However, purposive sampling was chosen as the sampling technique in relation to the objective of this study – to understand elements to minimise cyber attacks in e-retail organisations.

3.7 Data collection

Data collection is a process of gathering information from participants during a scientific investigation (Bhattacherjee, 2012b). Lewis (2015) also described the process of data collection as a series of interrelated activities designed to gather information. According to Hox and Boeije

(2005), in qualitative study, the data collection methods used are generally flexible and sensitive to the social context. There are also various procedures that are used to gather data such as questionnaires, interviews, focus groups and observations. These techniques enable the researcher to obtain the necessary or required information to carry out an investigation. Hox and Boeije (2005) also stated that data collected in any qualitative inquiry can be classified into primary data collection and secondary data collection. According to Hox and Boeije (2005), primary data is original (first-hand) data collected by the researcher for the purpose of answering the research objective. While, secondary data is data that has been collected, stored by other researchers in the form of documents and literature (Daas, 2012; Hox & Boeije, 2005; Bhattacherjee, 2012b).

Since this study seeks to understand the cyber-security environment of e-retail in South Africa within the retail sector, Table 3.6 below is an indication of how the data will be collected leading to the development of a framework. By looking at the cyber attacks currently happening in the e-retail sector; the research seeks to find out how these attacks can be stopped by looking at the current e-retail ecosystem. Table 3.6 below shows how the research will be conducted leading to the development of an e-retail framework.

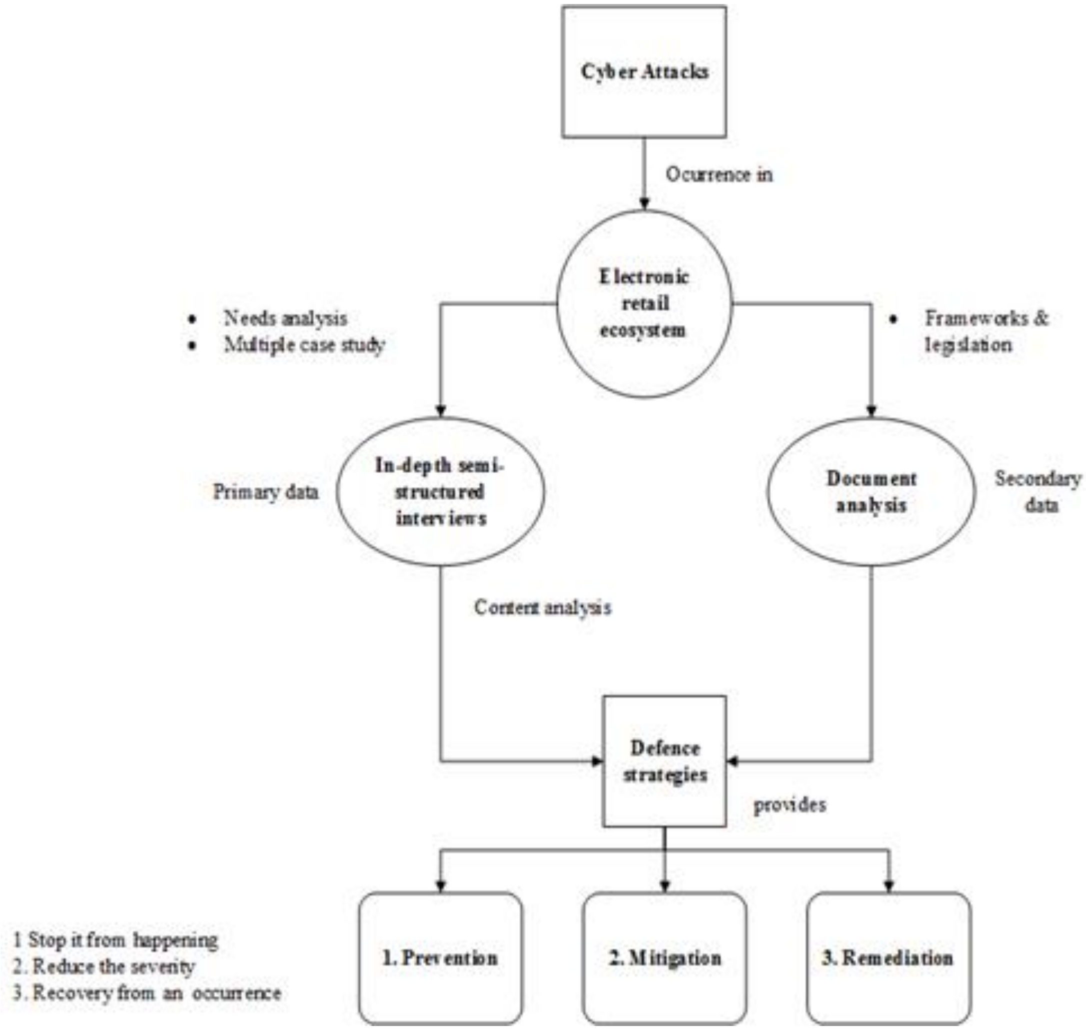


Figure 3.1: Data collection outline

However, for the purpose of this study, the empirical dataset consisted of e-Retail store databases from retail stores in South Africa. For this particular study, nine e-retail information security personnel from e-retail organisations across South Africa were purposefully selected. These e-retail and cybersecurity experts were then interviewed in the form of in-depth semi-structured interviews over a period of six months at their retail stores. Secondary data in the form of document analysis was performed on local and international legislation using the NCPF as a theoretical lens. Document analysis and in-depth unstructured interviews were employed to collect data (Bhattacherjee, 2012b).

3.7.1 Semi-structured interviews

In a semi structured interview; the interviewer ensures that he keeps the interview limited to the topics that are essential to the research. The interviewer at his discretion can make use of appropriate wordings and allocate a specific time for each question to encourage the respondents to provide details for relevant responses (Sreejesh et al., 2014). This technique calls for close discussion and interactions with experts, the interviewer must possess knowledge of the latest trends in the field of discussion. Although advantageous in many respects, the technique is known to have no provision to allow the interviewer to probe into unrelated issues cropping up during the interaction, which were not a part of the discourse (Sreejesh et al., 2014). The study made use of this type of interview as it allowed for deeper insights into cybersecurity, in addition the interviewer is able to provide rich and beneficial information outside the questions asked. The interviewer was able to provide information on that are important in cybersecurity based on experience and knowledge. From the e-retail ecosystem presented e-retail covers a number of aspects, therefore to fully understand how to secure e-retail different cybersecurity experts were interviewed. Such as Chief information security, payment gateway experts, government personnel, cybersecurity researchers and security engineers.

3.8 Data analysis

Data analysis involves the process of gathering information collected from data collection to make meaningful sense required to answer research questions. It is a process of engaging with text to summarise what is emerging from it, to gain deeper understanding of the meanings within the data to answer objects of the investigation (Grbich, 2013). This study is based on a qualitative research approach, where qualitative data was collected to gain in-depth understanding of e-Retail cybercrime challenges. The following analysis techniques namely: document analysis, content analysis and thematic analysis were used to analyse data for this research. By using multiple methods of data collection such as interviews and document analysis, it offered the opportunity for validating data through the triangulation process which provides valid conclusions to the researcher's conclusions. The key elements of data analysis were also critical to written results of research (Benbasat et al., 1987). As much as possible, the context and richness of data should be clearly presented, and a clear sequence of proofs established. The researcher's rational in establishing causality or drawing out hypotheses was also clearly stated and defended. Through this process, the research moved from objectives and questions, to assumptions and design choices, to specific data uncovered, and finally, to the results and conclusions (Benbasat et al., 1987). The process of data analysis is explained in a greater detail in sections below.

3.8.1 Qualitative content analysis

In this study, qualitative content analysis is defined as a research method for the subjective interpretation of the content of text data through the systematic classification process of coding and identifying themes and patterns (Hsieh & Shannon, 2005). In addition, qualitative content analysis also involves a structured examination of the content of a text (e.g., who said what, to whom, why, and to what extent and with what effect) in a qualitative approach. Qualitative content analysis is one of numerous research methods available to analyse text data (Hsieh & Shannon, 2005). Other methods include ethnography, grounded theory, phenomenology, and historical research. By using qualitative content analysis, the researcher is able to focus on the characteristics of language as a communication medium with intention to the contextual meaning of the text (Budd, Thorp & Donohew, 1967; Lindkvist, 1981; McTavish & Pirro, 1990). The qualitative content analysis process went beyond merely counting words to examining language intensely for the purpose of classifying large amounts of text into an sufficient number of categories that represented similar meanings (Hsieh & Shannon, 2005). The idea of qualitative content analysis is “to provide knowledge and understanding of the phenomenon under study” i.e cybercrime in e-Retail business organisations and how cyber-security can be used to prevent or mitigate such impact of cybercrime within the e-Retail sector of South Africa (Hsieh & Shannon, 2005).

Content analysis process

In this study, the qualitative content analysis process was conducted as follows. First, there were many texts to analyse (e.g., bills, articles, blog postings, online reviews and critiques, etc.), the researcher began by sampling a selected set of texts from the population of texts for focused examination. This process was not random, but instead, texts that have more pertinent content were chosen selectively. Secondly, the researcher identified and applied rules to divide each text into partitions or “chunks” that were handled as separate units of analysis. This process is called unitizing. For example, assumptions, effects, enablers, and barriers in text may constitute such units. During the third stage, the researcher constructed and applied one or more concepts to each unitized text segment in a process called coding. For coding purposes, a coding scheme was used based on the themes the researcher was searching for. Finally, the coded data was analysed qualitatively, in order of frequency of themes, in what contexts, and the relationship between them (Hsieh & Shannon, 2005).

The data qualitative content analysis process also started with repeated reading of all data to achieve immersion and obtain a sense of the whole (Hsieh & Shannon, 2005). Thereafter, data was perused word by word and highlighting the precise words from the text that appeared to capture key thoughts or concepts. Next, the researcher approached the text by jotting down notes of his first impressions, thoughts, and initial analysis (Miles, M.B. and Huberman, 1994; Hsieh & Shannon, 2005). As this process continued, labels for codes emerged that were reflective of more than one key thought. These came directly from the text and were selected as the initial coding scheme. Codes were sorted into categories based on how different codes were related and linked. These emergent categories were used to organize and group codes into meaningful clusters (Coffey, A. and Atkinson, 1996; Patton, 2002).

Depending on the relationships between sub-categories, the researcher can combine or organize the larger number of sub-categories into a smaller number of categories. Lastly, definitions for each category, sub-category, and code were developed. To prepare for reporting the findings. With a conventional approach to content analysis, relevant theories or other research findings are addressed in the discussion section of the study.

3.8.2 Document analysis

Bowen (2009) defines document analysis as a methodical procedure of reviewing or assessing both printed and electronic material. In this line of thought, document analysis is methodical because it necessitates locating, choosing, appraising and synthesising data contained in documents (*ibid*). According to (Gorichanaz & Latham, 2016), document analysis involves a thorough evaluation and assessment to understand the documents in question. The process of document analysis starts with selecting documents on the basis of relevance to the research (Olson, 2010). The researcher made use of document analysis as it was chosen to be right tool to scrutinise both local and international polices that include aspects of e-commerce, cyber attacks and cybercrime in them.

3.8.3 Data coding

Data coding is a procedure through which data is analysed, conceptualised and then reassembled in new ways. Data coding assisted the researcher in analysing the data to support the identification and development of key ideas from which meaning was drawn from (Strauss & Corbin, 1998). Atlas.ti was used to present in-depth interviews [see appendix D] and document analysis data to produce main themes and sub-topics from data. The interviews were recorded in audio format and then were transcribed using online web application called otrascribe

The coding technique involves a process of classifying and categorizing text data partitions or a set of codes (concepts), categories (constructs), and relationships. Strauss and Corbin (1998) describe three coding techniques for analysing text data: open, axial, and selective. Open coding is a procedure focused at identifying concepts or important ideas that are obscure within text data, which are potentially related to the phenomenon of investigation. The researcher examines the raw text data sequentially to identify discrete events, incidents, perceptions, and interactions of relevance that are coded as concepts (hence called in vivo codes). Each concept is linked to specific portions of the text (coding unit) for later validation. Some concepts may be simple, clear, and unambiguous while others may be complex, ambiguous, and viewed differently by different participants (Bhattacherjee, 2012a).

3.8.4 Use of Atlas.ti

This current investigation relied on various new computer-aided designs and techniques for thematically analysing qualitative content analysis data. The use of Atlas.ti, a program that has been used by many theorists in various fields, including information systems, was adopted for this research (Zhang & Wildemuth, 2009; Friese, 2011a). The use of Atlas.ti also helped in the process of automating various processes in the analysis of qualitative content such as cataloguing primary documents, organising of codes and code descriptions (Zhang & Wildemuth, 2009; Friese, 2011b; Menter et al., 2011). In addition, Atlas.ti also allowed the researcher to organise and catalogue all data in a complete and efficient way. In addition to the aforementioned strengths, Atlas.ti also made possible connections (relations) between codes, themes and sub-themes, as well as networking. Further to that, networks developed created the opportunity to highlight different relationships, similarities and differences (Kelle, 2004 :483; Lu & Shulman, 2008:105-107). Friese (2011b) also underlined the importance of Atlas.ti in asserting that Atlas.ti effectively manages search data by organising codes alphabetically, presenting code strength and graphically representing data.

3.9 Data Quality management

3.9.1 Confidentiality

Anonymity and confidentiality are of paramount importance to ethical research practices in social studies (Wiles et al., 2008) . Therefore, interview participants were assured of the efforts made to ensure the information provided as well as personal details about the sources remained anonymous (ibid). Furthermore, participants were also informed the research was purely for academic purposes. Therefore, the information gathered will only be used towards completing a university master’s degree. Pseudonyms in form of alphanumeric codes were also assigned to the names of the participants to protect their names and identities.

3.9.2 Ethical Considerations (Ethics and Consent)

Ethical considerations is an important aspect of social research which is a criteria to ensure confidentiality and anonymity of participants in carrying out research (Babbie, 2016). To comply with this requirement consent letters were obtained from all participants involved in the research. An ethical clearance letter was obtained from the Cape Peninsula University of Technology Ethics

Review Committee. This letter was to inform the participants of the research purpose and what it involves, further stating that participation was voluntary and confidential, giving the right to withdraw without reason. Permission was obtained from various e-Retail organisations, information obtained from e-Retail organisations was also kept anonymous, confidential and safe.

The research participants in the study were also not forced to take part in the study without their knowledge and consent at the time of data collection. This study did not involve participants who did not to give their consent. The research subject did not include discussion of sensitive topics, nor did it require invasive or potentially harmful procedures of any kind to collect the data. Before data collection commenced, ethics research applications were sent for approval by the Faculty of Informatics and Design at CPUT's Research Ethics Committee. Only after the application was approved, data collection took place. The participants indicated voluntary willingness to participate in the research. Additionally, the research aims and objectives were explained in this study to ensure that the interview participants met the requirement for the sampled selection criteria (Shenton, 2004) .

After agreement from the participants, interviews were scheduled. The dates and times were carefully chosen considering the demanding schedule of the participants that work to prevent cybercrime in e-Retail organisations. On the commencement of the interview, the aims and objectives of the research were explained to ensure that the research participants were able to make well-informed decisions (Mack et al., 2005) . Participation in this study was voluntary with the opportunity for e-Retail managers and other key informants to leave at any time without affecting their daily activities. In addition, written consent was obtained for all forms of data collection

3.9.3 Research limitations and how they were handled

While this study is on cyber-security in e-Retail business organisation and to provide a better solution on what should be done in e-Retail organisations to prevent or minimise cyber attacks in e-retail organisations; there were limitations associated with the research method, specifically multiple case-based research that impacted on the ability to draw generalisations from the findings. Another limitation of a multiple case-based approach was that of the influence of the researcher's own objectivities on the outcomes. The use of multiple data sources and different analytical methods provided evidence to address subjectivity (Creswell, J.W., Hanson, W.E., Clark Plano, V.L. and Morales, 2007). Data coding, the findings and the conclusion for the research came from a single perspective, that of the researcher.

3.10 Conclusion

In conclusion, this chapter provided explanation of the research approaches followed, the methods used to collect data, the data analysis process performed and importantly the ethical issues taken into thought in the study. In this chapter, the methodologies used to investigate the research problem were discussed. While the focus of this chapter was on the research approach adopted for the study, the methods and techniques used for the data collection as well as the data analysis process, at the same time there is a close relationship between the conceptual framework in section 3.2 and research methods adopted for this research. At this point, the policy frame framework in figure 3.2 and table 3.6 assisted in understanding and conceptualising the research problem. At the same time, the methodology chapter (chapter 3) helped in discovering the appropriate research methods and techniques needed to carry out the investigative process correctly. The research question and objective provided a basis and guideline for choosing the research methods. The next chapter (Chapter 4) describes the company, participants and the events that took place during the report work (data collection) process.

CHAPTER FOUR – FIELDWORK REPORT

4.1 Introduction

This chapter provides details as to how the collection of data (fieldwork) progressed. It demonstrates the necessary standards were adhered to strengthen the reliability dependability of the findings. In addition, the chapter gives a detailed account of the data collection procedure as well as the data analysis.

4.2 Duration of Data Collection

In-depth semi-structured interviews were conducted between the period of July 2017 and November 2017.

4.2.1 Description of companies researched

Eight (8) companies were purposively selected from different areas of expertise in relation to e-retail. A number of participants responded in the capacity of the office they hold in companies while others responded in their personal capacity. All but one are situated in the Cape Town Metropolis.

Table 4.1: Unit of analysis

Participant (P)	Areas of operation
1	ICT and services
2	ICT and governance
3	ICT and services
4	E-retailer
5	E-retailer
6	ICT and services
7	ICT and education
8	ICT, e-retailer

The character “P” and the corresponding number from (Table 4.1) above are used to distinguish these companies. In order to maintain the confidentiality of the participants the names of the companies were intentionally omitted. Pseudonyms are used instead through this thesis.

C1: This company is a development house that provides business solutions through innovative software design and implementation. It develops custom-built mobile and website applications for the private sector. They pride themselves on using the latest technology and security to develop premium applications across a number of software platforms.

C2: This company is a government institution that ensures access to services, facilities and open opportunities for all. They are in charge of providing internet access across a wide geographical area. They provide access to the government and NGOs on security risk management. They also provide internet and broadband access to communities.

C3: This Company offers a range of educational services; it is responsible for identifying skills requirements for government and the public sector. It aims to provide the necessary skills in the service sector for national economic growth.

C4: This company is a privately owned company: a very fast growing online fashion-shopping store. The company imports some of its raw materials and finished products overseas and also distributes its products nationally. The company collaborates with a number of third parties and sponsors to get their products to customers both nationally and internationally. It also maintains a growing following and network across South Africa. It prides itself on delivering customer satisfaction through fast and secure payments, speedy deliveries etc.

C5: This is an academic company providing academic material and resources nationally and on the continent. They offer products and services that support institutions and professionals across a plethora of disciplines. One of if not the oldest and largest supply store chain in Southern Africa, providing academic resource across Africa via retail and digital channels.

C6: This company is one of Africa’s best research and development organisations providing technological research and digital innovation. A leading multi-disciplinary research organisation for over 30 decades, researching in health, engineering, finance, defense, security, pharmaceutical, etc.

C7: This company helps enrich e-commerce in Africa. With a focus on trust, education, research and regulation around e-commerce. Their purpose is to foster sustainable growth of e-commerce business in Africa. With close dealings with the South African Chamber of commerce and the trade industry.

C8: This company is a well-established international brand: this company is heavily backed by international expertise and support though it operates in South Africa. Has been in existence in South Africa for over a decade however it has been operating internationally before its launch in

South Africa. It provides customers with a platform to purchase goods and products such as cars, jobs, items and property.

4.2.2 Participant sampling

All data in this research came from the aforementioned participants. As earlier stated, the participants were selected purposively as they were suitable to provide an understanding of the e-retail environment in South Africa, the cybersecurity challenges faced and possible solutions to mitigate cybersecurity challenges.

I. Description of participants

Table 4.2: Number of Respondents

Units of observation	Number of Participants	
E-retail organisations in the western cape	Selected (intended)	Responded (eventual)
Total Number of Participants	10	9

From the eight (8) companies that were selected, semi-structured interviews were conducted with nine (9) participants. Two participants of Company number 3 were jointly interviewed, as there were two (2) participants. The participants are described below:

Participant 1: This participant was an able young software engineer specialising in web applications. The interview took place in a coffee shop, in particular, Mug n Bean located in Canal Walk. The participant did not talk much and provided very little insight to the interview. The participant was not comfortable with the questions asked; perhaps he was not familiar with the nature and depth of questions.

Participant 2: This participant is an acting director in his organisation. Well advanced in age, very welcoming and found the study interested at such as time. The interview was held in boardroom 2 on a busy hour of the day. The participant showed vast knowledge of experience in the area of research citing a number of examples and instances. The participant has a number of certifications and courses in security.

Participant 3 & 4: The participants were very interested in the research but took a very general approach to it. The participants usually digressed and went off topic. The interview was very informative. The older of the participants mention he no tertiary education but had certification, courses and experience in abundance. While the younger gentleman though less talkative was immensely contributive to the interview. The interview took place in the canteen of the organisation around some water and coffee. This was the longest interview of the lot due to the digression, insights and strong interaction between the researcher and participants.

Participant 5: This bright young woman (probably in her late 30s) was very willing and receptive during the interview. She occupied the position of Chief Executive Officer. She found the interview interested and requested a copy of my findings and recommendations after my study. However, she was limited in technical aspects of the subject matter.

Participant 6: This is the Chief Information Officer of the organisation, a well-aged soft-spoken man. There was an initial visible reluctance to share information but as the interview progressed, he became much willing. Ended up being one of the most informative interviews in terms of day-to-day technical aspects of cybersecurity.

Participant 7: A researcher and a well-established scholar, also holding the position of Principal Researcher. Very knowledgeable with years of experience in practice and research. Should be in her late 50s. She spoke with courage and was apt and well aware of the challenges and what is required.

Participant 8: A Chief Executive Officer (probably late 60s). With alot experience. Has been a contract specialist for reputable firms providing expert advice. The researcher asked many probing questions to obtain the needed information. He answered the questions in a dual manner: what is being done and what ideally should be done.

Participant 9: She held the position of Chief Technology Officer; she knew the tenets of the interview at her fingertips. However, she had varying responses to the questions asked. She was quite careful not to give away company protocols or processes. The researcher highlighted that proprietary secret are not required but are welcomed.

II. The interview protocol and process

- All ethical obligations were sought by a written application to the faculty ethics committee and a written consent granted to the researcher to approach e-retail organisations for data collection.
- The researcher sent out research participation requests to e-retail organisations. The interview dates were set and confirmed via email.
- On initial contact with e-retailer, the researcher explained what the researcher objectives and intentions.

- Consequently, an individual informed consent letter was presented to participants requesting participant's permission just before the commencement of the interview. The participants were given the option to participate in their official or personal capacity.
- Permission for an audio recording of the interview was requested
- The interview proceeded when permission was granted.

There were pre-set interview questions that were asked, based on the responses of the participants follow up questions were asked that were found beneficial to the relevance of the study. This was important as there were useful insights based on skills and experience. The intended duration of each interview was 45 minutes. However, some interviews like Participant 3, 4 and 9 lasted for over 60 minutes due to the in-depth conversations that were held. At the consummation of the interview, participants were warmly thanked for participation in the study. The audio conversations were recorded on a mobile device and were swiftly uploaded to Google Drive for safekeeping.

III. Transcription of interview

Succeeding each interview, the researcher transcribed verbatim the voice-recorded interviews to text using an open source web app called otranscribe, to enable the application of content analysis technique on the transcribed data. The length of the transcribed document depended on the length of the interview. Full transcripts can be located in the appendix section.

4.2.3 4.2.3 Summary

Relevant literature, document and in-depth semi-structured interviews were main sources of data collected. Nine (9) participants from eight (8) companies that were selected. The interview was considered a success with all participants interested and responsive during the interview sessions. Companies are involved in some area of e-retail or another and have some valuable experience. Participants stressed that cybersecurity is an increasing issue and one that e-retail is not immune to. Further stating that research like this is a step in a good direction for e-retail in South Africa.

4.3 Conducting qualitative content analysis

The transcribed interview texts [Appendix E] could be of little or no use without performing some analysis on them. The sections the analysis that unfolded from a rigorous systematic qualitative content analysis technique (as fully described in chapter 3) was used to unearth meaningful information from the interview transcripts. The content analysis technique aided the researcher to recognize the variables and attributes of the pre-existing issues of investigation through several stages of descriptive coding and categorization process. The aforementioned descriptive presentation was aided by the use of a statistical software called ATLAS.ti. The analysis was proceeded by identifying and usage of a combination of coding methods. For the coding process, three methods of coding were conducted. Firstly, vivo coding according to Saldana (2008) codes is assigned to the participant own language. In other words, phrases were obtained from content of interview transcripts. Secondly, value coding was employed to label subjective views and ideas from data. This is normally opinion based, in this line the participant's gestures and facial expressions were also taken into consideration and coded. And finally, descriptive coding was carried out to categorize synthesis of views and opinions stated by all the participants (Saldana, 2008; Saldana, 2016).

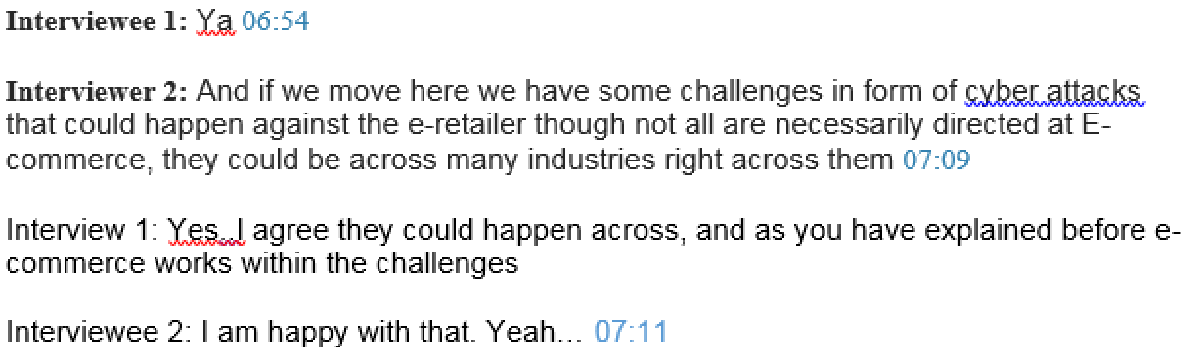
4.3.1 The analysis process

The interview data were partitioned into operational practices and ecosystem requirements. Operational practices are procedure and activities individual participants perform in the process of ensuring the security of their organisations. While ecosystem requirements are practices that should be in place for holistic cybersecurity in e-retail, this is form the foundation or parameters of the e-retail cybersecurity framework the aim research sought to investigate.

- As described in the preceding section the transcribed data underwent several coding stages to conclude at categories and themes in this study. In addition to the coding methods below are types used to conclude on the categories that were identified by the analyses:
- Transcribed data were thoroughly read several times for extensive absorption and recognition of the text
- At the analysis stage, the interview transcripts were seen as the major entity being analyzed.
- Thereafter, the interview data were split up into subdivisions prevention, mitigation, and remediation.
- **Deductive category assignment** or deductive category application was used. In this, the researcher used predefined categories based on literature or theory (Gondim & Bendassolli, 2014). This method of categorization stems from the prototype theory of the theories of categorizations where we have in mind typical exemplars of the category. Comparison of objects observed and those exemplars for similarities. If similarities exist then categorization is performed. The procedure is referred to as deductive for the reason categories are established before coding the text. The categories are derived from theory,

previous studies or research (Mayring, 2014). Developing categories or variables from theory or previous studies in qualitative research especially at data analysis (Berg, 2001).

- At the commencement of interviews, participants were briefed on the context and objectives of the research. Based on an extensive literature study done on some of the cybersecurity challenges faced by e-retailer organisations, a taxonomy of cybersecurity challenges [Figure 2] was presented to the participants to comment on. Participants agreement was one of the many bases for the commencement of the interview. Amongst numerous cybersecurity challenges faced by e-retail organisations the following cyber attacks were identified: (i) Internet/Online fraud (ii) Denial of service attacks (iii) Drive by download and (iv) Social engineering as broad hierarchies of cybersecurity cyber attacks.
- Figures 4.1 to 4.4 show excerpts of interviews transcripts were participants gave approval to the cybersecurity challenges. All excerpts are in verbatim as said. Full sample transcripts can be viewed in [appendix E].



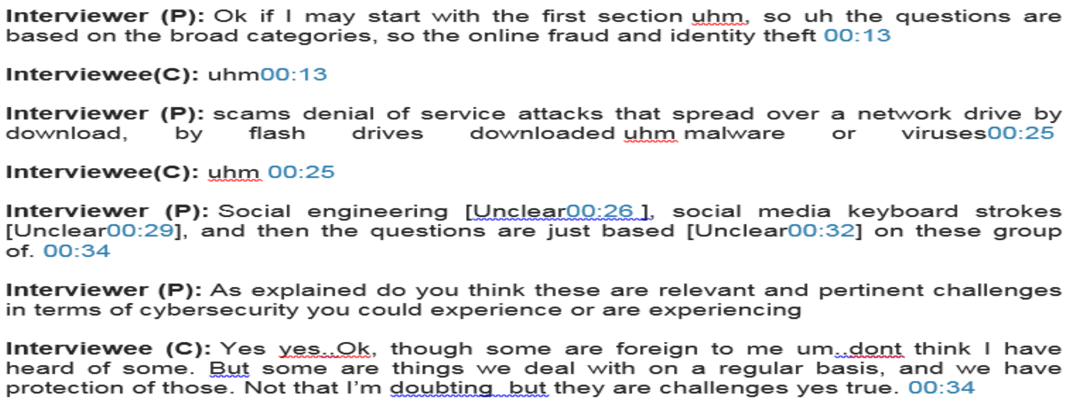
Interviewee 1: Ya 06:54

Interviewer 2: And if we move here we have some challenges in form of cyber attacks that could happen against the e-retailer though not all are necessarily directed at E-commerce, they could be across many industries right across them 07:09

Interview 1: Yes, I agree they could happen across, and as you have explained before e-commerce works within the challenges

Interviewee 2: I am happy with that. Yeah… 07:11

Figure 4.1: P1 Excerpt on cybersecurity challenges



Interviewer (P): Ok if I may start with the first section uhm, so uh the questions are based on the broad categories, so the online fraud and identity theft 00:13

Interviewee(C): uhm00:13

Interviewer (P): scams denial of service attacks that spread over a network drive by download, by flash drives downloaded uhm malware or viruses00:25

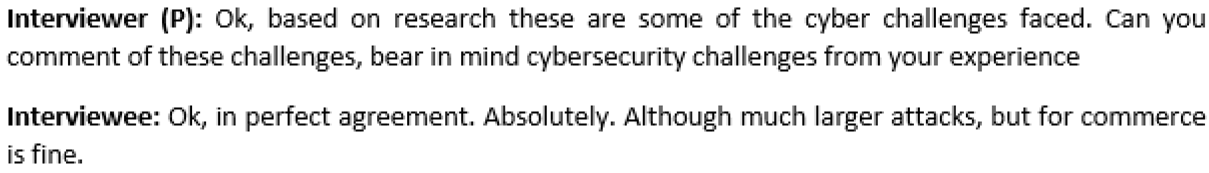
Interviewee(C): uhm 00:25

Interviewer (P): Social engineering [Unclear00:26], social media keyboard strokes [Unclear00:29], and then the questions are just based [Unclear00:32] on these group of. 00:34

Interviewer (P): As explained do you think these are relevant and pertinent challenges in terms of cybersecurity you could experience or are experiencing

Interviewee (C): Yes yes..Ok, though some are foreign to me um..dont think I have heard of some. But some are things we deal with on a regular basis, and we have protection of those. Not that I'm doubting but they are challenges yes true. 00:34

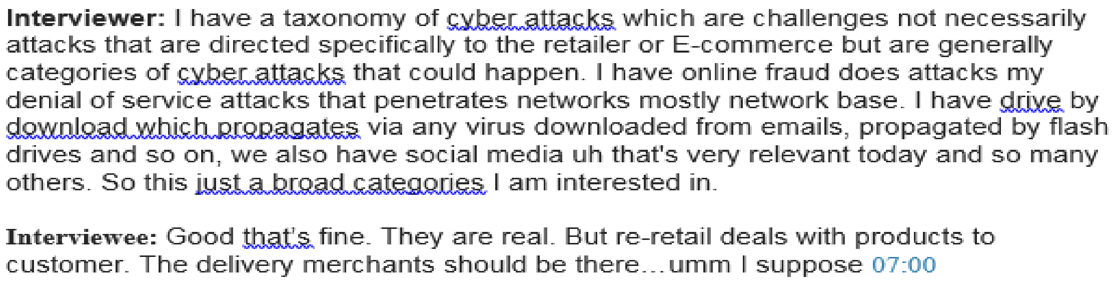
Figure 4.2: P2 Excerpt on cybersecurity challenges



Interviewer (P): Ok, based on research these are some of the cyber challenges faced. Can you comment of these challenges, bear in mind cybersecurity challenges from your experience

Interviewee: Ok, in perfect agreement. Absolutely. Although much larger attacks, but for commerce is fine.

Figure 4.3: P3 Excerpt on cybersecurity challenges

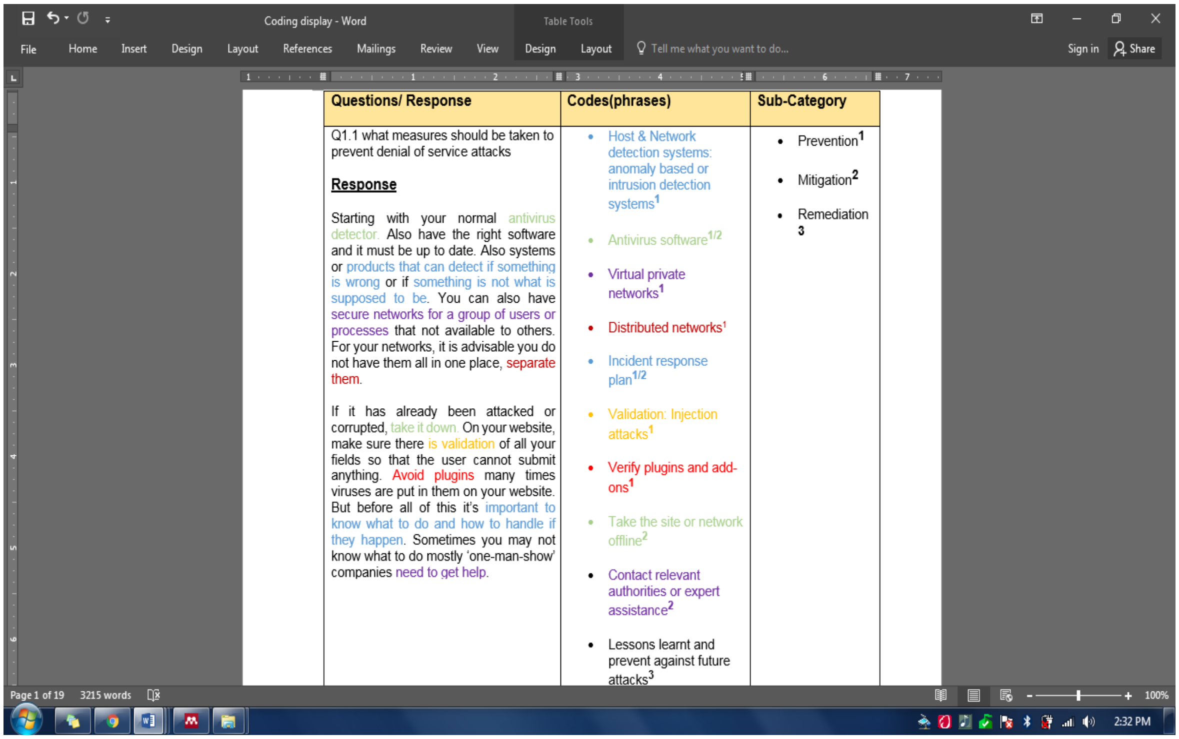


Interviewer: I have a taxonomy of cyber attacks which are challenges not necessarily attacks that are directed specifically to the retailer or E-commerce but are generally categories of cyber attacks that could happen. I have online fraud does attacks my denial of service attacks that penetrates networks mostly network base. I have drive by download which propagates via any virus downloaded from emails, propagated by flash drives and so on, we also have social media uh that's very relevant today and so many others. So this just a broad categories I am interested in.

Interviewee: Good that's fine. They are real. But re-retail deals with products to customer. The delivery merchants should be there…umm I suppose 07:00

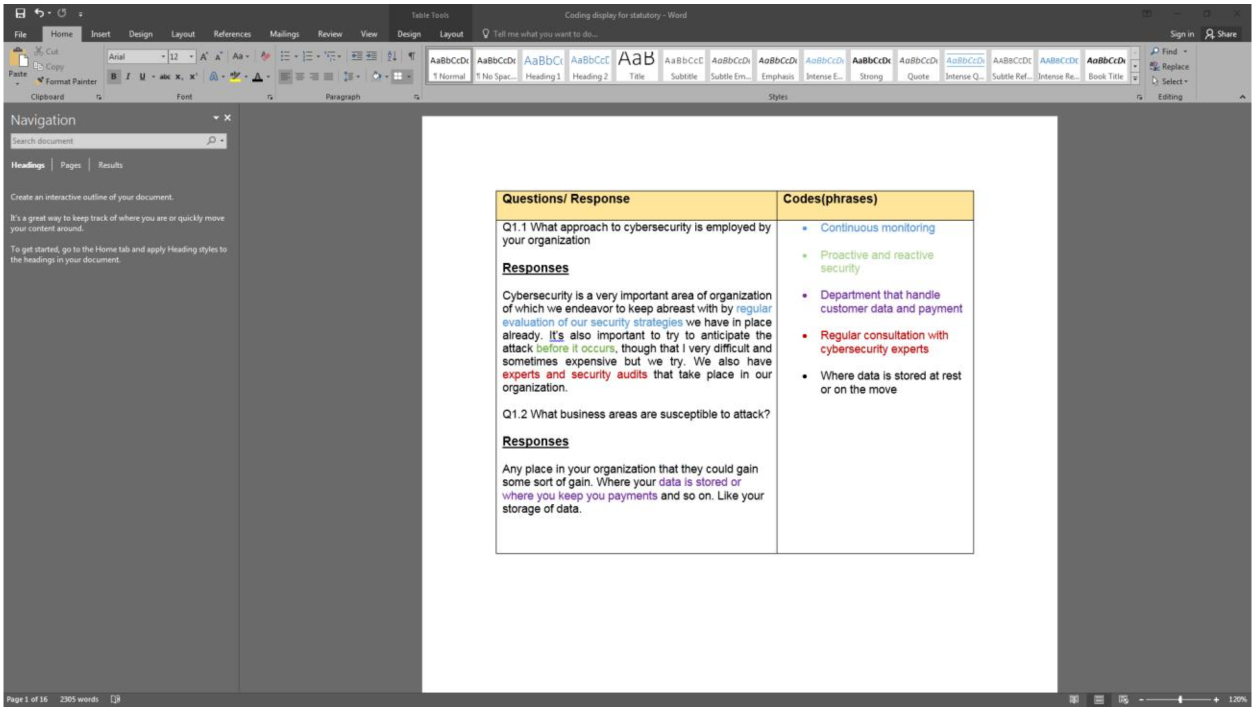
Figure 4.4: P4 Excerpt on cybersecurity challenges

- Figure 4.5 and Figure 4.6 shows colour coded interview texts with the identified codes, codes as descriptions were suggested by the text. With the relevant sub-category. The subcategories are prevention (stop from happening), mitigation (reduce its effect) and remediation (recover from).



Questions/ Response	Codes(phrases)	Sub-Category
Q1.1 what measures should be taken to prevent denial of service attacks **Response** Starting with your normal antivirus detector. Also have the right software and it must be up to date. Also systems or products that can detect if something is wrong or if something is not what is supposed to be. You can also have secure networks for a group of users or processes that not available to others. For your networks, it is advisable you do not have them all in one place, separate them. If it has already been attacked or corrupted, take it down. On your website, make sure there is validation of all your fields so that the user cannot submit anything. Avoid plugins many times viruses are put in them on your website. But before all of this it's important to know what to do and how to handle if they happen. Sometimes you may not know what to do mostly 'one-man-show' companies need to get help.	- Host & Network detection systems: anomaly based or intrusion detection systems[1] - Antivirus software[1/2] - Virtual private networks[1] - Distributed networks[1] - Incident response plan[1/2] - Validation: Injection attacks[1] - Verify plugins and add-ons[1] - Take the site or network offline[2] - Contact relevant authorities or expert assistance[2] - Lessons learnt and prevent against future attacks[3]	- Prevention[1] - Mitigation[2] - Remediation[3]

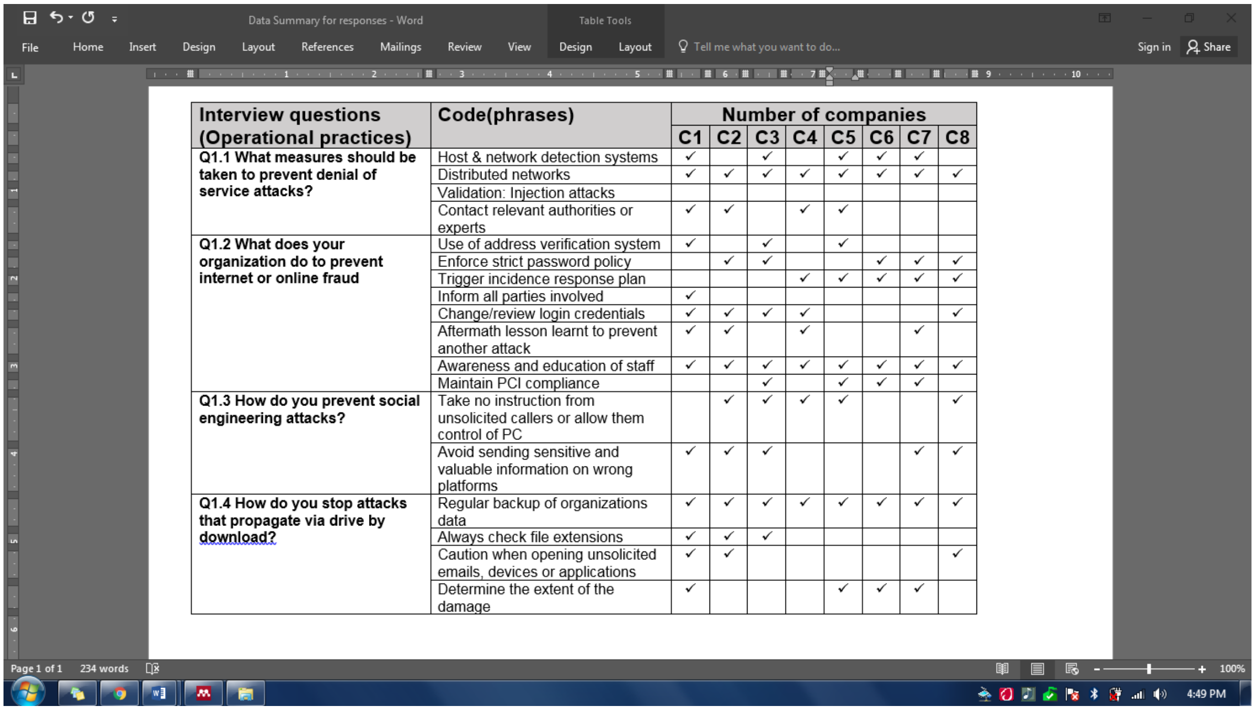
Figure 4.5: Data coding for operational practices


Coding display for statutory - Word
Table Tools
Navigation
Search document
Headings | Pages | Results
Create an interactive outline of your document.
It's a great way to keep track of where you are or quickly move your content around.
To get started, go to the Home tab and apply Heading styles to the headings in your document.
Page 1 of 16
2305 words

Questions/ Response	Codes(phrases)
Q1.1 What approach to cybersecurity is employed by your organization **Responses** Cybersecurity is a very important area of organization of which we endeavor to keep abreast with by regular evaluation of our security strategies we have in place already. It's also important to try to anticipate the attack before it occurs, though that I very difficult and sometimes expensive but we try. We also have experts and security audits that take place in our organization. Q1.2 What business areas are susceptible to attack? **Responses** Any place in your organization that they could gain some sort of gain. Where your data is stored or where you keep you payments and so on. Like your storage of data.	- Continuous monitoring - Proactive and reactive security - Department that handle customer data and payment - Regular consultation with cybersecurity experts - Where data is stored at rest or on the move

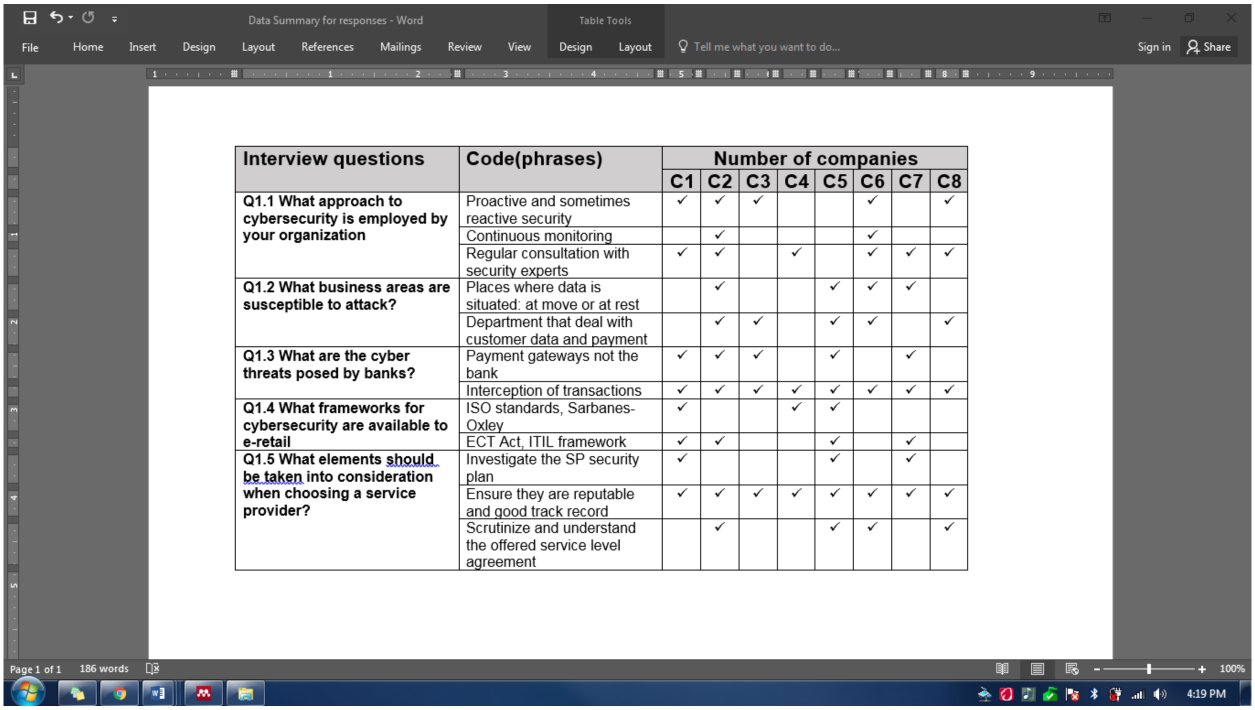
Figure 4.6: Data coding for ecosystem requirements

- Thereafter, codes and phrases from the texts were summarized by establishing similarities and dissimilarities from the responses of participants by the company as shown in Figure 4.6 and Figure 4.7.



Interview questions (Operational practices)	Code(phrases)	Number of companies							
		C1	C2	C3	C4	C5	C6	C7	C8
Q1.1 What measures should be taken to prevent denial of service attacks?	Host & network detection systems	✓		✓		✓	✓	✓	
	Distributed networks	✓	✓	✓	✓	✓	✓	✓	✓
	Validation: Injection attacks								
	Contact relevant authorities or experts	✓	✓		✓	✓			
Q1.2 What does your organization do to prevent internet or online fraud	Use of address verification system	✓		✓		✓			
	Enforce strict password policy		✓	✓			✓	✓	✓
	Trigger incidence response plan				✓	✓	✓	✓	✓
	Inform all parties involved	✓							
	Change/review login credentials	✓	✓	✓	✓				✓
	Aftermath lesson learnt to prevent another attack	✓	✓		✓			✓	
	Awareness and education of staff	✓	✓	✓	✓	✓	✓	✓	✓
	Maintain PCI compliance			✓		✓	✓	✓	
Q1.3 How do you prevent social engineering attacks?	Take no instruction from unsolicited callers or allow them control of PC		✓	✓	✓	✓			✓
	Avoid sending sensitive and valuable information on wrong platforms	✓	✓	✓				✓	✓
Q1.4 How do you stop attacks that propagate via drive by download?	Regular backup of organizations data	✓	✓	✓	✓	✓	✓	✓	✓
	Always check file extensions	✓	✓	✓					
	Caution when opening unsolicited emails, devices or applications	✓	✓						✓
	Determine the extent of the damage	✓				✓	✓	✓	

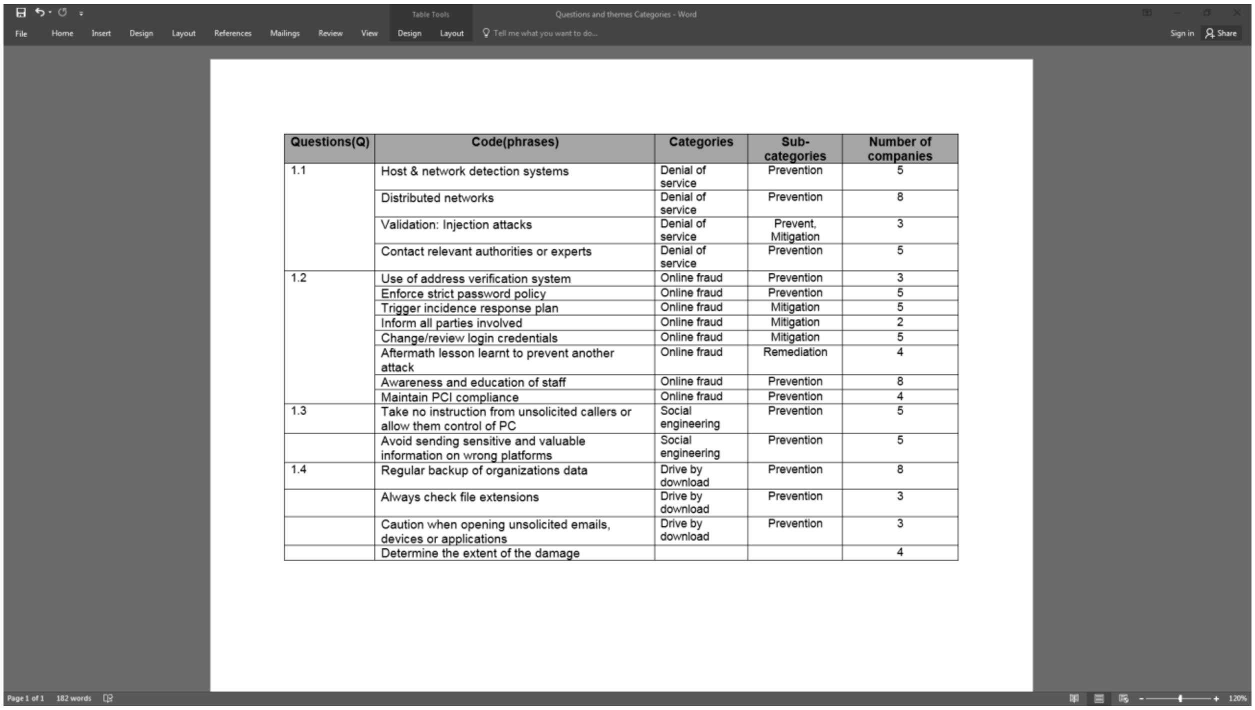
Figure 4.7: Data summary for operational practices



Interview questions	Code(phrases)	Number of companies							
		C1	C2	C3	C4	C5	C6	C7	C8
Q1.1 What approach to cybersecurity is employed by your organization	Proactive and sometimes reactive security	✓	✓	✓			✓		✓
	Continuous monitoring		✓				✓		
	Regular consultation with security experts	✓	✓		✓		✓	✓	✓
Q1.2 What business areas are susceptible to attack?	Places where data is situated: at move or at rest		✓			✓	✓	✓	
	Department that deal with customer data and payment		✓	✓		✓	✓		✓
Q1.3 What are the cyber threats posed by banks?	Payment gateways not the bank	✓	✓	✓		✓		✓	
	Interception of transactions	✓	✓	✓	✓	✓	✓	✓	✓
Q1.4 What frameworks for cybersecurity are available to e-retail	ISO standards, Sarbanes-Oxley	✓			✓	✓			
	ECT Act, ITIL framework	✓	✓			✓		✓	
Q1.5 What elements should be taken into consideration when choosing a service provider?	Investigate the SP security plan	✓				✓		✓	
	Ensure they are reputable and good track record	✓	✓	✓	✓	✓	✓	✓	✓
	Scrutinize and understand the offered service level agreement		✓			✓	✓		✓

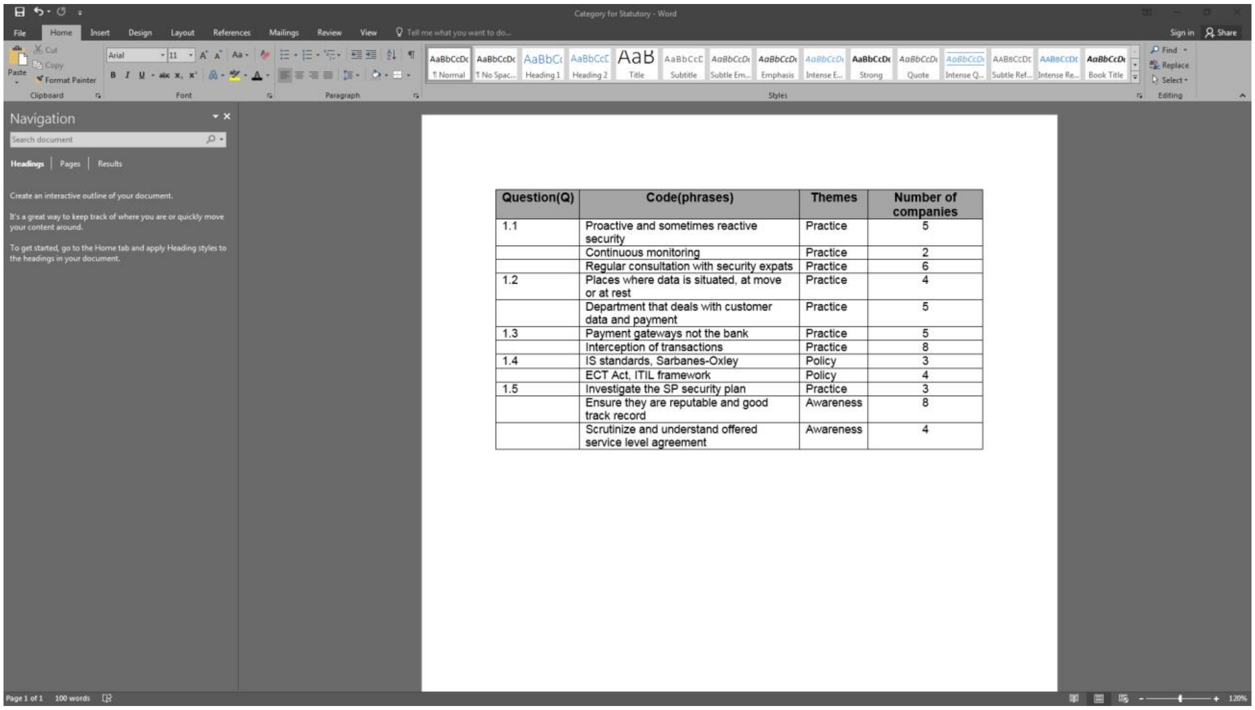
Figure 4.8: Data summary for ecosystem requirements

- The codes and phrases of the operational practices were then categorized and themed with similarities amongst the company responses as shown in Figure 4.8 and Figure 4.9



Questions(Q)	Code(phrases)	Categories	Sub-categories	Number of companies
1.1	Host & network detection systems	Denial of service	Prevention	5
	Distributed networks	Denial of service	Prevention	8
	Validation: Injection attacks	Denial of service	Prevent, Mitigation	3
	Contact relevant authorities or experts	Denial of service	Prevention	5
1.2	Use of address verification system	Online fraud	Prevention	3
	Enforce strict password policy	Online fraud	Prevention	5
	Trigger incidence response plan	Online fraud	Mitigation	5
	Inform all parties involved	Online fraud	Mitigation	2
	Change/review login credentials	Online fraud	Mitigation	5
	Aftermath lesson learnt to prevent another attack	Online fraud	Remediation	4
	Awareness and education of staff	Online fraud	Prevention	8
	Maintain PCI compliance	Online fraud	Prevention	4
1.3	Take no instruction from unsolicited callers or allow them control of PC	Social engineering	Prevention	5
	Avoid sending sensitive and valuable information on wrong platforms	Social engineering	Prevention	5
1.4	Regular backup of organizations data	Drive by download	Prevention	8
	Always check file extensions	Drive by download	Prevention	3
	Caution when opening unsolicited emails, devices or applications	Drive by download	Prevention	3
	Determine the extent of the damage			4

Figure 4.9: Categorization for Operational practices



Question(Q)	Code(phrases)	Themes	Number of companies
1.1	Proactive and sometimes reactive security	Practice	5
	Continuous monitoring	Practice	2
	Regular consultation with security expats	Practice	6
1.2	Places where data is situated, at move or at rest	Practice	4
	Department that deals with customer data and payment	Practice	5
1.3	Payment gateways not the bank	Practice	5
	Interception of transactions	Practice	8
1.4	IS standards, Sarbanes-Oxley	Policy	3
	ECT Act, ITIL framework	Policy	4
1.5	Investigate the SP security plan	Practice	3
	Ensure they are reputable and good track record	Awareness	8
	Scrutinize and understand offered service level agreement	Awareness	4

Figure 4.10: Categorization for ecosystem requirements

The figure above shows the full arrangement of the codes and phrases into categories and themes. Due to the length, it cannot be presented in the main body of the thesis. However, a full arrangement is contained in the accompanying CD of this thesis.

4.3.2 Categories and themes after analysis

A total of (3) categories and (3) sub-categories emerged after a succession and aggregation of the codes from interview data. The categories were derived from literature and were verified by the participants. The themes emerged from the questions, interview data and the analysis thereof. The themes were

Table 4.3: shows a summary of the categories and sub-categories that emerged for operational practices

Challenge(cyber attacks)	Category	Sub-category
Operational practices	Online fraud	Prevention, Mitigation and remediation
	Denial of service attacks	Prevention, Mitigation and remediation
	Drive-by download	Prevention, Mitigation and remediation
	Social engineering	Prevention, Mitigation and remediation

Table 4.4: represents categories and themes of ecosystem requirements

Requirement	**Category**	**Themes**
Ecosystem	Continuous monitoring. Proactive and reactive security Consultation with expats	Security continuous monitoring
	Network & security knowledge Certification and experience	Awareness and training
	Secure personal identifiable information Adherence to best practices	Information protection processes and procedures
	Audit e-retail practices Cybersecurity framework	Compliance

	Industry best practice standard	
	Investigate security plan	Risk assessment
	Integration level of service providers	Risk management strategy

In total, the study produced seven themes of which six fits into the Framework for Improving critical infrastructure cybersecurity (NIST, 2014:19). The six NIST framework categories are (i) Security continuous monitoring; (ii) Awareness and training; (iii) Information protection processes and procedures; (iv) Governance; (v) Risk management strategy; (vi) Risk assessment.

4.4 Summary of Chapter Four

The fieldwork was a tedious process, however, a good learning on how to approach and interact with professionals and experts. Data was gathered from relevant documents, literature and nine participants from eight organisations all but one spread around Cape Town. The entire research process enabled the researcher to learn and show competencies in fieldwork. This chapter presented details on seeking consent from participants, collecting data, transcribing, presentation and analyzing the data with various coding methods and narrowing to a conclusion of categories and themes

The proceeding chapter (chapter Five) presents a thematic presentation of the research findings.

CHAPTER FIVE: THE RESEARCH FINDINGS

5.1 Introduction

As reiterated in preceding chapters the aim of this study is to explore the current cybersecurity environment of e-retail in South Africa. With an important focus on identifying the elements that should be included in an e-retail organisations cybersecurity framework. The steps followed include:

i. Understanding the cybersecurity challenges e-retail organisations face.
ii. Identifying the cyber attack profile of e-retail organisations.
iii. Determining defence profiles to adopt against a specific cyber attack.

The preceding chapter provided an exposition on how fieldwork was carried out, describing the researched companies and the nine participants. It demonstrated methods and procedures on how data analysis took place. This chapter presents the detailed findings from the analysis of the multiple case study regarding e-retail cybersecurity in the South African context.

The findings report on cybersecurity profile of eight organisations in South Africa, amalgamating the NIST Cybersecurity framework categories and the operational practices performed by the e-retail organisation.

5.2 Descriptive presentation of data

This section draws on interview transcripts to outline the findings. The findings are divided into a descriptive outline of challenges, strategies currently adopted and the requirements for a holistic security strategy.

5.2.1 ONLINE FRAUD

The researcher aimed to gain a general understanding of the challenges and specifically, how each has manifested within their organisation. As explained in chapter four where challenges were classified into taxonomic units:

I. Prevention

a. Information protection processes and procedures

These are best practices adopted by e-retail organisations in certain areas of operation, these include security practices maintained and used to manage the protection of IT systems, processes and assets. This theme appears in both the operational practices and the ecosystem requirements (Tables 4.2 & 4.3). Participants stressed the importance of **validating payments processes**. Participant 1 stated, “You need to have a system that checks the address of the person wanting to pay with the credit card”. Participant 5 said: “The CVV number on the card is there to reduce credit card fraud". Participant 8 confirmed by saying: "the verification is handled by the payment gateway".

Organisations understand the need for **update and patch management**; it was stated by all 9 participants. Participant 7 stated "And in terms of the general measure that you should take is to make sure you download the latest version of patches, you know, of Windows update. I know from this previous ransomware that came in maybe 'wanna cry' and those ones attack could have been prevented if people had the latest versions of Windows installed and the patches that are sent by Windows or Microsoft." Participant 6 supported and called for the need for regular updates and installing patches to software stating some of the attacks are avoidable through a regular software update. Further stating "most of the explodes of ransomware that you've seen the last couple of months has been exploding on systems that's been not updated regularly so". All 9 participants said that regular updating is one basic and important measure you must take.

Regular backup of systems and files is a very important preventative strategy in the event of an attack or catastrophe. All 9 participants (100%) stressed backup management as basic and important measure closely linked to update and patch management. Participant 8 mentions performing two types of backup "make sure that you have the online and offline backups". Online backup provides uninterrupted backup that is always active. In addition, it eliminates offline or downtime.

b. Risk management strategy

The risk management strategy describes the organisations risk priorities and processes to support the operationalizing of risks decision when they occur. "Risk management strategy involves the blueprint or plan of action to mitigate risks in the organisation," mentioned by participant 8. Participant 8 went on further to say that "an **incidence response plan** is the first step in dealing with these attacks, without it how do you try to solve any type of risk you might be currently facing". Participant 7 also mentioned it is an important plan to have: "you can see the impact level or how severe the risk might be". Many organisations do not have a cyber-incidence response plan, because many do not take the threat of attacks seriously. From the comment, participant 8 is bringing out a perception issue. Some organisations have the perception that cyber attacks and its prevention are not key businesses matters they should be dealing with. An incident response plan comprises of pre and post actions to mitigate risks. Participant 8 was passionate about having an incident response plan in place, going on further to say all organisations need one, even at a national it should be a consideration. This comment is worthy of note, in the event of a national cyber-attack, what procedures and actions will be followed to address the impact of the cyber-attack on society?

Another risk management strategy that organisations are encouraged to adopt is that of **cyber resilience**. Participant 7 and 8 made it clear that this is a much more advanced safeguard strategy to reach. Ideally, resiliency is implemented on highly critical infrastructure and a very essential asset to maintaining critical infrastructure. Participant 8 says there are pillars that make up a resilience program. More details on the resilience program can be found in the interview transcripts in appendix E. Both the incident response plan and the cyber resilience program constitutes a set of itemized tasks to be performed as will be discussed in Chapter 6.

c. Awareness and training

This theme describes the knowledge and perception that staff within e-retail organisations should have to be able to recognize internet or online fraudulent activities. All 9 participants (100%) stated that awareness and training cannot be left out. Participant 5, 6, 8 and 9 noted: “You must know the characteristics of how online fraud manifests for you to be able to recognize and know what to do to prevent it”. Awareness programs are very useful and important says participant 4. Even as little as sticking posters in designated walls and passageways:

> “I think awareness in, in government lately got some attention, so there has been from campaigns, programs and I don't know if you might have seen it. There were some posters that they put up in the building and all of that, and actually very helpful to keep you constantly in awareness and remind you of security do and some don’ts”

Participants 1, 2 and 3 said not only training and awareness of cyber attacks but it must be continuous training and awareness. Owing to the fact that cyber-attack methods continue to change and present themselves in various forms. Course-based employee training where employees are taught how to identify and appropriately handle cyber attacks is an important aspect to the prevention of online fraud and cyber attacks.

d. Compliance

This theme addresses some security standards e-retail organisation should maintain as a measure amongst others to prevent online fraud. This section was fully addressed in the legislation section of the findings. However, participant 6 mentions

> “In order to prevent credit card fraud in your organisation you must make sure you comply with the Payment Card Industry Data Security Standards because as an e-retailer you probably handle credit card information, you need to make sure your organisation is

> secure to do that. If not you could have people stealing money from your customer cards which is a crime and you can be prosecuted for that."

Three of the nine participants think compliance with security standards is important today, as these standards help retailers to protect their business and customers from internet fraud. "We also comply with best practices in our industry, and we have auditors yearly that provide us with security advice" participant 2 says. A common suggested point by a number of participants was that there should be compliance to international benchmark standards.

e. Access control

This theme addresses limiting access to IT systems to authorized users in e-retail organisations. Only authorized users should be able to access processes, tasks and infrastructure. Participants 1, 7, 8 and 9 have strictly enforced a password policy for all account users with an expiration date, thereafter employees have to change their passwords. Participants 1 and 9 make use of single sign-on while participants 7 and 8 have hesitation to single sign-on and is in support of having different sign-on credentials for multiple devices. Participant 1 and 9 say there are a number of benefits of using single sign-on, and that there a reason for adopting it. "You don't have to keep signing in to multiple systems, it saves time and we have so many transactions happening". Participant 8 indicates that a stringent password policy is not all it requires, but also policing of the policy to make sure it is institutionalised in their organisation. In addition, further going on to explain access control also should address physical access control: restricted places for restricted people. Physical access control devices are an important aspect to access control. "Not data store or places you keep your physical data should not be accessible to anyone. It should not be in a common place, I think it must be secluded both with physical barriers and other access control devices".

f. Security continuous monitoring

This theme involves regular examination of assets, information system and processes of cybersecurity events. Monitoring of personnel, devices, software, processes and events. To ascertain the effectiveness of already established protective measures. All 9 participants highlighted this as an indispensable means to maintain a cyber-secure organisation. Participant 8 stated: "When we have placed measures, we always go back to re-evaluate them. Only then can you know your security readiness". Participant 7 stated: "In particular to online fraud, you also need to monitor the normal things like your statements: I mean bank payments, you need to know what is going on there". A constant review of devices and assets within the organisation is required on a scheduled basis. From the network, physical environment, personnel activity, to an external service provider should be a review for abnormalities. Participant 3 states: vulnerability scans can be performed to show areas of weakness in your system. Depending on the complexity, organisations can seek the help of expats to scan the entire organisations for areas of possible weaknesses. Participant 7 stated: personnel activity is a key vulnerability area that should be monitored, either to personnel carelessness or a deliberate attack perpetuated using personnel credentials. The participant was reluctant to disclose the tool or external organisations that perform vulnerabilities scans. However Company 6, participant 7 did mention Deloitte as the company's auditors, further stating Deloitte performs an IT risk assessment on an annual basis.

Summary of findings for prevention of online fraud

- The prevention category, which represents the security practices adopted by e-retail organisations to prevent the occurrence of online fraud. In summary, these are some preventative activities:
- An incidence response plan and resilience programs are the first steps to the prevention of online fraud.
- Personnel awareness training is indispensable to enable personnel to handle its various forms.
- Maintaining compliance best practice standards.
- Continuous monitoring of assets and processes.
- Regular update and patch management system.
- Use of dedicated platforms for secure communication.
- Enforcing and policing of password, sign-on and accounts policy.

II. Mitigation and remediation

In the event, an e-retail organisation has become a victim of online fraud. Participants provided insights as to what steps to take to reduce its severity and to recover from such an attack. Participants 7 and 8 said: "At this time you execute your incident response plan or resilience strategy if you have one". Participants 1 and 2 though did not mention the above but said it is important to determine the type of attack. Determining the type of attack is one of the many steps contained in an incident response plan. Participant 2 stated: "you need to know, is it a phishing attack, is it clean fraud". Determination of the type of attack will help in the diagnosis of the type of measures to take towards mitigation says Participant 1. All 9 participants (100%) hinted that **communication** is important when dealing with the mitigation of attacks. Participant 2 and 3 said "we inform all parties involved of any breach. If we are unable to find a solution we do have places where we can seek external help." Both internal and external parties should be made aware of any breach that is experienced. This entails a critical review of all compromised assets conducted, review of user credentials, accounts, and user rights should be performed. Participants 6, 7 and 8 mentions that in some cases you have to blacklist accounts or certain assets that are severely compromised. Participant 8 says lessons learnt is always over-looked in the mitigation process and should not be so. It is important to review the circumstance around which an attack occurred, to prevent future occurrence. Participant 8 stated: “When I took the CompTIA Security+ course and certification, lessons learnt is an unmistakable aspect to mitigation of cyber attacks. It will help you not to repeat the same mistakes”. Participant 8 said there are a number of security products of varying price which organisations can purchase. As soon as a DOS attack happens, the website or network should be taken offline, “there will be some downtime. It can be brought back up when the damage is rectified”. All relevant parties including the service providers alerted and made aware of the nature of the attack. After a remedy or solution has been reached, it is important to evaluate and review the lessons learnt.

5.2.2 DENIAL OF SERVICE ATTACKS

This a cyber-attack to prevent legitimate users from accessing of computer networks or systems. Denial of service attacks occurs at various levels such as host, network or distributed attack. This section reports on the experience adopted by e-retail organisations to prevent, mitigate and remediate against denial of service attacks.

I. Prevention

a. Information protection processes and procedures

This section reports on measures currently employed by interviewed organisations. These are security practices maintained and used to manage the protection of IT systems, processes and assets. Practices e-retailers are encouraged to adopt to avert falling a victim of a denial of service attack.

Participant 8 stated that to provide network defence, the organisation makes use of a software package called Stormshield. **Stormshield** Security Solutions application that provides network protection for small to large businesses. With four areas of protection which includes: Network security, data security, endpoint security and virtualized infrastructure protection. Further stating: “It is a recommendable service to get.” Participant 8 also encourages organisations to make use of network monitoring products that involves **artificial intelligence**, which provides predictive analysis based on data flow. On the line of thought on predictive analysis, participants 5 and 6 who were jointly interviewed said: “I think that is the future of security before it happens how can we know, so that we prevent it from happening”. Participant 6 added by stating: “most of what we do is reactive security, we are always reacting in most cases, the future is proactive or offensive". Participant 7 says: "For small businesses, though it may be difficult, is to have **distributed networks**", having separate networks, so that if one is attacked the other can function properly.

Firewall management and configuration: participants 1, 3, 5, 6, 7 and 8, in summary, said firewall configuration is vital in understanding how to protect your network. Participants 6 and 7 deliberated on the use of filters in particular, **Ingress and egress**. Participant 6 stated: "you need a filter to identify and block potentially harmful traffic, as a standard there should be default deny without appropriate labelling identify all your inbound and outbound traffic". Participant 7 stated "many admins are mostly concerned about inbound connections, what about outbound (Egress), data may be leaving your network without you knowing that is leaving. Probably in that case be stolen." However, participants 1 and 3 mentioned that organisations should not be dependent on the firewall "Do not rely on the firewall, it is not enough." In summary, filtering best practice should be given a serious thought i.e. Ingress and Egress filtering. Participant 5 and 6 mentioned the use of **Access Control Lists**, "we use that to specify what users or processes should have or be given access". Similar to the firewall, Participant 8 and 9 mention the use of a **proxy server**. "I will advise as we do to use a proxy server for maybe exceptional cases, it will act as an intermediary of some sort to request stuff. You get different types depending on what you want".

Load balancing is a key component mentioned by participants 5, 6 and 7. "A proper load balancing will help improve performance"; "you've probably seen some sites that crash when too many people access it. Yes, it because of poor load balancing". Load balancing is key for any application or service that involves multiple active services. Participant 7 stated your network and web infrastructure should be able to handle large amounts of traffic. This can be achieved through the use of intrusion detection systems to monitor network and host traffic. Participants 4, 5 and 6 acknowledge they use various **intrusion detection systems** for particular purposes. Participant 4 stated: "yes in government, we use a network IDS, the specific I am not at liberty to tell you, but we use it to monitor and analyses also. We also have some host-based ones also". Participant 6 stated: "We make uses of IDS and the most recent one we purchased was for checking anomalies". The participant in this case referred to an anomaly-based intrusion detection system. Participant 2, a software developer says: "For websites, I use security plugins and its good you use them especially for websites". **Security plugins** for open source content management systems like WordPress, Joomla etc. Going on further to say **SSL certificate**, "you know on some sites also you see the padlock thing, Yes! You should have one of those". This certificate shows that the site is considered secure for a credit card, data transfer and login transactions. Participant

8 who had earlier mentioned the need for an incidence response plan and a resilience program in the prevention of online fraud says: “You need to know the readiness of your organisation”. Ascertain the **cybersecurity readiness** of your organisation. This can be achieved by conducting **simulation and penetration tests**; she says,

> “We run virtual penetration tests to uncover attacks or what we call vulnerability points. Remember as I earlier told you, what did I say? Your incidence response plan. You simulate an attack to see how you respond and you learn from that. A cyber-attack simulation should be a common practice. It is good you carry it out on a scheduled basis, on then can you know your readiness. You cannot know your readiness or whether you can withstand an attack by doing nothing. Simulate what attack, what was lost, or how do we handle and recover. That is security.”

Participant 5 and 6 also mentioned penetration tests are good indicators of areas of weakness. All 9 participants mentioned service monitoring; if an unrecognized service is running, it is advisable to turn off. Participant 4 stated: “…you should know what is running in your pc or network, if you see a service that you are not sure of turn it off”. Participant 5 stated, “Many services run in the background, and depending on what ports are allowed and open something serious can be running”. Participant 6 added on by saying: “…rootkits and scripts may not be visible, but run in the background. It could be doing damage”. Participants 5 stated application level security products are the best level to address security. Application layer security refers to the application layer of the OSI model. All 9 participants stated applying **security patches** to software and having a good **antivirus software** are all important as basics to protect against denial of service attacks.

Summary of findings for prevention of Denial of service attacks

- Good firewall configuration management
- Simulation and penetration tests to ascertain cyber-attack readiness of the organisation
- Use of network monitoring products
- Distributed networks
- Adopting appropriate filtering techniques
- Use of intrusion detection systems
- Load balancing to keep up with transactions and processes
- Use of access control lists
- Use of security plugins on open source content management systems
- Use application-level security products

II. Mitigation and remediation

This sub-section covers participant's insights in the event an e-retail organisation has become a victim of a denial of service attacks. Participants provided insights as to what steps to take to reduce its severity and to recover from such an attack. Participant 5, 6, 7 and 8 had specific experience and knowledge in denial of service attacks. Participant 8 referred back to the importance of having an incident response plan. The first step is to determine the type of attack, what is lost and how much is lost. Additional information such as time of the attack and the extent of the damage caused. E-retail organisations should solicit for help in cases of uncertainty on how to stop denial of service attacks.

5.2.3 DRIVE BY DOWNLOAD

This is another cybersecurity challenge faced by e-retail organisations. It is one of the common ways through which malware propagates. Drive-by download refers to the unintentional download or transfer of malware to devices. Participants gave their insights on their experiences with Drive-by download attacks. This section describes the findings suggested by participants on how to manage drive-by download attacks.

I. Prevention

This sub-section describes the prevention practices or deterrents generally employed by e-retail organisations. These include technical and on-technical measures. Therefore, measures fall under the Information protection processes and procedures category of the NIST framework.

II. Information protection processes and procedures

A common suggestion from all participants was that: care and caution should be exercised when opening **unsolicited emails**. Participant 1 and 4 said email embedded malware can be executed by an event. Unrecognized email attachments should be verified before download. Participant 8 an email verification system to validate email called the **Sender Policy Framework**. "This framework can be of benefit to the organisation". Participant 1, 2 and 3 said file extensions should be checked before they are downloaded and installed, batch scripts containing malware could accompany attachments. **File extensions should be shown** and not hidden. All participants said regular installation of updates and patches in order for identifying latest known signature viruses. A response that is applicable to all types of attacks is the incident response plan, the **incidence response plan** will detail procedural steps. A common view reflected by all participants is to have a **security awareness program** or culture in the organisation, where information and security tips are constantly shared. Participants 5 and 6 stated increased browser security with trusted add-ons will help to heighten the security of the browser. Participant 5 stated, "…macros can be disabled, you can also block pop-ups from running". Participant 6 also stated: "…I advise blocking sites that want to accept cookies, though there is a move away from cookies, still legacy attacks do happen". **Blocking of P2P sharing and unknown IP addresses**, "…P2P sharing uses lots of bandwidth, it should be disabled and block on the network" said participant 6. Participant 5 added by stating: "that is what your whitelist and blacklist is for". Having an up to date antivirus software can go a long way in preventing viruses in hardware devices said participant 8. Participant 8 said **honeypots** can be used "though this may be advanced to implement. There are 2 ways you can use honeypots. This may not be suitable for just an e-retailer". In addition, an **intrusion detection system** can also detect malware in the network. A scheduled backup should be in place as said by all 9 participants.

III. Summary of findings for prevention of Drive by Download attacks

- Caution for unsolicited emails.
- Shown and check hidden file extensions.
- Maintain a security awareness program or culture.
- Sender policy framework.
- Use of IDs systems and honeypots.
- Increased browser security.
- An incidence response plan.
- Use of up to date antivirus software.
- Regular installation of updates and patches.

IV. Mitigation and remediation

In the event, an e-retail organisation has become a victim of drive-by download attacks. Participants provided insights as to what steps to take to reduce its severity and to recover from such attack. Participant 1 to 5 recommends an organisation-wide scan of all devices and peripherals to minimize the spread of the malware. Participant 8 said you execute your incidence response plan, further stating you determine the nature or type of the attack and perform the necessary operations. Infected systems, sub-systems or devices should be taken off the network to prevent further infestation.

5.2.4 SOCIAL ENGINEERING

This section describes techniques to avert social engineering attacks that are influenced by humans in order to divulge confidential information. Participants in this study highlight some preventative and mitigation measures. From the responses, participants were not familiar with social engineering attacks. The response rate in this category was very low.

I. Prevention

Participants 8 stated the best prevention strategy for social engineering is Education and awareness, "…Staff training normally attackers study and learn the victim, so victims should ensure they safeguard their information: I think that is sear-phishing". Participant 1 and 2 said the organisation should prohibit password sharing or writing down passwords or codes and placing them in plain sight. Participant 7 advises data in transit or at rest be encrypted to ensure the right people know or can read the information. Participant 8 suggested the organisation understand the personality traits of their staff. "…There is a social engineering personality framework where organisations can understand how personality traits influence susceptibility". Participant 5 and 6 mentioned password sharing should be prohibited and placing passwords in plain sight as on sticky notes should not be allowed. As stated in the introduction to this section, participants were not too familiar with the concept of social engineering attacks in e-retail. This was also evident from the amount and content of data obtained from the participants as compared to the previous cyber-attack types.

II. Summary of findings for prevention of Social engineering attacks

- Staff awareness and training should be conducted on a basis.
- Avoid password sharing or exposing sensitive credentials in plain sight
- Use of Social engineering personality framework to understand personnel

III. Mitigation and Remediation

This sub-section covers the participant's insights suggested by participants in order to reduce the impact of social engineering attacks. Participants 8 said: "in this stage, you execute what your incidence response plan says". Participant 7 mentioned the importance to access the damage, so ascertain the extent of the damage. This provides a good indication of the necessary steps to take. Documentation and evaluation are also important for future reference in order to prevent the subsequent occurrence.

5.3 ECOSYSTEM REQUIREMENTS

As earlier stated, the previous section was to understand the cybersecurity challenges faced by e-retail organisations and to know the specific practices in place to prevent and mitigate against such cyber challenges. In addition, participants were asked generic questions based on the e-retail ecosystem presented in this study [see appendix F]. These are requirements for a holistic security strategy at an organisational level and an extension to the nation. Citing the niches in the ecosystem such as are e-retailer, banking, legislation and service provider. Participants were asked to provide knowledge to each niche's role in terms of cybersecurity. The findings of each niche are presented below:

5.3.1 The e-retailer

Participant 7 said an e-retailer should be proactive about security, further to mention advancement in technology and its persuasiveness has brought the need for cybersecurity. However, participants 4 and 5 believe there is no such thing as only proactive security. They buttressed their argument by stating: “How can you protect against what you do not know”. Both participants are of the opinion that both reactive security and proactive is what is required and cost-effective for small enterprises. They do not completely disagree with the concept of proactive security. It certainly has its place but is quite difficult to implement. Participant 9 and 8 said cybersecurity should be a key deliberation point in any organisations strategic planning. Often cybersecurity is given the least priority or none at all, “...that should not be the case in this era of all things technology and crime”. Participant 1 said: “My company regularly consults with expats because we don’t really have a capacity to manage our security”. Participants 5, 6, 7 said continual monitoring is important, “you need to evaluate all your security installations to know if they are working or not”, “to remain safe you need to always check your controls”, “you should have key security areas which you routinely check like your firewall configuration, is it blocking and working like it was set up to do?”

Participant 7 said personnel should have the necessary skills to handle cybersecurity. Network security expertise coupled with experience and certifications to complement existing knowledge. Participant 2 said personnel should be able to see extraordinary things, innovative and attention to detail. In addition to the skills set, participant 5 said they should be problem and challenge solvers and be abreast with the latest emergent technology. All 9 participants stressed that the threat of cybercrime is real and should be given much deliberation and the attention. Participant 7,8 and 9 highlighted some areas in businesses that are vulnerable to attacks if not properly secured: “places where data is stored either at rest or on the move”, “Data capturers”, “customer service departments”, “procurement”, “Customer data and payment systems”. Participant 7 said, “cybersecurity is good but if it is not administered properly it could be ineffective”. Accountability is important; someone or a group of people must take responsibility for security in the organisation. Participants 7, 8 and 9, development of national legislation be with consultation from expat cybersecurity personnel and groups.

From the findings above, some themes emerge from the categories in the NIST framework. These themes include Security continuous monitoring, awareness and training, and governance.

5.3.2 Banking

Participant 5, 6, 7 mentioned the payment gateway the e-retailer uses is the most important aspect not the bank, “the payment gateway handles the transaction and validates it; the bank just collects your money”. Participant 8 said there should be some security safeguards that the payment gateway should have, to avoid interception of transactions or an attack on payment systems.

From the findings above, some themes emerge from the categories in the NIST framework. The category that emerges is information protection processes and procedures.

5.3.3 Legislation

All 9 participants said legislation does play a role in cybersecurity. Participant 3 and 4 said but having legislation does not necessarily mean cybersecurity, though is a step in the right direction. Participant 1 and 2 said legislation helps to provide recommended best practices or standards. Participant 6,7 and 8 said there are framework or legislation that e-retail organisation could find beneficial such as ITIL framework, Cobit framework, ECT act, ISO standards, protection of critical infrastructure (NIST) and Sarbanes-Oxley. These standards will be discussed in the following chapter. Participant 1, 2, 5 and 7 mentioned there was no compliance with any framework or standard, neither was there policing or reporting to measure compliance to legislation. However, participant 7 said on an annual basis IT risk assessment is carried out by external auditors. Participant 9 a government official as explained in the previous chapter said the government is in the process of creating CERTs to handle cybersecurity security incidents.

From the findings above, the emergent theme from the NIST framework category is Compliance.

5.3.4 Supplier

On the security privileges that should be granted to the supplier. Participant 2, 3, 4 and 5 said it is dependent on the integration level of the supplier to the e-retailer. Participant 7 said secure file transfers can be used to secure both parties. Participant 4 mentions the use of web services. Participant 7 said the integration level should be settled in the SLA between the e-retailer and the supplier.

From the findings above, the following themes from the NIST framework categories emerge which are Information protection processes and procedures and risk management strategy.

5.3.5 Service Provider

Participant 3 said: “Cybersecurity requirements must be imposed on services providers if we want to block all areas of entry to attacks”. Participant 7 said an investigation should be made into the service providers security plan, further stating the SLA be explicit and clearly mark out responsibilities and duties. More details will be discussed in the following chapter.

From the findings above, the emergent theme from the NIST framework category is Risk assessment.

5.4 Summary of findings

- Proactive and reactive security is integral.
- Priority should be given to cybersecurity in organisational planning.
- Continuous monitoring.
- Personnel should be network and security apt.
- Cybercrime poses a real threat to organisations and the effects are crippling.
- Customer data and payment systems are vulnerable business areas to cyber attacks.
- Accountability: taking ownership.
- Develop legislation with expats.
- Payment gateway.
- Interception of payments.
- There are frameworks to guide e-retail organisations.
- Use of secure file transfer protocols.
- Service level agreement.

The following chapter discusses the research findings in relation to literature to define the contribution of this research to the body of knowledge.

CHAPTER SIX: DISCUSSION OF FINDINGS

6.1 Introduction

The previous chapter presented findings from participants in organisations from a multiple-case study on the cybersecurity of e-retail organisations, highlighting challenges and opportunities for creating a framework for e-retail organisations. Findings are presented based on themes that emerged from the data. Eight themes were identified: Information protection processes and procedures, risk management strategy, awareness and training, compliance, access control, security continuous monitoring, governance, and risk assessment. These themes form the basis of discourse for this chapter. Chapter Six examines, validates and authenticates the findings by comparing them to previous related research studies from literature. This process of validating and interpretation findings using literature provides clarification of findings on the subject area. It also helps to verify the findings to make sure they are valid and authentic.

The research problem identified for this study is focused on mitigating the occurrence of cyber attacks in e-retail SMEs. Despite the number of avenues for cyber securing organisations, SMEs are commonly not able to incorporate these practices and procedures. This chapter provides explanations based on the findings to address the main research and sub-questions as presented in Chapter 1.

The two main research questions are:

What are the specific cybersecurity challenges faced by e-retail organisations

How can SA e-retail organisations mitigate against the occurrence of cyber attacks?

The research sub-questions are:

1. What are the peculiarities of the e-retail industry in terms of cybersecurity?
2. What measures have e-retail organisations taken to comply with current cybersecurity laws?
3. How can South African e-retail organisations ensure cybersecurity practices?
4. What should characterize a cybersecurity e-retail framework?

The discussion of findings was guided by the study’s aim, which was to explore elements that should be included in an e-retail cybersecurity framework. The process followed was to understand the e-retail environment of South Africa, identify the challenges e-retail organisations face and determine how an e-retail framework can be developed for SMEs in particular. The study also serves as a means of creating awareness to small e-retail organisations on the means through which cyber attacks can be mitigated.

6.2 Peculiarity of the e-retail environment

In recent years, the retail industry has encountered transformation, driven by constant technological innovations. In South Africa, the transition to e-retail has been characterized by a number of challenges such as unequal economic and infrastructure distribution as well as cybercrime among various other challenges (Alexander & Mason, 2017). To a significant extent, e-retail activities are facilitated by the use of ICT. Although technological innovation opens up new opportunities for business for SME's, it calls for investment to partake, comes with risks and requires technical and operational skills to support the emerging opportunities (Alexander & Mason, 2017). For a greater grasp of the issue of cybercrime and cybersecurity in e-retail, it is imperative firstly to understand what e-retail involves, its distinctive characteristics (ecosystem) and how it operates. A better understanding of the e-retail ecosystem helps to better device a proper framework that will guide South African SME's in their daily business activities against cybercrime. Cybersecurity is of paramount importance to any business activity that involves the use of ICT to support business activity (Elbeltagi & Agag, 2016).

From its definition in biological sciences, an ecosystem is a community of living organisms (plants, animals and microbes) in conjunction with non-living elements of their surrounding interacting as a system (Iglesias-Pradas et al., 2013). Borrowing from this definition, an e-retail ecosystem is described as a complex network of interconnected systems such as banks, service providers, suppliers and legislation that make up an e-retail ecosystem. This e-retail activity with different actors within the ecosystem can also be best described as a lifecycle of an online purchase that involves banking, supplying and service provision (Chaffey, 2015). The various actors in this ecosystem have peculiar business processes and procedures they abide by. A blend of all the various actors and the processes that take place between them brings out the peculiarity in the e-retail environment. The e-retail ecosystem proposed for this study is shown in figure 16 below

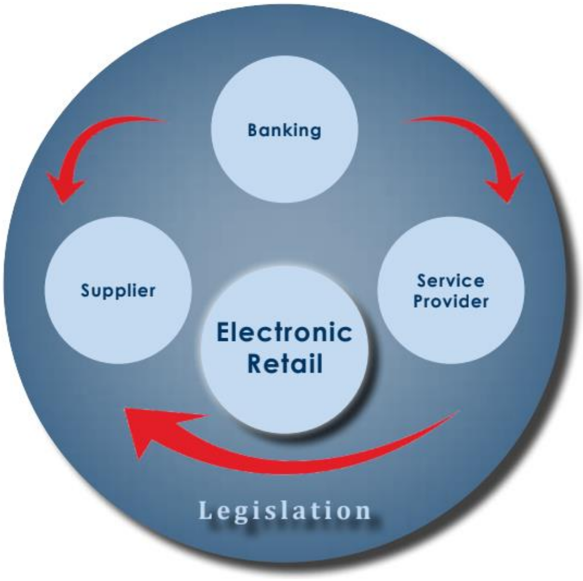


Figure 6.1: Interaction of niches or actors in the e-retail environment

The ecosystem shown in figure 16 above is a unique, a system made up of four major actors that interact together while being governed by respective legislation whose mandate among others is to address issues of internet-related crime or cybercrime. The ecosystems recognize salient global, regional and national legal imperative that support cybersecurity for e-commerce (Laudon & Laudon, 2016). Amongst a plethora of frameworks is the NIST cybersecurity framework which as used lens for the research findings. The NIST framework is one of the frameworks that should govern e-retail activities. The e-retail ecosystem seeks to create a secure cyber environment that facilitates protection of critical infrastructure. The Cybercrime and Cybersecurity Bill soon to be a law, acts as a comprehensive document that guides the cybersecurity within South Africa by imposing penalties which have a bearing on cybercrime (Department of Justice, 2015). The ECT act provides regulation of electronic communications and transaction, with a specific mandate of improving the use of ICT amongst SME's in South Africa (Government Gazette, 2002). The POPI Act seeks to safeguard personal identifiable information, stipulating how data should be processed and stored by custodians of data. (Mohideen, 2016). In the e-retail ecosystem, the banking actor also is also an integral aspect of the ecosystem. This actor provides financial services to the e-retailer. However, banks do not directly handle processing of transactions from purchase to delivery. This is process is done by a third party or merchant service; transactions are handled and processed by payment gateways. Payment gateways are intermediaries between the e-retailer, customer, and bank. Payment gateways validate online and card payments, granting approval or denial of transactions. Payment gateways operate on behalf of the bank to authorize payments. Also, payment gateways provide global business activities through the transfer of value and information among financial institutions, merchants, businesses and government entities (Anderson, Barton, Bohme, et al., 2013). Participants 5 and 8 as presented in Chapter 5 mentioned all validation of online or card payments is performed by the payment gateway. Participants 5, 7 and 8 mentioned the payment gateway the e-retailer uses is the most important aspect, not the bank. Further stating that "the payment gateway handles the transaction and validates it; the bank just collects your money". Participant 8 said there should be some security safeguards that the payment gateway should have, to avoid interception of transactions or an attack on payment systems. It acts as an interface between the bank and the e-retailer or payee. Payments gateways facilitate automated payment transactions between the e-retailer (seller) and buyer of goods and services (customer) (Meng & Zhang, 2005; LeBlanc, 2018; Nguyen et al., 2000). Examples of payment gateways in South Africa include PayPal, Pay4It, PayFast, PayU etc. (Theforge, 2012). Banks and payment gateways are also involved in customer data processing and other outsourced services within the IT services industry and the Information Technology sector (Alexander & Mason, 2017). As a result, they should be regulated by the *Protection of personal information act,* which ensures that they safeguard personal identifiable information used by companies for business purposes.

In order to be fully functional and effective, the e-retail ecosystem hinges on service providers whose roles are to provide technology hardware storage and peripherals to the e-retailer (Kumar & Bharati, 2016). This particular group of actors in the ecosystem also includes other sub-providers such as Internet service providers, data storage houses, web development companies for the creation of e-commerce websites. The supplier though considered a minute actor still plays a role in the ecosystem. The supplier main role is to supply products to the e-retailer and maintain an inventory list. Participants 2, 3, 4, 5 and 7 mentioned in areas where suppliers are granted system privileges to update stock, some security precautions should be taken. The security measures are dependent on the integration level of the supplier to the e-retailer. Participant 7 said secure file transfers can be used to secure both parties. Participant 4 mentions the use of web services. Participant 7 said the integration level should be settled in the SLA between the e-retailer and the supplier. All the activities within each actor in the ecosystem make use of ICT and happen on the cyberspace, hence the need for a cybersecurity within this various actors.

6.2.1 Ecosystem requirements

For an in-depth understanding of this proposed ecosystem, specific questions on each actor (retailer, banks, service providers, legislation) were asked to participants. This was done to understand the role each actor plays in this ecosystem. In addition, how South African SME e-retailers stand to benefits from each actor.

I. The e-retailer

Reactive measures aim to counter attacks, these reactive measures are based on lessons learned from previous attacks which have been analysed to improve on defensive measures (Biggio & Roli, 2017). Reactive strategies are often more convenient and cost-effective compared to proactive approaches aimed to mitigate against future attacks (unknown attacks). A proactive approach to cybersecurity seeks to anticipate threats and attacks in two ways (i) identification of threats against infrastructure under design and simulating attacks. (ii) Conceiving suitable countermeasures (ibid). Al-Tarawneh et al., (2012) recommend a balance of both reactive and proactive security measures. Organisations are encouraged to move from solely informal, reactive approaches to more adaptive and proactive risk approach. Through proactive approaches, organisations will remain abreast to an ever-evolving threat landscape, which in turn will provide insight to who, what, where, when and how attacks manifest (Rege et al., 2018). With the increase in internet use and crimes, cybersecurity can no longer be a back burner in organisations. It has to be a major consideration for any organisation in particular e-commerce (Mcintyre, 2018). Cybersecurity should be given a priority in organisations strategic planning, many a times cybersecurity is seen as a time waster in organisations especially SME's (Von Solms, 2015).

II. Legislation and Standards

Legislation plays an important role in cybersecurity. Legislation in this study includes frameworks, policies, acts, and laws around ICT and cybersecurity. Legislation exposes organisations to best practices and standards. In addition, it also acts as benchmarks through which e-retail organisations can measure there cybersecurity initiatives and practices. A number of cybersecurity legislation and frameworks could be of benefit to e-retail organisations. SME's often encounter challenges to implement information security frameworks as a result of a lack of resources and the comprehension of these frameworks (Alshboul & Streff, 2015).

Table 6.1: Description of legislation and standards

Legislation/Standard/Framework	Description
ITIL	Information Technology Infrastructure Library (ITIL) is a set of detailed practices for aligning IT services to business needs. The framework focuses on streamlining IT services with organisational needs. It provides a set of interconnected best practices that

	provide guidance for developing, delivering and managing IT services within an organisation (UpGuard, 2017). The ITIL framework can act as a good start for foundational stages for an organisations security program. However, the standards such as these have come under immense criticism; some organisations implement the ITIL frameworks but still have major cyber breaches. A number of authors suggest that the COBIT, ITIL and ISO standards are not cybersecurity standards but are management standards (Chora et al., 2015). Further stating that standards like the PCI-DSS provide very specific technical controls aimed at reducing credit card fraud.
COBIT	The Control Objectives for Information and Related Technologies framework was created by ISACA for IT management and governance. It is an internationally accepted set of tools for ensuring organisations meet their goals and objectives (Information Systems Audit and Control Association, 2015). Supporting Chora et al., (2015) argument, COBIT focuses on IT governance and not fully address cybersecurity. However, the COBIT framework has a domain called Delivery and support which is concerned with the management of security and continuity (Information Systems Audit and Control Association, 2014). Under the DS5 Ensure Systems Security: • Management IT Security • IT security plan • Security testing • surveillance and monitoring • security incident definition • protection of security technology • network security

	Though an IT management and governance framework, it contains important aspects of basic cybersecurity practices.
ISO/IEC 27032	An international standard created by International Electro-technical Commission in 2012. A number of ISO standards exist but of particular interest to cybersecurity is the ISO/IEC 27032. Provides directions on security practices for all contributors in the cyberspace. It also provides technical guidance on how to mitigate against cyber attack profiles (Fan et al., 2017; Garae & Ko, 2017). More so, it provides a model for the establishment, implementation, operation, monitoring, reviewing, maintaining and improving IT practices (Aggarwal, 2014).
NIST	The NIST describes an approach that enables organisations irrespective of size, risk degree or cybersecurity sophistication to apply principles and best practices of risk management to improve the security and resilience if infrastructure (Johnson et al., 2014)

III. Supplier

The supplier forms one of the actors as clearly illustrated in the e-retail ecosystem. In fact, the supplier could also fall under the service provider, as they offer products or services to the e-retailer. In traditional retailing supplier provides a product or service based on a pre-determined and agreed inventory list (Olsen & Ellram, 1997). However, today there is a closer relationship between the supplier and the e-retailer. Large organisations such as Walmart provides its suppliers with sales and inventory data using web technology (Kumar, 1996). In addition, Chrysler Corporation gives direct access to suppliers to certain of its inventory processes (ibid). With the proliferation of ICT, the power of suppliers has become influential. Many large organisations are able to provide its suppliers with a direct access to its IT infrastructure (Laudon & Laudon, 2012). Therefore, it will be ideal for suppliers to take responsibility of their cybersecurity. In addition, it is advised that organisations place cybersecurity requirements on suppliers to ensure they are used as baits to targets organisations. The level of cybersecurity should depend on the relationship between the e-retailer and the supplier. What are the activities, access, and processes are the supplier able to perform on the e-retailers' infrastructure? Security requirements should be based on the integration level of the supplier and the e-retailer.

IV. Service Provider

As discussed earlier, service providers are third party companies that provide services to the e-retailer such as Internet service providers, data storage houses, web development companies for the creation of e-commerce websites. Service providers are usually brought in to handle non-critical aspects of the business while critical aspects are handled in-house (Bhisikar, 2011). Service providers should also seek to address aspects of their business that require cyber securing. Cybersecurity-related services should be imposed on service providers by the e-retailers; this should be agreed upon in the service level agreement. An SLA is a contractual document that contains various promises & measurable terms regarding services that a provider intends to provide (Gulia & Sood, 2013; Barrel, 2015). The SLA is usually a legally binding contract between both parties, which transparently details the roles and responsibility of the service provider to the e-retailer and vice versa (Dash et al., 2014). Cybersecurity should be one of the parameters contained in the SLA, where both parties have to agree and lay down measurable terms on how it plans to handle cybersecurity.

6.3 Mitigation strategies

6.3.1 Information protection processes and procedures

I. Validating payments to prevent online fraud

The Payment Card Industry Data Security Standard (PCI DSS) provides service providers and e-commerce merchants with benchmarks on how to implement stronger security infrastructure to reduce cyber risks. Payments processes involve a number of stakeholders including e-retail merchants, payment gateways, banks and other payment card networks (Liu et al., 2010). For instance, a purchase is made on an e-retailers site using a card it goes through the e-retailers bank and the payment card network. On successful verification, the amount of the product is debited to the payment card account. This entire process requires the e-retailer to obtain and store the card information and the transaction details on its computer systems. Thereafter, the transaction details are sent over the network to the card issuer. Any vulnerability in this payment cycle could result in significant damage to all the stakeholders as mentioned above (Lupu et al., 2016; PCIDSS, 2017).

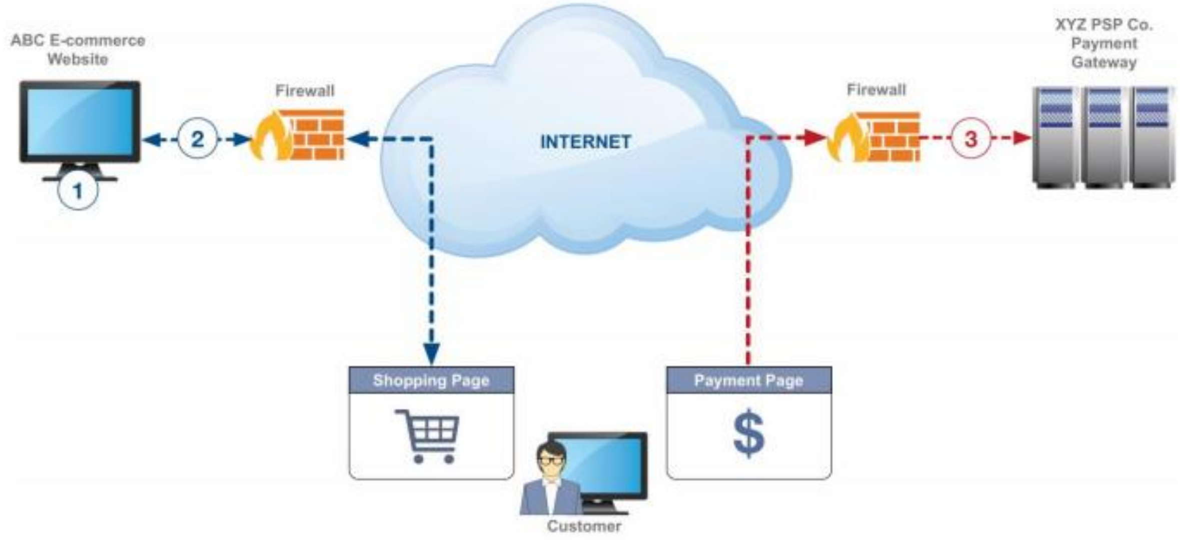


Figure 6.2: Payment card flow

Figure 17 above shows an e-retailer called ABC, outsourced its e-commerce website to a service provider. The service provider is responsible for hosting, management and development for ABC's website. A firewall is shown between the internet and e-retailers website. From the presentation of findings presented in chapter five, a number of participants stressed the need for e-retailer to comply and abide by the PCI DSS. The PCI DSS applies to any organisation that accepts or processes payment cards (Liu et al., 2010). The PCI DSS prescribes 12 operational security requirements for developing a secure Card security payment system (PCI-DSS, 2016).

Table 6.2: PCI data security standards (PCI-DSS, 2016)

Goals	PCI DSS REQUIREMENTS
Build and Maintain a Secure Network	1. Install and maintain a firewall configuration to protect cardholder data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	5. Use and regularly update anti-virus software or programs 6. Develop and maintain secure systems and applications
Implement String Access Control	7. Restrict access to cardholder data by business need-to-know 8. Assign a unique ID to each person with computer access 9. Restrict physical access to cardholder data

Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes
Maintain an Information Security Policy	12. Maintain a policy that addresses information security for employees and contractors

II. Patch management Antivirus, backup

Not running the latest updates was identified as some of the reasons for the spread of the wanna cry ransomware in 2008. Furthermore, it was discovered that computers that were infected were not running the latest windows updates. This allowed for the propagation to other victims (Koopman, 2017). System-wide updates are important techniques to prevent cyber attacks in particular ransomware attacks. System-wide refers to all applications running on an organisations network. A system-wide updates ranging from antivirus software, operating systems, applications, scripts to removable media. Unpatched security holes are methods through which ransomware propagates. System-wide updates include regular backup of all systems and data on a scheduled basis. Cloud back-up services are available to organisations, providing more cost-effective methods to traditional backup methods (Ganorkar & Kandasamy, 2017). Participant 7 presented the need of installing updates, this was also suggested by (Akkas et al., 2017) stating that installing latest updates solves the latest bugs, flaws and security threats.

Backup and recovery management is a vital mitigation practice, involving periodic and regular backups and testing the backups (Myalapalli, 2014). It should fall under the disaster recovery plan of any organisation that makes use of ICT. It involves copying physical or virtual files to a secondary site or device for preservation in the event of a disaster, to ensure continued operation of the organisation (Jensen et al., 2007).

Most SME's operate from a single location, which means backups are normally stored in the same location as the other organisations computer devices. This means in the event of a disaster, there will be destruction to both the devices and backups that were meant to ensure continued operation of the organisation. The price for storage is decreasing, a number of new backup options such as cloud-based storage are available. With all the above reasons, it is logical for SME's to improve their availability of backups. However, there are concerns about storing sensitive and business-critical information on foreign devices. To alleviate these fears there are a number of safe and secure backup systems that can be used such as Resilia and other cloud-based options (ibid). There are situations where backup data is corrupted resulting in unrecoverable data. It is recommended that service providers perform incremental online and offline backups of very important data. Incidences of ransomware attacks often target stored data, in an aim to make the data unrecoverable (Popoola et al., 2017). Regular backups cannot be overemphasized; an up-to-date backup kept off-site. It is also advisable to encrypt backed up data so that only an authorized user can restore it (Tailor & Patel, 2017). However, this process may only be applicable to e-retailer who outsource their database management to third-party service providers.

III. Use of Security products

With the advancement in technology and research, there are products that SME's could purchase to ensure effective application and network security. One of such and mentioned by a participant is a product called Stormshield. Stormshield is a UTM product that provides network protection for small to large businesses. With four areas of protection which includes: Network security, data security, endpoint security and virtualized infrastructure protection. Very importantly, it is aimed at ensuring security for small businesses. Its UTM design ensures effective application and network vulnerability through a single firewall. Vulnerable applications and workstations across multiple servers monitored in real time and an adapted protection can be applied. In addition, it helps organisations control and manage internet usage (Katata et al., 2009; Nycz et al., 2015).

IV. Firewall configuration management and detection systems

Intrusion detection systems are one of the solutions to protect from DOS attacks; they act as both reactive and proactive protection against attacks. Organsation use routers as access points to the internet and other shared resources. Therefore, the choice of the router is important, more pertinently, the use of packet filtering router is encouraged. Packet filtering accommodates the use of filtering techniques such as Ingress and Egress filtering (Piskozub, 2004). Using these two filtering methods, organisations are able to detect and filter spoofed packets. Ingress and egress filtering are Spoofing Prevention Methods (SPM) to prevent spoofing attacks on networks. (Bremler-Barr & Levy, 2005). A spoofed packet is a packet that has a source address that is different to any address assigned to the system which sent the packet (Jones, 2004). In other words, it is a forged packet from an attacker whose address does not match the address from the source (Reddy et al., 2017). Ingress filtering is a technique by which routers and firewalls determine what traffic is allowed to pass through (Patil & Perkins, 2005). Ingress filtering rejects packets with an invalid source address; packets are dropped with tampered addresses. In egress filtering a router filters out packets leaving the network whose address does not match the network address space (Bremler-Barr & Levy, 2005). Egress filtering filters outgoing traffic to make sure only legitimate packets are allowed to leave the network. Ingress and egress filtering can be used to prevent spoofed packets from reaching their destination (Karig & Lee, 2001).

However, implementing ingress and egress filtering is liable to incur significant costs from labour, equipment etc. As a result, a number of ISPs decide to use it. Egress filtering requires a proper configuration because if configured wrongly could block legitimate traffic (Bremler-Barr & Levy, 2005). Other router-based filtering include: (i) disabling unused services: To prevent attacks from using unused services, disabling services and ports is advisable. (ii) Applying security patches: To ensure the latest security patches are installed to prevent new known attack signatures. (iii) Changing IP address: this is a solution when the infected IP address is known, it involves changing the IP to a new one, then allowing routers to drop the infected IP. (iv) Disabling IP broadcasts: used to prevent Internet Control Message Protocol (ICMP) flood and smurf attacks and (v) Creating client bottlenecks: use of zombie computers to entrap attackers. Although these preventative measures ensure increased security, they are unable to completely eliminate the risk of an attack (Xianjun Geng & Whinston, 2000; Douligeris & Mitrokotsa, 2003; Maciá-Fernández et al., 2007).

6.3.2 Risk management strategy

The risk management strategy falls under the identify core of the NIST cybersecurity framework. The Identify core involves the development of organisational understanding to manage cybersecurity risks (NIST, 2014). A strategy is a plan of action designed to achieve an aim. The first step in risk management strategy is to prepare a cybersecurity incident response plan (CSIRP) (Theohary & Rollins, 2009). The cybersecurity incident response plan, also known as the cyber incident response plan or computer security incident handling guide, is a comprehensive response plan to manage security events in order to limit the damage, reduce cost and recovery time. A cyber-incident response plan should not be a static document. It is vital to integrate it into organisational processes and to review and update on a regular basis (Pritchett, 2017; Darville, 2017; Oakes, 2018). It is a critical step towards the protection of critical infrastructure (Brooks, 2017). A CSIRP presents organisations with key tools to use after a cyber attack. A basic incident comprises of six phases: preparation, detection, containment, investigation, remediation and recovery (Cichonski et al., 2012; Tucker et al., 2013; Raderman, 2015). The Computer Security Incident Handling Guide prescribed by U.S Department of Commerce provides the life cycle of an Incident response plan as shown below

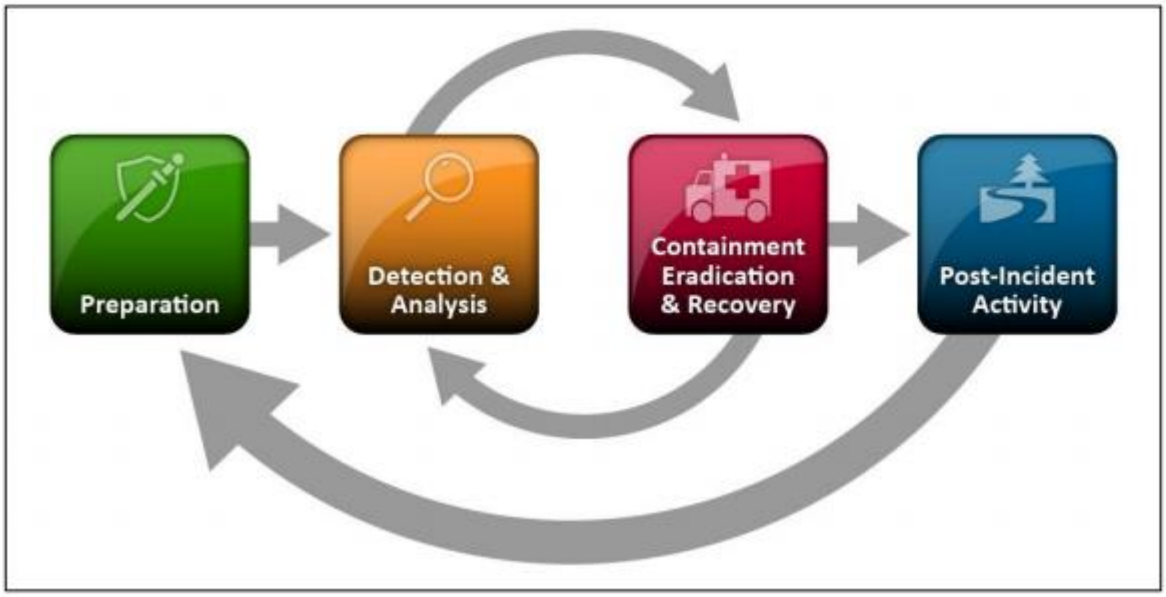


Figure 6.3: Incident Response Life Cycle

Preparation involves ensuring systems, assets and applications are sufficiently secure. There should be a periodic risk assessment of systems and application. Each risk is prioritized and categorized according to its severity. Hosts should be patched and the principle of least privilege should be configured, in addition, organisational wide system or host hardening. The physical network perimeter should deny all activity that are not permitted. Users should be educated on the policies and procedures regarding the use of networks, systems and applications. Lessons learnt from previous incidents should be circulated for all to learn. Staff trained to maintain organisational security standards to minimize the frequency of incidents. Detection involves determining if an incident has occurred, the type of incident, the extent of the damage. This is normally a challenging phase for organisations. Signs of an incident fall into two categories: precursors and indicators. A precursor is a sign that an incident may occur in the future while an indicator is a sign that an incident may have occurred or may be ongoing. Intrusion detection and prevention systems, antivirus and antispam software, file integrity and checking software are all common sources of precursors and indicators. Detection, containment and investigation often occur in the same circle under a broad theme of Detection and analysis. The initial analysis phase involves knowing the expected activity of networks and systems. In order to easily identify deviations from normal activity. Secondly, a retention log should be kept of incidences that happened in the past as they may show reconnaissance activity or previous instances of the attack. Containment is important to prevent the incident from overspreading and causing severe damage, one major component of containment is decision making. Decisions taken will be aided by having in place a predetermined strategy and procedure for containing the incident. Lastly, but in no way the least is the Post-incident activity or lessons learnt. This is normal an overlooked and omitted stage, it is important as it shows committed to learning and desire for improvement. In this stage, all parties are involved to review and reflect on the incidents to seek new and improved ways of dealing with such incidents (Cichonski et al., 2012). In addition, the Centre of Cybersecurity Belgium provides key elements of a cyber-incident response plan.

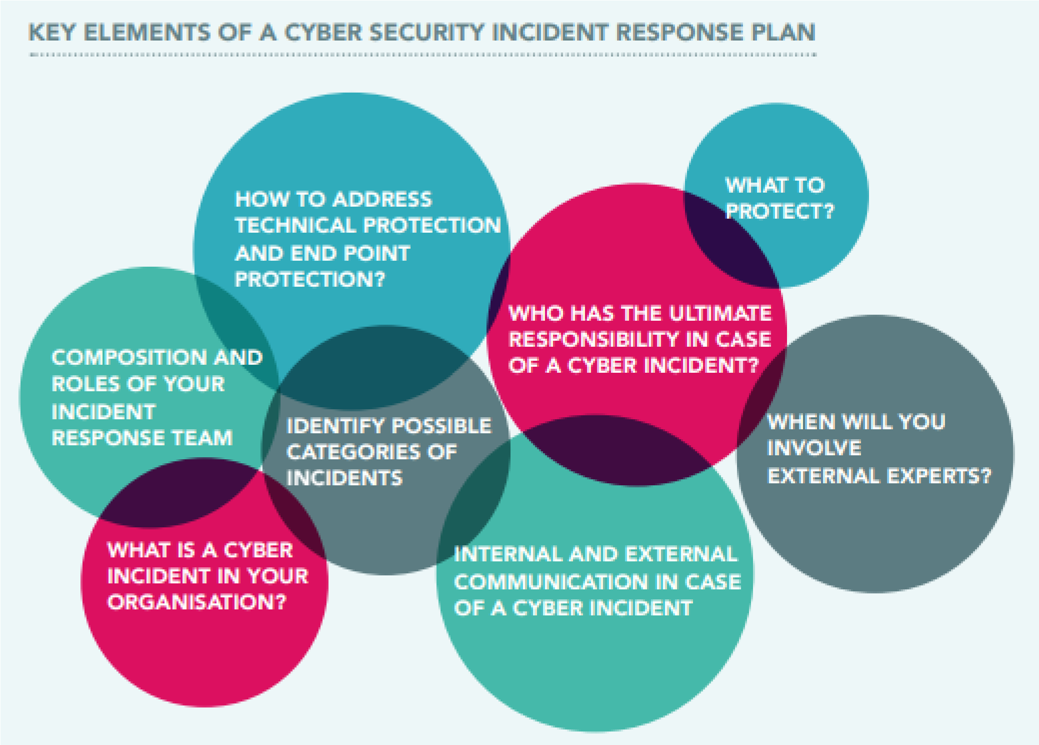

KEY ELEMENTS OF A CYBER SECURITY INCIDENT RESPONSE PLAN
HOW TO ADDRESS TECHNICAL PROTECTION AND END POINT PROTECTION?
WHAT TO PROTECT?
COMPOSITION AND ROLES OF YOUR INCIDENT RESPONSE TEAM
WHO HAS THE ULTIMATE RESPONSIBILITY IN CASE OF A CYBER INCIDENT?
IDENTIFY POSSIBLE CATEGORIES OF INCIDENTS
WHEN WILL YOU INVOLVE EXTERNAL EXPERTS?
WHAT IS A CYBER INCIDENT IN YOUR ORGANISATION?
INTERNAL AND EXTERNAL COMMUNICATION IN CASE OF A CYBER INCIDENT

Figure 6.4: Key elements of a Cybersecurity Incident Response Plan

Figure 19 above poses some key questions that a CSIRP for any organisation should consider. It begins with an identification of all assets that are valuable and vulnerable. An incident response team should be established, having the responsibility to execute decisions in the event of an incident. The team should consist of capable and qualified personnel with the required knowledge to respond to incidents. Irrespective of the size of the organisation, it is expensive to develop and maintain all needed expertise and skills for incident response in house. It is advisable and cost-effective to collaborate with external cybersecurity response teams to provide other specialized expertise. The CSIRP is a very important document that ICT organisations must have (Darville, 2017). Participant 8 mentioned “an incidence response plan is the first step in dealing with these attacks, without it how do you try to solve any type of risk you might be currently facing”. “An incident response plan comprises of pre and post actions to mitigate risks. Participant 8 was passionate about having an incident response plan in place, going on further to say all organisations need one, and that incidence response plan will detail procedural steps to mitigate cyber attacks. The CSIRP provides the organisation with the course of action that an organisation embark on in the event of a security breach or cyber-attack.

6.3.3 Awareness and training

To preserve a cyber-secure environment e-retail organisations are to ensure personnel are equipped with relevant cybersecurity awareness education and trained to perform cybersecurity-related duties and responsibilities in accordance with related policies, procedures and agreements. According to the (NIST, 2014), awareness and training involves (i) All users are informed and trained. (ii) Privileged users understand roles and responsibilities. (iii) Service providers understand roles and responsibilities. (iv) Senior executives understand roles and responsibilities. (v) Physical and information security personnel understand roles and responsibilities. For e-retailers that operate with service providers to provide a resource or the other should ensure service providers also provide cybersecurity-related services, which should be agreed upon in the service level agreement. Developing an effective cybersecurity awareness culture is important and should be driven by the top management of the organisation. Through awareness and training programs a security culture is encouraged (CREATe, 2016). Participant 4 shared an example of how his organisation is trying to instil a cybersecurity culture within an organisation. Use of posters in designated walls and passageways on basic do’s and don’ts. In addition, where organisations are not sufficiently equipped to provide training, organisations should consider sending personnel on workshops and short courses on cybersecurity (Taylor et al., 2004). A well-structured training and awareness program on cybersecurity issues should be given to personnel to be able to identify and handle cyber threats. The main purpose of a security awareness programme is to educate and raise employee cybersecurity awareness. The success lies in the manner in which awareness programme is communicated and delivered (Abawajy, 2014; Ghazvini, Arash and Shukur, 2016; Alshaikh et al., 2018). There are a number of commonly used methods through which cybersecurity awareness training can be administered namely:

A. Conventional delivery method

Use of paper-based security awareness delivery methods like posters and flyers, this method cuts across all electronic resources and paper resources. Reminding users about the appropriate use of a company’s assets, do and don’ts. For example, reminding users not to keep passwords in plain sight. However with this method, the challenge lies in keeping track of whether it has been read or understood by all (ibid).

B. Instructor-led delivery

This includes a number of formal presentations facilitated by an instructor (local or external) expert. With seminars, workshops etc. One advantage of this method is that instructors are able to interact with trainees, perceive nonverbal clues and modify instructional methods to suit the needs of the trainees. Group and collective tasks can be done to encourage participation and improve comprehension of the content taught.

C. Online delivery method

This method is often used to support multimodal teaching methods. It consists of online content such as online discussions, webinars, animations and multimedia. This method is often used when participants reside in different geographical locations, where a face-to-face training is impossible. The web-based delivery method also falls under online delivery methods. Use of email to remind staff actions that improve organisational security posture, screensavers that display important security points. This is one of the most effective means of the delivery of security training and awareness (Ghazvini, Arash and Shukur, 2016).

D. Game-based delivery method

This method is often used to supplement one of the more traditional methods. The advantage of this method is the challenge and user engagement that is experienced. Due to the interactive nature of games, organisations can adopt this method to engage staff on organisational security awareness objectives. CyberCIEGE is an example of a game-based information security awareness delivery method which has been successfully used by various organisations to teach security concepts to staff (Irvine et al., 2005).

E. Video-based delivery method

This method is facilitated by educational videos to support the drive for awareness. The benefit of this method is that it provides audiovisual learning for trainees, and are able to access the training at their convenience as it is not time-dependent. This is one of the ideal training methods as it allows for user interaction and reusability, as the videos can be watched on repeated occasions. Distribution is another benefit, soft copies can be forwarded and pass to a wide variety of audience.

F. Simulation-based delivery method

This method involves trainees being immersed in a scenario. Trainees are immersed in an environment where they have to carry out specific security incidents and are required to perform the necessary practical steps to curb the incident. In recent times, this method has received attention. It allows for user engagement, trainees are able to simulate real events in a controlled environment.

6.3.4 Compliance

The Merriam-Webster dictionary defines compliance as conformity in fulfilling official requirements. It is important for e-retail organisations to benchmark organisational activities and procedures to international standards. Compliance is important; a number of benchmark standards are available for organisation to measure against in terms of their cybersecurity efforts. One of such is the International Organisation for Standardization (ISO). Catalogue ISO/IEC 27032 provides guidance on how organisations can improve and fulfil the necessary cybersecurity criteria. Implementing the ISO/IEC will contribute significant improvement to cybersecurity in the following areas: information security, network security, internet security and critical information infrastructure protection (Zeneli, 2016). Specific to e-retailer or organisations that process card payments is the Payment Card Industry Data Security Standard (PCI-DSS) as discussed in section 6.3.1.1 where the requirements were presented. The PCI DSS applies to all organisations that process, store or transmit cardholder data (Morse & Raval, 2008; Chorney, 2016).

6.3.5 Access control

According to the (NIST, 2014) Access control addresses that access to assets, facilities, processes and transactions is restricted to authorized users and it involves (i) Identities and credentials are managed for authorized devices and users. (ii) Physical access to assets is managed and protected. (iii) Remote access is managed. (iv) Access permissions are managed, incorporating the principles of least privilege and separation of duties. (v) Network integrity is protected, incorporating network segregation where appropriate. An access control policy determines the access granted under circumstances to a user. Access control policies are divided into 3 categories

a) Discretionary Access Control

In discretionary access control, access rights are granted based on the identity of the subjects. Access is granted to a subject (user). It is based on granting or denying access privileges for the use of system objects (Jukic et al., 2002). The user is granted discretionary access and is capable of passing on that access to another subject (Alhaqbani & Fidge, 2008). Access is granted based on the prerogative of an object owner (Narayanan & Gunes, 2011). In light of the above descriptions, access to organisational resources is based ‘need-to-know’ and ‘need-to-use’ bases. The user should be restricted to have only what is needed for a task. The challenge with discretionary access control is that there is no control on the flow of information from one subject to another (Sandhu, 1993).

b) Mandatory Access Control

In mandatory access control, access control is overseen by a central authority and not by the individual owner of the object. Compared to the discretionary access control privileges cannot be pass on to other subjects (Alhaqbani & Fidge, 2008). Only the authority can grant access to the subjects, however, the subjects cannot pass on privileges to others. This is considered an ideal access control method with impressive security advantages however, its rigidity allows minimal room for flexibility (Jukic et al., 2002).

c) Role-based Access Control

In role-based access control, access control is associated with roles and users are assigned relevant responsibilities (Narayanan & Gunes, 2011). Privileges are granted based on individual roles that users have within the organisation. Users take on different roles, and then access rights are granted based on the roles. The principle of 'Need-to-know' exists because permissions are granted to the subjects whose roles require them (Alhaqbani & Fidge, 2008). One advantage of role-based access control is that higher organisational rules can be implemented, the policy is based on a certain hierarchy of roles and not be individual subjects (Sohr et al., 2008). This access control method allows and promotes separation of duties; separation of duties is valuable in deterring fraudulent practices as no single individual can execute all transactions (Ferraiolo et al., 2001).

6.3.6 Security continuous monitoring

According to the (NIST, 2014) security continuous monitoring addresses requires that assets, practices and activities be monitored on a schedule basis to identify cybersecurity events and corroborate the effectiveness of protective measures. More closely, it involves (i) Schedule monitoring of network to detect potential vulnerabilities. (ii) Monitoring of the physical environment. (iii) Personnel activity is examined to detect potential abnormalities. (iv) External service provider activity is monitored to detect potential anomalies. (v) Scheduled vulnerability scans are performed. Continuous monitoring is a process because the information security landscape changes, so also organisational processes and security strategies must actively adapt to the evolving threats (Mlelwa & Yonah, 2017). Participant 8 spoke about cyber resilience as a level all organisations aspire to attain. Cyber resilience is the ability to defend and survive from a cyber incident and return to a normal functioning state (Williams & Manheke, 2010). In addition, "The ability to continuously deliver the intended outcome despite adverse cyber events" (Björck et al., 2015). Tatar et al., (2017) described Cyber resilience as the robustness of an organisation against cyber attacks. From the above definitions, cyber-resilience is a process that can only be achieved through continuous improvements of security practices. To attain cyber-resilience requires investment in control mechanisms (de Crespigny, 2012).

6.4 Validating research findings

This research lead to findings that correlate with a combination of previously established frameworks and provides valid outcomes that tie into Eisenhardt's procedure of building theory when using case study research. Which states that theoretical induction is the close link with empirical reality that allows the development of testable, relevant and valid theory (Eisenhardt, 1989). The guided processes are:

- Getting started: defining the tenets of the research from prior knowledge with interrogating questions.
- Selecting cases: cases for the study were identified and selected from a population. Bearing in validity, in order for replication of findings.
- Crafting instruments and protocols: use of multiple data collection methods to ensure the authenticity of findings
- Entering field: allows the researcher to gain insight into emergent themes and unique case features.
- Analyzing data: the researcher is able to engage data across multiple views resulting in an in-depth understanding of data and constructs of the theory.
- Shaping hypothesis/assumptions: the researcher is able to identify logic across cases through the repeated detail of constructs by demonstrating reasons that confirm and validate the theory.
- Enfolding literature: contrasting constructs against similar or conflicting literature hones the description of constructs and thus elevates the theoretical and expands generalizability.
- Reaching closure: reaching theoretical saturation, at this point the process ends.

6.5 Conceptualizing E-retail and cybersecurity

As stated by Saldana (2016), "the development of an original theory is not always a necessary outcome for quantitative inquiry, but acknowledge that pre-existing theories drive the entire research enterprise, whether you are aware of them or not".

In order to understand and conceptualize e-retail and cybersecurity, insights were taken from elements found in literature and interview questions answered. Emergent finding such as Compliance has been added to the framework for Improving critical infrastructure cybersecurity by NIST (2014:19) to produce an extended framework for Improving critical infrastructure cybersecurity framework (Figure 5). The newly added construct is shown in green (Figure 5)

The latest version 2018 version of the NIST framework was taken into consideration, however, this research made extensive use of the NIST framework of 2014.

Table 6.3: Added category to the NIST framework

Function	Category
Protect	Access Control
	Awareness and Training
	Data Security
	Information Protection Processes and Procedures
	Maintenance
	Protective Technology
	Compliance

6.6 Summary of Chapter Six

Chapter Six expounded the themes that emerged from the findings and gave a preamble answer to the research questions with the aid of prior proven literature. The emergent theme is shown in the green shade in Table 12.

Findings show that e-retail organisation do experience cybersecurity challenges. It also shows that cybersecurity needs strategic planning. This will help organisations achieve business goals with the certainty of protection against cyber attacks within the cyberspace. The findings revealed some practices that can drive cybersecurity within organisations. It further provided a scheme for ensuring protection against cyber attacks on small e-retail organisations, which were represented by an existing framework to ensure verifiability and validity of the research findings.

The next chapter (Chapter Seven) is the final chapter of this research study. It brings closure to the research by addressing the main aim of the study which is to understand the e-retail organisation and propose elements for an e-retail cybersecurity framework. It also brings to a conclusion the entire process.

CHAPTER SEVEN: CONCLUSION AND RECOMMENDATION

7.1 Introduction

Cybersecurity needs to be the strategic focus of organisations and at a national level. Several authors, including Ghernouti-Hélie (2010); Ahmad et al., (2014); Romero-Mariona et al., (2017) plead that organisations engage in activities that improve the security posture of their organisations. There are factors contributing to lethargy to cybersecurity, one of which is the cost implication. However, the cost implications of protection in most cases is far less than the cost of mitigation or remediation (recovery) in the event of an attack. There are cost effective and scalable security measures SME's can adopt, rather than having no defence against numerous attacks.

The research problem engaged in this study was to understand the cybersecurity challenges amongst e-retail organisations. Despite the well-documented protection variants and the benefits thereof, it appears that SMME's are not adopting cybersecurity into their strategies. This has wide-ranging reasons from lack of skilled personnel to fear of cost implications. In addition, the implications and consequence of being prone to attacks that cripple the business as highlighted in chapter one will ultimately result in unforeseen operational, financial, strategic and other challenges to the organisation and the country at large.

In an attempt to understand the challenges e-retail organisations face, this study explored the organisational perception of cybersecurity. Findings point to the challenging aspects and opportunities for cybersecurity practices. The gained insight and understanding do not solve the problem, but it contributes to the resolution by discovering problems and avenues that require addressing. The study's aim and objective was accomplished by adopting a multiple case study design. Semi-structured interviews and a literature review were sources of data collection. Participants purposefully selected, which included CIO's, Security developers and security researchers.

This chapter concludes this study by presenting answers to the research questions set out in (chapter 1). Some recommendations to guide SMME's and policymakers is presented based on the cognizance gained from the study. Furthermore, the research contributions, limitations and further research are addressed in this chapter.

7.2 Answers to research sub-questions

Research sub-question 1: What are the peculiarities of the e-retail industry in terms of cybersecurity?

The findings show that e-retail operates across a number of industrial sectors and actors. The findings are:

i. Banking: payment gateways validate online and card payments, proving approval or denial of transactions. Payment gateways operate on behalf of the bank to authorize payments.
ii. Service Providers provide services to the e-retailer such as Internet service providers, data storage houses, web development companies for the creation of e-commerce websites.
iii. Suppliers supply products or render a service to the e-retailer and maintain an inventory list
iv. Legislation as benchmarks through which e-retail organisations can measure there cybersecurity initiatives and practices

Research sub-question 2: What measures have e-retail organisations taken to comply with current cybersecurity laws?

The answers below address this particular sub-question:

i. There is no blueprint guide organisations follow to mitigate against cyber attacks
ii. Organisations are aware of legislation but do not necessarily comply with legislation
iii. There are no compliance regulators to ensure organisations are cyber secure.

Research sub-question 3: How can South African e-retail organisations ensure cybersecurity practices?

i. Continuous improvement and monitoring of organisational practices
ii. Staff members awareness and training programs
iii. Adherence to frameworks and standards
iv. Scheduled consultation with experts in cybersecurity

Research sub-question 4: What should characterize a cybersecurity e-retail framework?

I. A framework that takes into account salient technical frameworks on cybersecurity.
II. A framework that built from actors within the cybersecurity ecosystem.

7.3 Answers to main Research Question 1

One of the main research questions is: What are the specific cybersecurity challenges faced by e-retail organisations?

There are challenges faced by e-retail organisations are:

a) E-retail in Africa and in particular in South Africa is still in its infancy compared to developed countries, there are a shortage and need for cybersecurity expats to provide knowledge and expertise on how organisations can trade securely.

b) Development and implementation of cybersecurity policy that evolves with advancements in cybercrime.

c) Dissemination of cybersecurity awareness within organisations and collaboration amongst academia, private and public sector.

d) All participants examined experience security issues that required some form of mitigation.

e) The South African cybersecurity is heavily reliant on security products.

f) The e-retail organisation requires the assistance of government to prioritize cybersecurity in terms of passing legislation, frameworks and the policing thereof.

g) Organisations are not aware of legislation and frameworks available for cybersecurity.

h) There is an increasing amount of outsource IT expertise, hence organisations have no control over the security of data and processes outsourced to service providers.

i) Cybersecurity is not a given priority in most organisations, some organisations perceive cybersecurity as a needless exercise that requires significant financial input.

j) The current South African legislation focuses or contextualized to large organisations, without taking into account the peculiarities of small businesses.

From an organisational viewpoint, challenges differ from an organisation to the other. Therefore, it will be practically impossible to have a one-solution fits all strategy to address these challenges.

7.4 Answers to main Research Question 2

The second research question is: How can South African e-retail organisations mitigate against the occurrence of cyber attacks?

It is important to understand the place of the cyberspace and the e-retail environment found in this study. These concepts of cyberspace, attack profiles, and e-retail are important in terms of the cyber attack mitigation. Figure 7.1 is a proposed framework to mitigate attack profiles in the cyberspace against e-retail.

7.5 Framework presentation and discussion

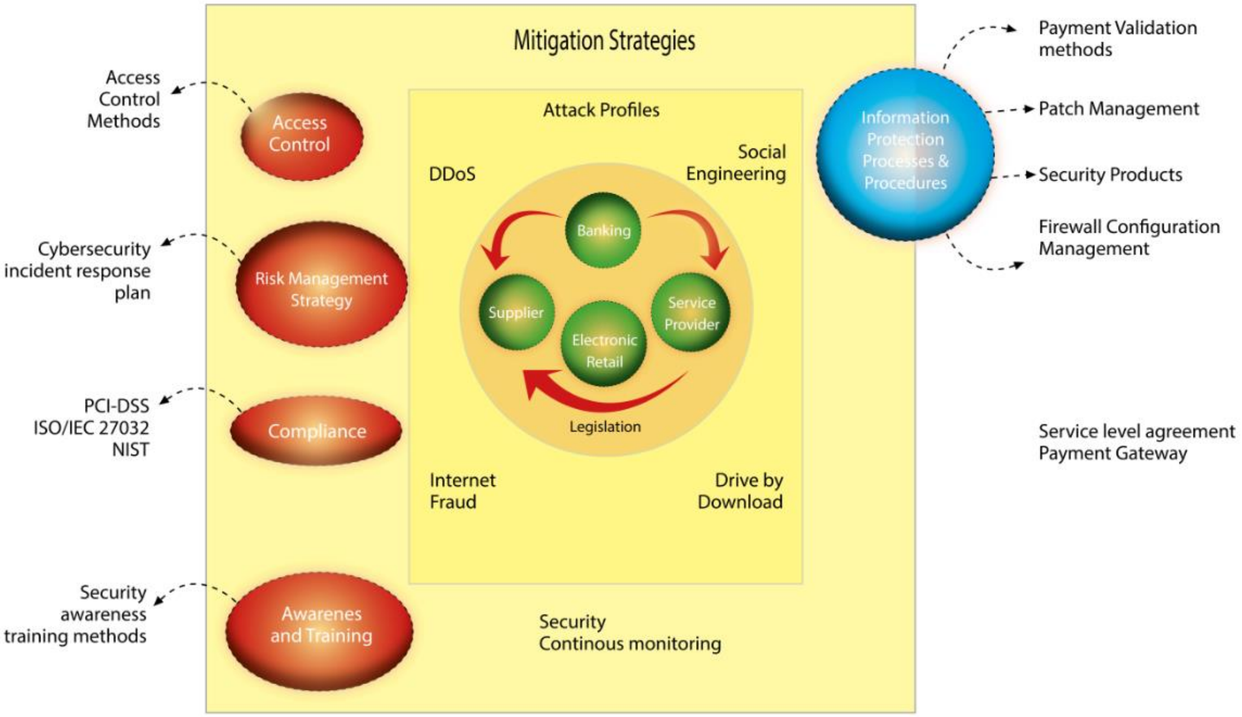


Figure 7.1: Electronic retail cybersecurity framework [source: author]

This framework from literature, cybersecurity frameworks and mostly importantly insights from participants and the companies interviewed in this study. It composed of a number of layers:

- *E-retail ecosystem:* at the centre of the framework is the e-retail ecosystem was discussed extensively in 6.2 of Chapter 6. The ecosystem brings to light the various actors around which a functioning e-retail venture revolves around. Furthermore, 100% of the companies agreed to this and/or have a type of e-retail circle as the above.
- *Attack Profiles:* As e-retail is reliant on the internet and ICT, therefore it operates within the cyberspace. The cyberspace is the realm of communication and interaction between computers facilitated by data exchange via the internet. As a result, surrounding the e-retail ecosystem is a plethora of cyber attacks, which could negatively affect the processes that are conducted within the e-retail. For simplicity of presentation, only the classification of cyber attacks has been presented in this framework as attack profiles. 100% of companies agreed on this to be a challenge within organisations.
- *Mitigation strategies:* These are methods organisations conduct to mitigate against attack profiles. These methods were then validated against standard cybersecurity frameworks from a thorough literature review.

7.6 Recommendations

To improve the cybersecurity of organisations in South African some concerns and issues need attention. The recommendations focus on raising awareness of staff members, organisations and government on cybersecurity. It covers the importance of strategic planning, skills requirement and government involvement

7.6.1 Strategic planning

The challenges listed in section 7.3 have led to the state of cybersecurity in e-retail organisations in South Africa. The start of the solution should be within organisations to place cybersecurity as part of organisational goals and objectives. Cybersecurity initiatives and campaigns need to be part of the organisations policy structure. Strategic planning is advantageous because it aims at goals within a well-established framework by moulding the future of an organisation and its surroundings. The cybersecurity readiness of an organisation will depend on the plan of action adopted during its strategic planning.

Organisations require a strategic vision on the protection of critical infrastructure and other core business processes that operate within the cyberspace, as more business processes and function are heavily reliant on the internet and ICT.

7.6.2 Skills requirement

There are cyber attacks occurring on a daily basis. This calls for the need to develop a workforce with the requisite skill set to meet the demands of cybercrimes. Studies have long shown the need for developing a workforce with the required skills in the cybersecurity space. It is recommended that attention is given to building capacity in cybersecurity. The National Research Council Professionalization of Nations cybersecurity workforce report can be utilized by decision makers to develop a working strategy to establish a cybersecurity workforce at a national level.

Qualifications and certifications are important and have their place in shaping a cybersecurity workforce. However, a workforce equipped with appropriate knowledge, skillset and abilities to protect critical infrastructure and improve cyber-resilience is required. Recalling from the comments of participant 8, South Africa is very reliant on security products and tools to combat cyber risks and globally there is that trend of administering countermeasures to mitigate risks, but there needs to be a particular focus on people. Irrespective of how superb a security tool or technology may be, its effectiveness is limited if it is not embraced and executed properly by a workforce that follows a well-defined process.

7.6.3 Government involvement

The government has a role to play and is needed in the development of cybersecurity at a national level and areas of industry. Creating educational and awareness policies would encourage cybersecurity in public, private and industrial sectors. Not only at the professional level but also at grassroots level within schools, colleges and universities. The government can adopt various awareness methods to create a consciousness of the importance of cybersecurity. The government can also embark on incentive initiatives to encourage organisational cybersecurity efforts. The government can also provide financial support and expert guidance to SMME's.

For a more radical approach to encouraging cybersecurity practices, government can constructively launch a security program similar to the BEE act to empower SMME's to improve their cybersecurity. Government an also encourage collaborations amongst universities, research groups and the international community to embark on knowledge sharing and foster continued collaboration.

7.7 Research contributions

In this section, the theoretical and practical contributions this study has provided is discussed

7.7.1 Theoretical contribution

The study's theoretical contribution is to the cybersecurity literature with a particular interest in the e-retail sector. It includes practices used to improve the cybersecurity readiness of organisations. The findings resulted in the extension of the NIST (2014:19). In addition, through conceptualization and syntheses of other frameworks to propose a guideline to assist e-retail organisations in mitigating cyber attacks.

7.7.2 Practical contribution (a framework to guide e-retail organisations)

Knowledge was gained that organisations and the country stand to benefit from adopting good cybersecurity practices. Though not usually quantifiable, good cybersecurity practices could significantly reduce the cost incurred post occurrence.

Furthermore, the study could provide organisations, decision makers, and policymakers with information that on how to reduce cybercrimes. This study also assists organisations to evaluate their current practices in line with standardized frameworks. This study's conceptual model presented in (Figure 7.1) is a proposed guide for e-retail organisations to adopt and evaluate cybersecurity practices in e-retail in South Africa.

The study affirms and confirms the need for the prioritizing of cybersecurity readiness amongst organisations and the nation at large.

7.8 Research limitations

The population size of this investigation was limited to eight (8) organisations from different areas of operation as provided in (Table 4.1), ranging from small to multinational organisations. All but two of the organisations was from the Western Cape Province, South Africa and Gauteng Province. This makes constraints a generalization of this study. Nine (9) individuals or office bearers participated in the study.

This study focused on understanding South Africa's cybersecurity profile and exploring methods to mitigate cyber attacks.

7.9 Recommendation for further research

Bearing in mind some aforementioned limitations of this research, future research could broaden the discourse on this subject matter

i. Further research could focus on quantifying the benefits of cybersecurity practices within e-retail
ii. Research needs to be done on providing reasons for cyber attacks in e-retail in South Africa
iii. Research is required on the roles customer play in the e-retail cybersecurity ecosystem.
iv. Further research on identification and evaluation of cost-effective cybersecurity strategies for small e-retailers.

REFERENCES

Abawajy, J. 2014. User preference of cyber security awareness delivery methods. *Behaviour & Information Technology*, 33(3): 237–248.

Adamsky, F., Aubigny, M., Battisti, F., Carli, M., Cimorelli, F., Cruz, T., Di Giorgio, A., Foglietta, C., Galli, A., Giuseppi, A., Liberati, F., Neri, A., Panzieri, S., Pascucci, F., Proenca, J., Pucci, P., Rosa, L. & Soua, R. 2018. Integrated Protection of Industrial Control Systems from Cyber-attacks: the ATENA Approach. *International Journal of Critical Infrastructure Protection*, 21: 72–82.

Adeyeye, M. 2008. e-Commerce, Business Methods and Evaluation of Payment Methods in Nigeria. *Electronic Journal Information Systems Evaluation Volume*, 11(1): 1–6.

Aggarwal, P. 2014. Review on cyber crime and security. *International Journal of Research in Engineering and Applied Sciences*, 02(01): 48–51.

Ahmad, A., Maynard, S.B. & Park, S. 2014. Information security strategies: towards an organizational multi-strategy perspective. *Journal of Intelligent Manufacturing*, 25(2): 357–370. http://link.springer.com/10.1007/s10845-012-0683-0.

Akkas, A., Chachamis, C.N. & Fetahu, L. 2017. *Malware Analysis of WanaCry Ransomware*.

Al-Tarawneh, M., Al-Tarawneh, H. & Ma'aitah, M. 2012. The Effect of Computer Crimes on the Application of Information System in Banks in Jordanian Firms. *European Journal of Business Management*, 4(19): 37–49.

Alexander, B. & Mason, R. 2017. The South African e-Retail change Agenda: A curriculum development perspective. *Electronic Journal of Information Systems in Developing Countries*, 82(1): 1–21.

Alexander, B., van Vuuren, J., Hermanus, T., Dassah, R. & Mason, R.. 2016. *E-Retail in South Africa and the Impact on Skills Development in the South African Retail Sector*. http://wrlc.org.za/wp-content/uploads/2017/01/2015_13-e-Retail-in-SA-161020.pdf.

Alhaqbani, B. & Fidge, C. 2008. Access Control Requirements for Processing Electronic Health Records. In *Proceedings Business Process Management 2007 Workshops: First International Workshop on Process-Oriented Information Systems in Healthcare*. 371–382. http://link.springer.com/chapter/10.1007/978-3-540-78238-4_38.

Alshaikh, M., Maynard, S.B., Ahmad, A. & Chang, S. 2018. An Exploratory Study of Current Information Security Training and Awareness Practices in Organizations. In *51st Hawaii International Conference on System Sciences*. 5085–5094.

Alshboul, Y. & Streff, K. 2015. Analyzing Information Security Model for Small-Medium Sized Businesses. In *Twenty-first Americas Conference on Information Systems*. 1–9.

Amaratunga, D., Baldry, D., Sarshar, M. & Newton, R. 2002. Quantitative and qualitative research in the built environment: application of "mixed" research approach. *Work Study*, 51(1): 17–31. http://www.emeraldinsight.com/doi/10.1108/00438020210415488.

Anderson, R., Barton, C., Bhöme, R., Clayton, R., Van Eeten, M., Levi, M., Moore, T. & Savage, S. 2013. Measuring the Cost of Cybercrime. In *Workshop on the Economics of Information Security (WEIS)*. 1–31.

http://scholar.google.ca/scholar?q=anderson+%60cost+of+cybercrime%60&btnG=&hl=en&as_sdt=0,5#2.

Anderson, R., Barton, C., Bohme, R., Clayton, R., Van Eeten, M., Levi, M. & Moore, T. 2013. Measuring the Cost of Cybercrime. In *The Economics of Information Security and Privacy*. Springer: 265–300. https://link.springer.com/chapter/10.1007/978-3-642-39498-0_12.

Ankita & Lavisha. 2012. Odyssey Of Data Security With A New Perception 1. *International Journal of Computer Science Issues*, 9(3): 303–311.

Ardalan, K. 2008. The philosophical foundation of the lecture-versus-case controversy. *International Journal of Social Economics*, 35(1/2): 15–34. http://www.emeraldinsight.com/doi/abs/10.1108/03068290810843819.

B, H. De & Little, M.W. 2001. *Regulatory Issues for Global E-Tailers : Marketing Implications*.

Babbie, E. 2016. *The basics of social research*. 7th ed. Wadsworth: Cengage Learning. 9781305503076.

Banday, M.T. & Mir, F.A. 2012. A study of Indian approach towards cyber security. In *Proceedings on 2012 1st International Conference on Emerging Technology Trends in Electronics, Communication and Networking, ET2ECN 2012*. 1–6.

Barrel, N. 2015. Systems and methods for defending against cyber attacks at the software level. : 7. https://patents.google.com/patent/US20150121532A1/en.

Baxter, P. & Jack, S. 2008. Qualitative Case Study Methodology: Study Design and Implementation for Novice Researchers. *The Qualitative Report 544-The Qualitative Report Volume 13 Number 4 December 2008*, 13(4): 544–559.

Benbasat, I., Goldstein, D.K. & Mead, M. 1987. The Case Research Strategy in Studies of Information Systems. *MIS Quarterly*, 11(3): 369–386. https://www.jstor.org/stable/248684?seq=1#page_scan_tab_contents.

Berg, B.L. 2001. *Qualitative Research Methods for the Social Sciences*. 4th ed. Boston: Allyn and Bacon.

Bessette, D., LeClair, J., Sylvertooth, R. & Burton, S. 2015. Communication, Technology, and Cyber Crime in Sub-Saharan Africa. In D. Maurice, ed. *New Threats and Countermeasures in Digital and Cyber Terrorism*. IGI Global.

Bhattacharya, D. 2015. Evolution of Cybersecurity Issues In Small Businesses. In *ACM Conference: Research in Information Technology*. New york: 11.

Bhattacherjee, A. 2012a. *Social Science Research: principles, methods, and practices*.

Bhattacherjee, A. 2012b. *Social Science Research: Principles, Methods, and Practices*. 2nd ed.

Bhisikar, A. 2011. G-Cloud : New Paradigm Shift for Online Public Services IaaS PaaS SaaS. *International Journal of Computer Application*, 22(8): 24–29.

Biggio, B. & Roli, F. 2017. Wild Patterns: Ten Years After the Rise of Adversarial Machine Learning. *Computer Vision and Pattern Recognition*: 32–37.

Björck, F., Henkel, M., Stirna, J. & Zdravkovic, J. 2015. Cyber Resilience – Fundamentals for a Definition. In *International Cyber Resilience Conference*. 311–316. http://link.springer.com/10.1007/978-3-319-16486-1_31.

Bowen, G.A. 2009. Document analysis as a qualitative research method. *Qualtative Research Journal*, 9(2): 27–40. http://dx.doi.org/10.3316/QRJ0902027%5Cnhttp://%5Cnhttp://dx.doi.org/10.3316/QRJ0902018.

Bradley, N. 1999. Sampling for Internet surveys. An examination of respondent selection for Internet research. *Journal of the Market Research Society*, 41(4): 387.

Bratt, M. 2018. Online shopping growing in popularity in SA, but lags global pace. *The media online*. https://themediaonline.co.za/2018/01/48086/.

Bremler-Barr, A. & Levy, H. 2005. Spoofing prevention method. In *Proceedings IEEE 24th Annual Joint Conference of the IEEE Computer and Communications Societies.* IEEE: 536–547. http://ieeexplore.ieee.org/document/1497921/.

Brooks, F. 2017. *Why cyber incident response planning is a critical enterprise capability*.

Bryman, A. 2015. *Social research methods*. 5th ed. Oxford University press.

Budd, R.W., Thorp, R.K. and Donohew, L. 1967. Content analysis of communications.

Buhalis, D. 2016. *eCommerce*. J. Jafari & H. Xiao, eds. Springer International Publishing.

Burke, M.E. 2007. Making choices: research paradigms and information management. *Library Review*, 56(6): 476–484.

Burmeister, O., Phahlamohlaka, J. & Al-saggaf, Y. 2014. *National security governance exemplified by South Africa’s cyber security policy implementation*.

Burrell, G. & Morgan, G. 1979. *Sociological Paradigms and organisational Analysis - Elements of the Sociology of Corporate Life*. Ashgate Publishing Limted.

Burton, A., Kwak, J. & Haley, W. 2004. Elder caregiving. *Encyclopedia of Applied Psychology*: 724.

Byron, Lord & Green, H.S. 2007. *Electronic Commerce and Security*. Prentice Hall Press.

Chaffey, D. 2015. *Digital Business and E-Commerce Management*. Pearson Education Limited. www.pearson-books.com.

Chaisiri, S. & Ko, R.K.L. 2016. From Reactionary to Proactive Security: Context-Aware Security Policy Management and Optimization under Uncertainty. In *2016 IEEE Trustcom/BigDataSE/ISPA*. IEEE: 535–543.

Chora, M., Kozik, R., Renk, R. & Houbowicz, W. 2015. A practical framework and guidelines to enhance cyber security and privacy. In *Advances in Intelligent Systems and Computing*. Springer International Publishing Switzerland: 485–495. http://link.springer.com/10.1007/978-3-319-19713-5_42.

Chorney, R. 2016. *Payment Card Industry Data Security Standards Table of Contents*. Winnipeg. http://umanitoba.ca/admin/financial_services/media/PCI_DSS_Compliance_FinalNov_01_-_PDF.pdf.

Cichonski, P., Millar, T., Grance, T. & Scarfone, K. 2012. *Computer Security Incident Handling Guide : Recommendations of the National Institute of Standards and Technology*. Gaithersburg, MD. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-

61r2.pdf.

Clarke, R. 1999. Key Issues in Electronic Commerce and Electronic Publishing. http://www.rogerclarke.com/EC/Issues98.html#EC.

Coffey, A. and Atkinson, P. 1996. *Making sense of qualitative data: Complementary research strategies*. Sage Publications, Inc.

Committee of Experts on Crime in Cyber-Space (PC-CY). 2001. *Explanatory report of the Convention on Cybercrime*. https://rm.coe.int/16804d873c.

Coppel, J. 2000. *E-Commerce: Impacts and Policy Challenges*.

Craigen, D., Diakun-Thibault, N. & Purse, R. 2014. *Defining cyber-security*.

CREATe. 2016. *CYBER RISK : Navigating the Rising Tide of Cybersecurity Regulation*.

de Crespigny, M. 2012. Building cyber-resilience to tackle threats. *Network Security*, 2012(4): 5–8. http://linkinghub.elsevier.com/retrieve/pii/S1353485812700247.

Creswell, J.W., Hanson, W.E., Clark Plano, V.L. and Morales, A. 2007. Qualitative research designs: Selection and implementation. *The counseling psychologist*, 35(2): 236–264.

Creswell, J.W. 2013. *Research Design: Qualitative, Quantitative and Mixed Method Aproaches*. 3rd, ed. SAGE Publications. http://libproxy.unm.edu/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=a9h&AN=51827937&site=eds-live&scope=site%5Cnhttp://content.ebscohost.com.libproxy.unm.edu/ContentServer.asp?T=P&P=AN&K=51827937&S=R&D=a9h&EbscoContent=dGJyMNLr40SeprI4.

Creswell, J.W. Research design.

Creswell, J.W. 2003. Research design Qualitative quantitative and mixed methods approaches. *Research design Qualitative quantitative and mixed methods approaches*: 3–26.

Creswell, J.W. & Poth, C.N. 2017. *Qualitative Inquiry and Research Design: Choosing Among Five Approaches*. 4th ed. SAGE Publications.

Cross, C. & Kelly, M. 2016. The problem of "white noise": examining current prevention approaches to online fraud. *Journal of Financial Crime*, 23(4): 806–818. http://www.emeraldinsight.com/doi/10.1108/JFC-12-2015-0069.

Daas, P. 2012. Secondary data collection. , (201206): 1–42.

Dan, C. 2014. Electronic Commerce : State-of-the-Art. *American Journal of Intelligent Systems*, 4(4): 135–141.

Darke, P., Shanks, G. & Broadbent, M. 1998. Successfully completing case study research: combining rigour, relevance and pragmatism. *Information Systems Journal*, 8(4): 273–289. http://doi.wiley.com/10.1046/j.1365-2575.1998.00040.x.

Darville, C. 2017. *Cyber Security Incident Management Guide*.

Dash, S.B., Saini, H., Panda, T.C. & Mishra, a. 2014. Service Level Agreement Assurance in Cloud Computing : A Trust Issue. *International Journal of Computer Science and Information Technologies*, 5(3): 2899–2906.

Dashora, K. & Patel, P.P. 2011. Cyber Crime in the Society: Problems and Preventions. *Journal* *of Alternative Perspectives in the Social Sciences*, 3(1): 240–259.

Deloitte. 2015. *Cyber risk in retail Protecting the retail business to secure tomorrow's growth*. https://www2.deloitte.com/content/dam/Deloitte/cl/Documents/risk/cl-ers-retail-cyber-risk-report.pdf.

Dennis, C., Fenech, T., Pantano, E., Gerlach, S. & Merrilees, B. 2004. *E-Retailing*. Routledge.

Department of Government Communication and Information System. 2016. *South Africa Offficial Yearbook 2016*. E. Tibane & N. Lentsoane, eds. http://www.gcis.gov.za/sites/www.gcis.gov.za/files/docs/resourcecentre/yearbook/SAYB1516.pdf.

Department of Justice. 2015. *Cyber Crime and Cybersecurity Bill*.

Department of Justice and Constitutional Development. 2016. South African Banking Risk Inforamtion Centre (SABRIC).

Donaldson, S.E., Siegel, S.G., Williams, C.K. & Aslam, A. 2015. Enterprise Cybersecurity Capabilities. In *Enterprise Cybersecurity*. Berkeley, CA: Apress: 311–334.

Douligeris, C. & Mitrokotsa, A. 2003. DDoS attacks and defense mechanisms: a classification. In *Proceedings of the 3rd IEEE International Symposium on Signal Processing and Information Technology (IEEE Cat. No.03EX795)*. IEEE: 190–193. http://ieeexplore.ieee.org/document/1341092/.

Drolet, M. 2017. Learn What NIST's Cybersecurity Framework Can Do For You. *Infosec at your service*.

Dubois, A. & Gadde, L.E. 2002. Systematic combining: An abductive approach to case research. *Journal of Business Research*, 55(7): 553–560.

Durham, L. 2011. Opportunities and challenges for South African retailers. *Supermarket & Retailer*, (May): 33–35.

e Silva, K.K. 2017. How industry can help us fight against botnets: notes on regulating private-sector intervention. *International Review of Law, Computers & Technology*, 31(1): 105–130. https://www.tandfonline.com/doi/full/10.1080/13600869.2017.1275274.

Eisenhardt, K.M. 1989. Building Theories from Case Study Research. *The Academy of Management Review*, 14(4): 532. http://www.jstor.org/stable/258557?origin=crossref.

Elbeltagi, I. & Agag, G. 2016. E-retailing ethics and its impact on customer satisfaction and repurchase intention. *Internet Research*, 26(1): 288–310. http://www.emeraldinsight.com/doi/10.1108/IntR-10-2014-0244.

Elo, S., Kääriäinen, M., Kanste, O., Polkki, T., Utriainen, K. & Kyngas, H. 2014. Qualitative Content Analysis: A Focus on Trustworthiness. *SAGE Open*, 4(1): 1–10. http://sgo.sagepub.com/lookup/doi/10.1177/2158244014522633.

Emhemed, E. & Pandey, R.. 2017. A Study of Computer Application in Resource Management and Developing a Model Network Adoption in Construction Projects. *International Journal of Scientific Engineering and Technology Research*, 06(08): 1670–1675.

ENISA. 2017. *European union cybersecurity initiatives*.

Entrust Datacard. 2012. *What is the European Union Agency for Network and Information*

Security ENISA.

Fan, W., Lwakatare, K. & Rong, R. 2017. Social Engineering: I-E based Model of Human Weakness for Attack and Defense Investigations. *International Journal of Computer Network and Information Security*, 9(1): 1–11. http://www.mecs-press.org/ijcnis/ijcnis-v9-n1/v9n1-1.html.

Fernie, J., Fernie, S. & Moore, C. 2013. *Principles of Retailing*.

Ferraiolo, D.F., Sandhu, R., Gavrila, S., Kuhn, D.R. & Chandramouli, R. 2001. Proposed NIST standard for role-based access control. *ACM Transactions on Information and System Security*, 4(3): 224–274. http://www.sciencedirect.com/science/article/pii/S0065245808602065.

Ford, M., Herselmanm, M. & Botha, A. 2014. Building an Mlearning Research Framework through Design Science Research. In *13th World Conference on Mobile and Contextual Learning*. Springer: 109.

Friese, S. 2011. *User's Manual for ATLAS. ti 6.0*. Berlin: ATLAS. ti Scientific Software Development GmbH.

Friese, S. 2011. Using ATLAS. ti for analyzing the financial crisis data. In Forum Qualitative Sozialforschung/Forum. *Qualitative Social Research*, 12(1).

Frost & Sullivan. 2015. *The Global B2B E-commerce Market Will Reach 6.7 Trillion USD by 2020*. https://ww2.frost.com/news/press-releases/global-b2b-e-commerce-market-will-reach-67-trillion-usd-2020-finds-frost-sullivan/.

Ganorkar, S.S. & Kandasamy, K. 2017. Understanding and defending crypto-ransomware. *ARPN Journal of Engineering and Applied Sciences*, 12(12): 3920–3925.

Garae, J. & Ko, R.K.L. 2017. Visualization and Data Provenance Trends in Decision Support for Cybersecurity. In *Data Analytics and Decision Support for Cybersecurity*. 243–270. http://link.springer.com/10.1007/978-3-319-59439-2.

Gernon, D. 2017. Online retailing in SA has plenty of room for growth. *Businesslive*. https://www.businesslive.co.za/bd/companies/retail-and-consumer/2017-05-09-online-retailing-in-sa-has-plenty-of-room-for-growth/.

Ghazvini, Arash and Shukur, Z. 2016. Awareness Training Transfer and Information Security Content Development for Healthcare Industry. *International Journal of Advanced Computer Science and Applications*, 7(5): 361–370.

Ghernaouti, S. 2013. *Cyber Power: Crime, conflict and security in cyberspace*. EPFL Press.

Ghernouti-Hélie, S. 2010. A National Strategy for an Effective Cybersecurity Approach and Culture. In *2010 International Conference on Availability, Reliability and Security*. IEEE: 370–373. http://ieeexplore.ieee.org/document/5438067/.

Gikas, C. 2010. A General Comparison of FISMA, HIPAA, ISO 27000 and PCI-DSS Standards. *Information Security Journal: A Global Perspective*, 19(3): 132–141.

Goldstuk, A. 2016. SA online retail to pass 1% of total. *World wide worx*. http://www.worldwideworx.com/retail2016/.

Gondim, S.M.G. & Bendassolli, P.F. 2014. The use of the qualitative content analysis in psychology: a critical review. *Psicologia em Estudo*, 19(2): 191–199.

http://www.scielo.br/scielo.php?script=sci_arttext&pid=S1413-73722014000200003&lng=pt&nrm=iso&tlng=en.

Gonzalez, M.D. 2015. International Perspectives of Cyber Warfare. *International Journal of Cyber Warfare and Terrorism*, 5(4): 59–68.

Goodman, S. 2008. Critical infrastructure protection. In *Reponses to Cyber Terrorism*. 24–33.

Gorichanaz, T. & Latham, K.F. 2016. Document phenomenology: a framework for holistic analysis. *Journal of Documentation*, 72(6): 1114–1133. http://www.emeraldinsight.com/doi/10.1108/JD-01-2016-0007.

Government Gazette. 2002. *Electronic Communication and Transactions Act*.

Graneheim, U.H. & Lundman, B. 2004. Qualitative content analysis in nursing research: Concepts, procedures and measures to achieve trustworthiness. *Nurse Education Today*, 24(2): 105–112.

Grbich, C. 2013. *Qualitative Data Analysis: An Introduction*. SAGE Publications.

Gubbi, J., Buyya, R., Marusic, S. & Palaniswami, M. 2013. Internet of Things (IoT): A vision, architectural elements, and future directions. *Future Generation Computer Systems*, 29(7): 1645–1660.

Gulia, P. & Sood, S. 2013. Automatic Selection and Ranking of Cloud Providers using Service Level Agreements. *International Journal of Computer Applications*, 72(11): 45–52.

Gustafsson, J. 2017. *Single case studies vs. multiple case studies: A comparative study*. http://www.diva-portal.org/smash/get/diva2:1064378/FULLTEXT01.pdf.

Hakim, S., Albert, G. & Shiftan, Y. 2016. Pipeline Security. In *Securing Transportation Systems*. John Wiley & Sons: 296.

Henderson, K. 1999. Electronic Commerce in the On-line and Electronic Publishing Industry : a Business Model for Web Publishing. *Proceedings from the Conference 'Electronic Publishing 99: redefining the information chain - new ways and voices*: 37–50.

Hox, J.J. & Boeije, H.R. 2005. Data Collection, Primary vs. Secondary. *Encyclopedia of Social Measurement*: 593–599. http://linkinghub.elsevier.com/retrieve/pii/B0123693985000414.

Hsieh, H.F. & Shannon, S.E. 2005. Three Approaches to Qualitative Content Analysis. *Qualitative Health Research*, 15(9): 1277–1288. http://www.ncbi.nlm.nih.gov/pubmed/16204405%5Cnhttp://qhr.sagepub.com/cgi/doi/10.1177/1049732305276687.

Iglesias-Pradas, S., Pascual-Miguel, F., Hernández-García, Á. & Chaparro-Peláez, J. 2013. Barriers and drivers for non-shoppers in B2C e-commerce: A latent class exploratory analysis. *Computers in Human Behavior*, 29(2): 314–322. http://dx.doi.org/10.1016/j.chb.2012.01.024.

Information Systems Audit and Control Association. 2015. CoBIT. *Icasa*: 5. http://www.isaca.org/Knowledge-Center/COBIT/Pages/Overview.aspx%5Cnwww.isaca.org/Knowledge-Center/cobit/Documents/CobiT-Products.pdf.

Information Systems Audit and Control Association. 2014. Deliver, Service and Support. *ISACA*. https://www.isaca.org/popup/Pages/DeliverandSupport.aspx 4 April 2018.

Irvine, C.E., Thompson, M.F. & Allen, K. 2005. CyberCIEGE: Gaming for Information Assurance. *IEEE Security and Privacy Magazine*, 3(3): 61–64. http://ieeexplore.ieee.org/document/1439504/.

Jansen van Vuuren, J., Leenen, L., Phahlamohlaka, J. & Jannie, Z. 2013. Development of a South African Cybersecurity Policy Implementation Framework. *Proceedings of the 8th International Conference on Information Warfare and Security*. https://scholar.google.co.za/citations?view_op=view_citation&hl=en&user=rG7tDNEAAAAJ&sortby=pubdate&citation_for_view=rG7tDNEAAAAJ:ULOm3_A8WrAC.

Jensen, C.D., Meira, F. & Nittegaard-Nielsen, J. 2007. Resilia: a Safe and Secure Distributed Backup System for Small and Medium Enterprises. In *Trust Management*. Boston, MA: Springer US: 383–398. http://dblp.uni-trier.de/db/conf/ifiptm/ifiptm2007.html#JensenMN07.

Johnson, C., Badger, L. & Waltermire, D. 2014. *NIST Special Publication 800-150 (Draft) Guide to Cyber Threat Information Sharing*. http://csrc.nist.gov/publications/PubsSPs.html.

Jones, G. 2004. *Operational Security Requirements for Large Internet Service Provider (ISP) IP Network Infrastructure*. G. Jones, ed. https://www.rfc-editor.org/info/rfc3871.

Jukic, N., Jukic, B., Meamber, L. & Nezlek, G. 2002. Improving e-business customer relationship management systems with multilevel secure data models. In *Proceedings of the 35th Annual Hawaii International Conference on System Sciences*. IEEE Comput. Soc: 2256–2265. http://ieeexplore.ieee.org/document/994156/.

Kamisli, Z. & Alegoz, M. 2017. E-Retailing from Past to Future: Definitions, Analysis, Problems, and Perspectives. In *Handbook of Research on Intelligent Techniques and Modeling Applications in Marketing Analytics*. 14. http://www.igi-global.com/chapter/e-retailing-from-past-to-future/170351.

Kaplan, S. & Sawhney, M. 2000. E-hubs: the new B2B (business-to-business) marketplaces. *Harvard business Review*: 97–103, 214.

Karig, D. & Lee, R. 2001. *Remote Denial of Service Attacks and Countermeasures*. http://www.princeton.edu/~rblee/ELE572Papers/karig01DoS.pdf.

Katata, F.B., Kadhi, N. El & Ghedira, K. 2009. Distributed Agent Architecture for Intrusion Detection Based on New Metrics. In *Third International Conference on Network and System Security*. IEEE: 321–327. http://ieeexplore.ieee.org/document/5319064/.

Kelle, U. 2004. Computer-assisted qualitative data analysis. *Qualitative research practice*: 473–489.

Kigen, P., Kisutsa, C., Muchai, C., Kimani, K., Mwangi, M. & Shiyayo, B. 2014. *Kenya Cyber Security Report 2014 Rethinking Cyber Security - "An Integrated Approach: Processes, Intelligence and Monitoring*.

Kiggins, R.D. 2014. US Leadership in Cyberspace: Transnational Cyber Security and Global Governance. In *Cyberspace and International Relations*. Berlin, Heidelberg: Springer Berlin Heidelberg: 161–180.

Kilani, M. Al & Kobziev, V. 2016. An Overview of Research Methodology in Information System (IS). *Open Acess Library Journal*, 03(11): 1–9. http://www.oalib.com/paper/pdf/5275653.

Kim, D., Ferrin, D. & Rao, R. 2009. Trust and Satisfaction, Two Stepping Stones for Successful E-Commerce Relationships: A Longitudinal Exploration. *Journal of Information Systems*

Research, 20(2): 237–257.

Kissel, R. 2013. Glossary of Key Information Security Terms Glossary of Key Information Security Terms. *NIST*, NISTIR 729(Revision 2).

Kitzinger, J. 1995. Qualitative research. Introducing focus groups. *British Medical Journal*, 311(7000): 299–302.

Koopman, M. 2017. *Preventing Ransomware on the Internet of Things*.

Korff, D. 2015. *Cyber Security Definitions – a selection (US) National Initiative for Cybersecurity Education (NICE):*

Kpmg. 2000. *E-COMMERCE AND CYBER CRIME: New Strategies for Managing the Risks of Exploitation*.

Kraemer-Mbula, E., Tang, P. & Rush, H. 2013. The cybercrime ecosystem: Online innovation in the shadows? *Technological Forecasting and Social Change*, 80(3): 541–555. http://dx.doi.org/10.1016/j.techfore.2012.07.002.

Kumar, N. 1996. The Power of Trust in Manufacturer-Retailer Relationships. *Harvard business review*, 74(6): 92–106.

Kumar, S. & Bharati, N. 2016. Cyber Security: Issue and Challenges in E-Commerce Santosh Kumar Maurya NagendraPratap Bharati UGC- NET / JRF Research Scholar , Department of Management Studies , Nehru. *Indian Journal of Research*, 5(1): 191–193.

Kumari, B., Jalees, Y. & Gupta, M. 2016. Cyber Security as a Backbone of E-Commerce. *International Journal of Advanced Scientific Research and Management*, 1(4): 2–5.

Lathrop, S.D., Trent, S. & Hoffman, R. 2016. Applying Human Factors Research Towards Cyberspace Operations: A Practitioner's Perspective. In 281–293. http://link.springer.com/10.1007/978-3-319-41932-9_23.

Laudon, K. & Laudon, J. 2012. *Management Information Systems: Managing the digital firm*. 12th ed. Pearson Education.

Laudon, K.C. & Laudon, J.P. 2016. *Management Information Systems: Managing the Digital Firm*.

LeBlanc, G. 2018. System and method for assuring commercial regulatory compliance. , (19).

Leszczyna, R. 2018. Cybersecurity and privacy in standards for smart grids – A comprehensive survey. *Computer Standards and Interfaces*, 56(July 2017): 62–73. https://doi.org/10.1016/j.csi.2017.09.005.

Levi-Faur, D. 2011. Regulatory networks and regulatory agencification: towards a Single European Regulatory Space. *Journal of Journal of European Public Policy*, 18(6): 810–829.

Lewis, S. 2015. Qualitative Inquiry and Research Design: Choosing Among Five Approaches. *Sage Journals*, 6(4): 473–475.

Liao, Z. & Cheung, M.T. 2003. Challenges to Internet e-banking. *Communications of the ACM*, 46(12): 248. http://portal.acm.org/citation.cfm?doid=953460.953507.

Lindkvist, K. 1981. Approaches to textual analysis. *Advances in content analysis*, 9: 23–42.

Liu, J., Xiao, Y., Chen, H., Ozdemir, S., Dodle, S. & Singh, V. 2010. *Payment Card Industry*

Data Security Standard. https://www.pcisecuritystandards.org/documents/pci_dss_v2.pdf.

Lu, C.J. and Shulman, S.W. 2008. Rigor and flexibility in computer-based qualitative research: Introducing the Coding Analysis Toolkit. *International Journal of Multiple Research Approaches*, 2(1): 105–117.

Lupu, S., Mual, M. & Stipout, M. van. 2016. *Ecommerce Payment Methods Report 2016*. https://www.febelfin.be/sites/default/files/InDepth/ecommerce_payment_methods_report_2016_aeu_global_payments_insights.pdf.

Maciá-Fernández, G., Díaz-Verdejo, J.E. & García-Teodoro, P. 2007. Evaluation of a low-rate DoS attack against iterative servers. *Computer Networks*, 51(4): 1013–1030. http://linkinghub.elsevier.com/retrieve/pii/S1389128606001666.

Mack, N., Woodsong, C., MacQueen, K.M., Guest, G. and Namey, E. 2005. Qualitative research methods: a data collectors field guide.

Majid, N., Ahmad, R.R., Din, U.K.S., Rambely, A.S., Suradi, N.R.M. & Shahabudin, F.A.A. 2012. Academic Research Process: A Review on Current Practices in School of Mathematical Sciences. *Procedia - Social and Behavioral Sciences*, 59(0): 394–398. http://www.sciencedirect.com/science/article/pii/S1877042812037408.

Marshall, M.N. 1996. Sampling for qualitative research Sample size. *Family Practice*, 13(6): 522–525.

Mastercard. 2014. *Online Shopping Security in the Spotlight – MasterCard Survey*. https://webcache.googleusercontent.com/search?q=cache:5tBNx37WUc8J:https://newsroom.mastercard.com/mea/press-releases/online-shopping-security-in-the-spotlight-mastercard-survey/+&cd=3&hl=en&ct=clnk&gl=za.

Mayring, P. 2014. *Qualitative content analysis: theoretical foundation, basic procedures and software solution*. Klagenfurt. https://www.ssoar.info/ssoar/handle/document/39517.

Mcintyre, A. 2018. Developing a Cybersecurity Protocol for Your Operational Environment. *Natural gas & electricity*, 34(April): 23–27.

McTavish, D.G. and Pirro, E.B. 1990. Contextual content analysis. *Quality & Quantity,*, 24(3): 245–265.

Meng, B. & Zhang, H. 2005. An electronic commerce system prototype and its implementations. In *Proceedings - Fifth International Conference on Computer and Information Technology, CIT 2005*. 966–970.

Menter, I., Elliot, D., Hulme, M., Lewin, J. and Lowden, K. 2011. *A guide to practitioner research in education*. London: Sage.

Miles, M.B. and Huberman, A.. 1994. *Qualitative data analysis: An expanded sourcebook*. Sage.

Miller, R. 1967. Task Taxonomy: Science or Technology? *Journal Ergonomics*, 10(2): 167–176.

Mirescu, S.V. & Maiorescu, T. 2010. The Premises and the Evolution of Electronic Commerce. *Journal of Knowledge Management, Economics and Information Technology*, 1(1): 44–56.

Mitrakas, A. 2007. Information security and law in Europe: Risks checked? Andreas Mitrakas. *Journal of Information & Communications Technology Law*, 15(1): 33–53.

Mlelwa, K.L. & Yonah, Z.O. 2017. Requirement ' s for Proposed Frameworks for Secure Ecommerce Transactions. *Communications on Applied Electronics*, 6(9): 1–15.

Modi, S.N. 2016. Role of Trustmark in E-commerce. *International Journal for Innovations in Engineering, Management and Technology*, 1(1): 35–40.

Mohanraj, M. & Sakthivel, M. 2016. *Customer Perception about Online Shopping*. 1st ed. EduPedia Publications. https://books.google.co.za/books?id=zubJDAAAQBAJ&dq=Mohanraj+%26+Sakthivel,+2016&source=gbs_navlinks_s.

Mohideen, F. 2016. The Cyber-Security State of our Nation: A Critique of South Africa's Stance on Cyber-Security in Respect of the Protection of Critical Information Infrastructure. In T. Zlateva & V. Greiman, eds. *11th International Conference on Cyber Warfare and Security: ICCWS2016*. Academic Conferences Limited.

Morse, E.A. & Raval, V. 2008. PCI DSS: Payment card industry data security standards in context. *Computer Law & Security Review*, 24(6): 540–554. http://dx.doi.org/10.1016/j.clsr.2008.07.001.

Myalapalli, V.K. 2014. An Appraisal to Overhaul Database Security Configurations. *International Journal of Scientific and Research Publications*, 4(3): 1–4.

Mybroadband. 2015. South African e-commerce revolution expected. https://mybroadband.co.za/news/business/122206-south-african-e-commerce-revolution-expected.html.

Nandy, P. 2010. Online fraud prevention using genetic algorithm solution. , 1(12): 1–4. file:///C:/Users/MiNusZerO/Downloads/US7657497.pdf.

Narayanan, H.A.J. & Gunes, M.H. 2011. Ensuring access control in cloud provisioned healthcare systems. In *2011 IEEE Consumer Communications and Networking Conference (CCNC)*. IEEE: 247–251. http://ieeexplore.ieee.org/document/5766466/.

Neuman, W.L. 2011. *SRM: Qualitative and Quantitative Approaches*. 7th ed. D. Musslewhite & Macey L, eds. Boston: Pearson Education.

Newbould, R. & Collingridge, R. 2003. Profiling — technology. *BT Technology*, 21(1): 44–55.

Nguyen, T., Haller, D. & Kramer, G. 2000. System, Method and Article of manufacture for a gateway payment architecture utilizing a multichannel, extensible, flexible architecture.

NIST. 2014. Framework for Improving Critical Infrastructure Cybersecurity. *National Institute of S*: 1–41. papers2://publication/uuid/DD40979D-D391-4678-9601-F14CF1CB8BF5.

Nycz, M., Martin, M.J. & Polkowski, Z. 2015. The cyber security in SMEs in Poland and Tanzania. In *7th International Conference on Electronics, Computers and Artificial Intelligence (ECAI)*. IEEE: AE-27-AE-34. http://ieeexplore.ieee.org/document/7301182/.

O'Leary, Z. 2007. *The social science jargon buster: the key terms you need to know*. SAGE.

Oakes, K. 2018. *DOES YOUR BUSINESS HAVE A CYBER INCIDENT RESPONSE PLAN?* https://newagencypartners.com/blog/does-your-business-have-a-cyber-incident-response-plan/.

Olsen, R.F. & Ellram, L.M. 1997. A portfolio approach to supplier relationships. *Industrial Marketing Management*, 26(2): 101–113.

http://linkinghub.elsevier.com/retrieve/pii/S0019850196000892.

Olson, M. 2010. *Encyclopedia of Case Study Research*. SAGE Publications.

Parahoo, K. 2014. *Nursing Research: Principles, Process and Issues*. Palgrave Macmillan.

Park, J., Cho, D., Kyu, J. & Lee Byungtae. 2017. *Economics of Cybercrime: The Role of Broadband and Socioeconomic Status*.

Parodi, F. 2013. The Concept of Cybercrime and Online Threats Analysis. *International Journal of information security*, 2: 59.

Passman, P. 2016. Cybersecurity regulation: 5 things multinational businesses need to know. *InsideCounsel Magazine*. http://www.insidecounsel.com/2016/06/22/cybersecurity-regulation-5-things-multinational-bu.

Patcha, A. & Park, J.M. 2007. An overview of anomaly detection techniques: Existing solutions and latest technological trends. *Computer Networks*, 51(12): 3448–3470.

Patil, B. & Perkins, C. 2005. Method and system for securing mobile IPv6 home address option using ingress filtering. https://patents.google.com/patent/US6973086B2/en.

Patton, M.Q. 2002. Two decades of developments in qualitative inquiry: A personal, experiential perspective. *Qualitative social work*, 1(3): 261–283.

PCI-DSS. 2016. *Requirements and Security Assessment Procedures*.

PCIDSS. 2017. *Information Supplement: Best Practices for Securing E-commerce*.

Perakslis, E.D. & Stanley, M. 2016. A Cybersecurity Primer for Translational Research. *Science translational medicine*, 8(322): 2–322.

Phillips, L., Ripley, D., Johnson, S. & Reed, J. 2004. *E-Commerce*. Clear Glass Press.

Piskozub, A. 2004. Denial of service and distributed denial of service attacks. In *Modern Problems of Radio Engineering, Telecommunications and Computer Science (IEEE Cat. No.02EX542)*. Lviv Polytech. Nat. Univ: 303–304. http://ieeexplore.ieee.org/document/1015977/.

Pope, C. & Mays, N. 1995. Reaching the parts other methods cannot reach: an introduction to qualitative methods in health and health services research. *British medical journal*, 311(6996): 42–45.

Popoola, S., Iyekekepolo, U., Ojewande, S., Sweetwilliams, F., John, S. & Atayero, A. 2017. Ransomware: Current Trend, Challenges, and Research Directions. In *Proceedings of the World Congress on Engineering and Computer Science*. San Francisco: 1–4.

PriceWaterhouseCoopers. 2015a. *Managing cyber risks in an interconnected world*. www.pwc.com/gsiss2015.

PriceWaterhouseCoopers. 2015b. *US cybersecurity: progress stalled*. https://www.ncjrs.gov/App/Publications/abstract.aspx?ID=269621.

PriceWatersHousecoopers. 2014. *Why you should adopt the NIST CYbersecurity Framework*. pwc.com/cybersecurity.

Pritchett. 2017. The Importance of Cyber Incident Response Plans and How to Create Them. *Elon Business law Journal*. http://blogs.elon.edu/blj/2017/06/30/the-importance-of-cyber-incident-response-plans-and-how-to-create-them/.

Raderman, L. 2015. *Computer Security Incident Response Plan*. https://www.cmu.edu/iso/governance/procedures/docs/incidentresponseplan1.0.pdf.

Raghavan, K., Desai, M.S. & Rajkumar, P. V. 2017. Managing Cybersecurity and e-Commerce Risks in Small Busi- nesses. *Journal of Management Science and Business Intelligence*, 9264(May): 2–1.

Reddy, T., Wing, D. & Patil, P. 2017. Short Term Certificate Management During Distributed Denial of ServiceAttacks. https://patents.google.com/patent/US20170331854A1/en.

Rege, A., Obradovic, Z., Asadi, N., Parker, E., Pandit, R., Masceri, N. & Singer, B. 2018. Predicting Adversarial Cyber Intrusion Stages Using Autoregressive Neural Networks. *IEEE Intelligent Systems*, PP(99): 5–7. http://ieeexplore.ieee.org/document/8255778/.

Reid, R. & Van Niekerk, J. 2014. From information security to cyber security cultures. *2014 Information Security for South Africa - Proceedings of the ISSA 2014 Conference*, 38: 97–102. http://dx.doi.org/10.1016/j.cose.2013.04.004.

Riek, M., Böhme, R. & Moore, T. 2016. Measuring the Influence of Perceived Cybercrime Risk on Online Service Avoidance. *IEEE Transactions on Dependable and Secure Computing*, 13(2): 261–273.

Romero-Mariona, J., Hallman, R., Kline, M., Palavicini, G., Bryan, J., Miguel, J.S., Kerr, L., Major, M. & Alvarez, J. 2017. An Approach to Organizational Cybersecurity. In *Enterprise Security*. 203–222. http://link.springer.com/10.1007/978-3-319-54380-2_9.

Roos, D. 2008. The History of E-commerce. *HowStuffWorks*: 1–4. http://money.howstuffworks.com/history-e-commerce2.htm.

Rostam, Y., Suwattana, T., Kallaya, Suntornvongsagul Hamimah, A. & Noraini, A. 2017. Post Occupancy Evaluation for Sustainable Neighborhood Development. *Advanced Science Letters*, 23(4): 3128–3131.

Saldana, J. 2008. *An introduction to codes and coding*.

Saldana, J. 2016. *The Coding Manual for Qualitative Researchers*. 3rd ed. Arizona: SAGE Publications Ltd.

Sandhu, R.S. 1993. Lattice-based access control models. *Computer*, 26(11): 9–19. http://ieeexplore.ieee.org/document/241422/.

Sarah, G. & Ford, R. 2006. On the definition and classification of cybercrime. *Journal in computer Virology*, 2(1): 13–20.

Saunders, M., Lewis, P. & Thornhill, A. 2009. *Research Methods for Business Students*. 5th ed. Pearson Education. http://books.google.com/books?id=u-txtfaCFiEC&pgis=1.

Scofield, M. 2016. Benefiting from the NIST Cybersecurity Framework. *Information and Management*: 25.

Shabut, A.M., Lwin, K.T. & Hossain, M.A. 2017. Cyber attacks, countermeasures, and protection schemes - A state of the art survey. *SKIMA 2016 - 2016 10th International Conference on Software, Knowledge, Information Management and Applications*: 37–44.

Shen, L. 2014. The NIST Cybersecurity Framework: Overveiw and Potential Impacts. *Scitech*

Lawyer, 10(4): 16–19.

Shenton, A.K. 2004. Strategies for ensuring trustworthiness in qualitative research projects. *Education for Information*.

Sherif, J.S. & Ayers, R. 2003. Intrusion detection: methods and systems. Part II. *Information Management & Computer Security*, 11(5): 222–229.

Shim, S.S.Y., Pendyala, V.S., Sundaram, M. & Gao, J.Z. 2000. Business-to-business e-commerce frameworks. *Computer*, 33(10): 40–47.

Shirey, R. 2007. *Internet Security Glossary*.

Shoemaker, D., Kohnke, A. & Sigler, K. 2016. *My library My History Books on Google Play A Guide to the National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework (2.0)*. 3rd ed. CRC Pres.

Shrivastava, O. 2014. To Study the Reasons For Customer Abandoning Their On-Line Shopping Cart Before Purchase Completion Stage. *The International Journal Of Engineering And Science*, 3(2): 51–73.

Sigler, K.E. & Rainey, J.L. 2016. *Securing an IT Organization through Governance, Risk Management, and Audit*. CRC Pres.

Singh, S. & Soni, S. 2018. Security of Data with 3DES & Watermarking Algorithm. *International Journal on Future Revolution in Computer Science & Communication Engineering*, 4(1): 137–142.

Skopik, F., Settanni, G. & Fiedler, R. 2016. A problem shared is a problem halved: A survey on the dimensions of collective cyber defense through security information sharing. *Computers and Security*, 60: 154–176. http://dx.doi.org/10.1016/j.cose.2016.04.003.

Smedley, L. 2014. *Virtual Entrepreneurship creating & operating a Home-based online business*. Academic e. https://books.google.co.za/books?id=HLWiAgAAQBAJ&pg=PT413&dq=online+retail+definition&hl=en&sa=X&ved=0ahUKEwjmtZiVjvzLAhXBXhoKHREhBz8Q6AEIKTAA#v=onepage&q=online retail definition&f=false.

Sohr, K., Drouineaud, M., Ahn, G.-J. & Gogolla, M. 2008. Analyzing and Managing Role-Based Access Control Policies. *IEEE Transactions on Knowledge and Data Engineering*, 20(7): 924–939. http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=4441714&url=http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=4441714.

Von Solms, B. 2015. Improving South Africa’s Cyber Security by cyber securing its small companies. *2015 IST-Africa Conference, IST-Africa 2015*: 1–8.

Von Solms, R. & Von Solms, B. 2004. From policies to culture. *Computers and Security*, 23(4): 275–279.

South African Government Gazette. 2013. *South Africa Protection Personal information Act, 2013*. http://www.gov.za/documents/download.php?f=204368 %5Cnhttp://www.greengazette.co.za/notices/act-no-4-of-2013-protection-personal-information-act-2013_20131126-GGN-37067-00912.

South African Government Gazette. 2015. *The National Cybersecurity Policy Framework*.

Sreejesh, S., Mohapatra, S. & Anusree, M. 2014. *Business research methods: an applied Orientation*. Springer. http://link.springer.com/content/pdf/10.1007/978-3-319-00539-3.pdf.

Stake, R.E. 1995. *The art of case study research*. Sage.

Stewart, B., Khare, A. & Schatz, R. 2017. Disruptions: Truth and Consequences. In *Phantom Ex Machina*. Cham: Springer International Publishing: 299–315. http://link.springer.com/10.1007/978-3-319-44468-0_20.

Strauss, A. and Corbin, J. 1998. *Basics of qualitative research techniques*. Sage Publications, Inc.

Tailor, J.P. & Patel, A.D. 2017. A Comprehensive Survey: Ransomware Attacks Prevention, Monitoring and Damage Control. *International Journal of Research and Scientific Innovation*, IV(November): 2321–2705. www.rsisinternational.org.

Tansay, O. 2007. Process Tracing and Elite Interviewing: A Case for Non-probability Sampling. *Political Science & Politics*, 40(4): 765–772.

Tatar, U., Gokce, Y. & Gheorghe, A. 2017. Strategic Cyber Defense: A Multidisciplinary Perspective. In *NATO Advanced Research Workshop on A Framework for a Military Cyber Defense Strategy*. Norfolk: IOS Press BV: 60.

Taylor, M.., Mcwilliam, J., England, D. & Akomode, J. 2004. Skills required in developing electronic commerce for small and medium enterprises: case based generalization approach. *Electronic Commerce Research and Applications*, 3(3): 253–265. http://linkinghub.elsevier.com/retrieve/pii/S1567422304000183.

Taylor, R., Fritsch, E. & Liederbach, J. 2014. *Digital Crime and Digital Terrorism*. 3rd ed. New Jersey: Prentice Hall Press. http://dl.acm.org/citation.cfm?id=2655330.

Teeter, P. & Sandberg, J. 2016. Cracking the enigma of asset bubbles with narratives. *Strategic Organization*. http://soq.sagepub.com/cgi/doi/10.1177/1476127016629880.

Thapa, D. & Harnesk, D. 2014. Rethinking the information security risk practices: A critical social theory perspective. *47th Hawaii International Conference on System Sciences*: 3207–3214. http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6758999.

The Department of Justice and Constitutional Development. 2016. *Cybercrimes and Cybersecurity Bill*.

Theforge. 2012. South African Payment Gateways. *The forge web creations*, (September).

Theohary, C.A. & Rollins, J. 2009. *Cybersecurity: Current Legislation, Executive Branch Initiatives, and Options for Congress*. https://fas.org/sgp/crs/natsec/R40836.pdf.

Tsakalidis, G. & Vergidis, K. 2017. A Systematic Approach Toward Description and Classification of Cybercrime Incidents. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, PP(99): 1–20. http://ieeexplore.ieee.org/document/7936557/.

Tucker, B., Brandley, J. & Kaplan, J. 2013. How good is your cyberincident-response plan? *McKinsey&Company*: 2–3. https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/how-good-is-your-cyberincident-response-plan.

Turban, E., King, D., Mckay, J., Marshall, P., Lee Jae, K. & Viehland, D. 2009. Electronic Commerce: A Managerial Perspective. , (October 2015).

Turianskyi, Y. 2018. *Balancing cybersecurity and internet freedom in Africa*.

United Nations Economic Commission for Africa. 2014. Tackling the challenges of cybersecurity in Africa. *Policy brief*, (8): 1–6.

UpGuard. 2017. COBIT vs ITIL vs TOGAF: Which Is Better For Cybersecurity? : 2–3. https://www.upguard.com/articles/cobit-vs.-itil-vs.-itsm-which-is-better-for-cybersecurity-and-digital-resilience.

US Cyber Command. 2008. *Air Force Cyber Command Strategic Vision*. http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA479060.

De Vaus, D. 2001. *Research Design in Social Research*. SAGE Publications.

Wegener, H., Barletta, W.A., Bosch, O., Chereshkin, D., Kamal, A., Krutskikh, A., Lehmann, A.H.R., Thomas, T.L., Tsygichko, V. & Westby, J.R. 2004. Toward a Universal Order of Cyberspace: Managing Threats from Cybercrime to Cyberwar Report and Recommendations. In *International Seminar on Nuclear War and Planetary Emergencies — 30th Session*. WORLD SCIENTIFIC: 385–435. http://www.worldscientific.com/doi/abs/10.1142/9789812702753_0044.

Wiles, R., Crow, G., Heath, S. & Charles, V. 2008. The management of confidentiality and anonymity in social research. *International Journal of Social Research Methodology*.

Williams, P. & Manheke, R.J. 2010. Small Business - A Cyber Resilience Vulnerability. In *International Cyber Resilience Conference*. http://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1013&context=icr.

Xianjun Geng & Whinston, A.B. 2000. Defeating distributed denial of service attacks. *IT Professional*, 2(4): 36–42. https://www.cert.org/information-for/denial_of_service.cfm?#1.

Yadav, A. 2018. Network Design: Firewall, IDS/IPS. *Infosec Institute*: 5–9.

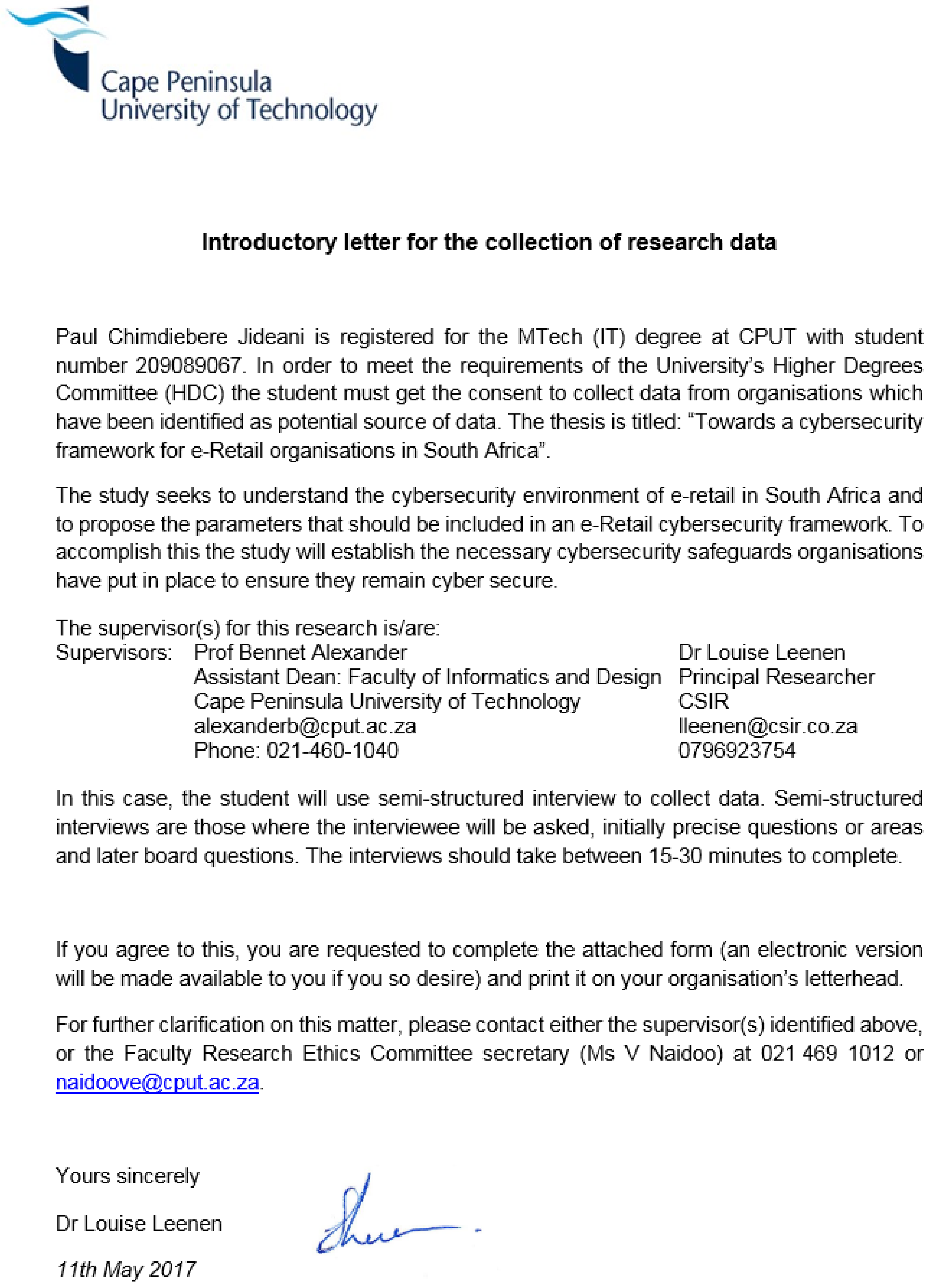
Yin, R.K. 2013. *Case study research: Design and methods*. SAGE Publications.

Yıldırım, E. 2013. The Effects of User Comments on e-Trust: An Application on Consumer Electronics. *Journal of Economics, Business and Management*, 1(4): 360–364. http://www.joebm.com/index.php?m=content&c=index&a=show&catid=33&id=347.

Zeneli, G. 2016. *Guidelines To Cyber Security With ISO/IEC 27032*. http://zih.hr/sites/zih.hr/files/cr-collections/3/iso-27032guidelinesforcybersecurity.pdf.

Zhang, Y. and Wildemuth, B.M. 2009. Qualitative analysis of content. Applications of Social Research Questions in Information and Library.

APPENDIX A: Introductory letter for data collection



Cape Peninsula
University of Technology

Introductory letter for the collection of research data

Paul Chimdiebere Jideani is registered for the MTech (IT) degree at CPUT with student number 209089067. In order to meet the requirements of the University's Higher Degrees Committee (HDC) the student must get the consent to collect data from organisations which have been identified as potential source of data. The thesis is titled: "Towards a cybersecurity framework for e-Retail organisations in South Africa".

The study seeks to understand the cybersecurity environment of e-retail in South Africa and to propose the parameters that should be included in an e-Retail cybersecurity framework. To accomplish this the study will establish the necessary cybersecurity safeguards organisations have put in place to ensure they remain cyber secure.

The supervisor(s) for this research is/are:

Supervisors:

Prof Bennet Alexander
Assistant Dean: Faculty of Informatics and Design
Cape Peninsula University of Technology
alexanderb@cput.ac.za
Phone: 021-460-1040

Dr Louise Leenen
Principal Researcher
CSIR
lleenen@csir.co.za
0796923754

In this case, the student will use semi-structured interview to collect data. Semi-structured interviews are those where the interviewee will be asked, initially precise questions or areas and later board questions. The interviews should take between 15-30 minutes to complete.

If you agree to this, you are requested to complete the attached form (an electronic version will be made available to you if you so desire) and print it on your organisation's letterhead.

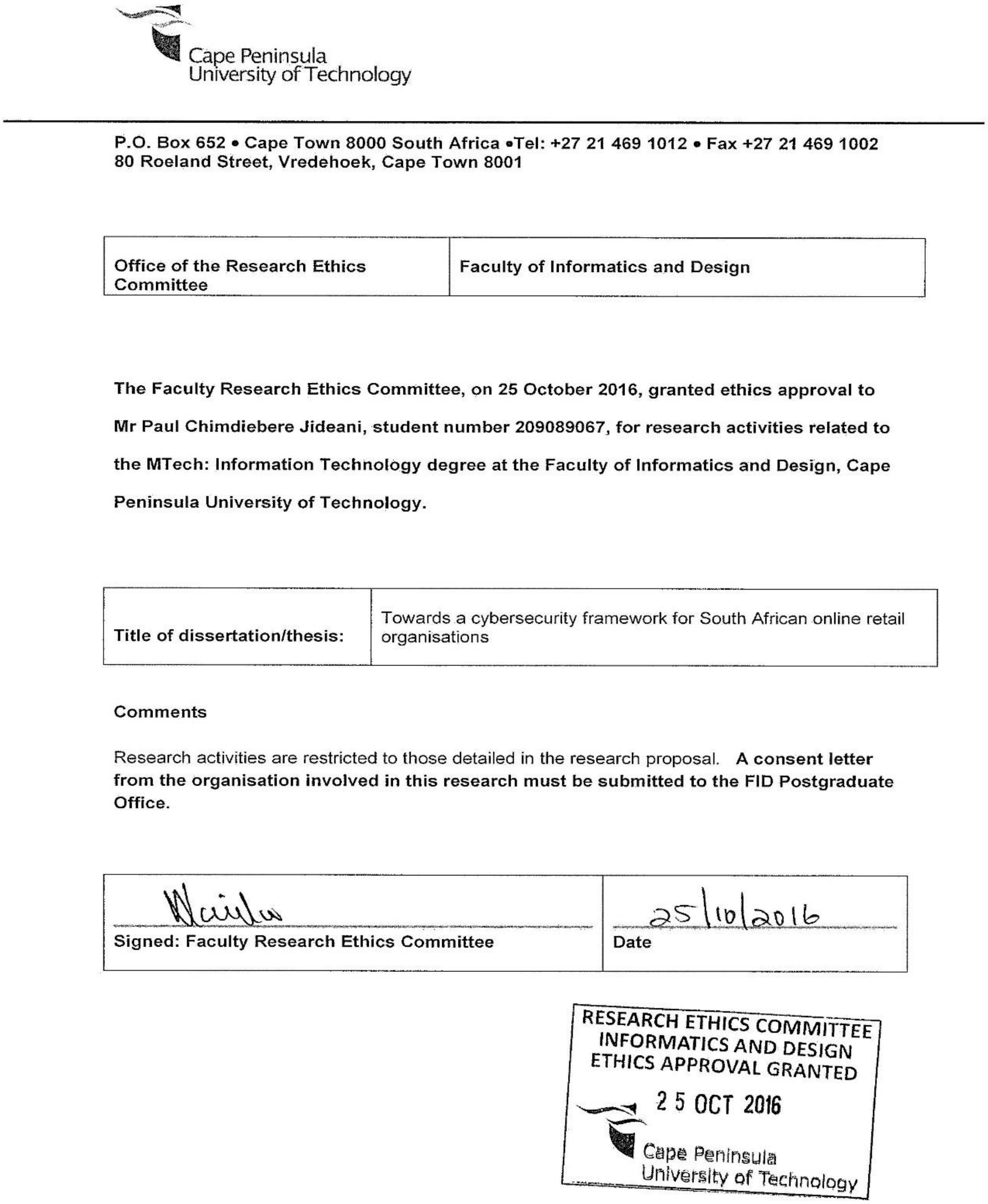
For further clarification on this matter, please contact either the supervisor(s) identified above, or the Faculty Research Ethics Committee secretary (Ms V Naidoo) at 021 469 1012 or naidoove@cput.ac.za.

Yours sincerely

Dr Louise Leenen

11th May 2017

Appendix B: Ethics Clearance certificate



Cape Peninsula
University of Technology

P.O. Box 652 • Cape Town 8000 South Africa •Tel: +27 21 469 1012 • Fax +27 21 469 1002
80 Roeland Street, Vredehoek, Cape Town 8001

Office of the Research Ethics Committee	**Faculty of Informatics and Design**

The Faculty Research Ethics Committee, on 25 October 2016, granted ethics approval to Mr Paul Chimdiebere Jideani, student number 209089067, for research activities related to the MTech: Information Technology degree at the Faculty of Informatics and Design, Cape Peninsula University of Technology.

Title of dissertation/thesis:	Towards a cybersecurity framework for South African online retail organisations

Comments

Research activities are restricted to those detailed in the research proposal. **A consent letter from the organisation involved in this research must be submitted to the FID Postgraduate Office.**

Signed: Faculty Research Ethics Committee	25|10|2016 **Date**

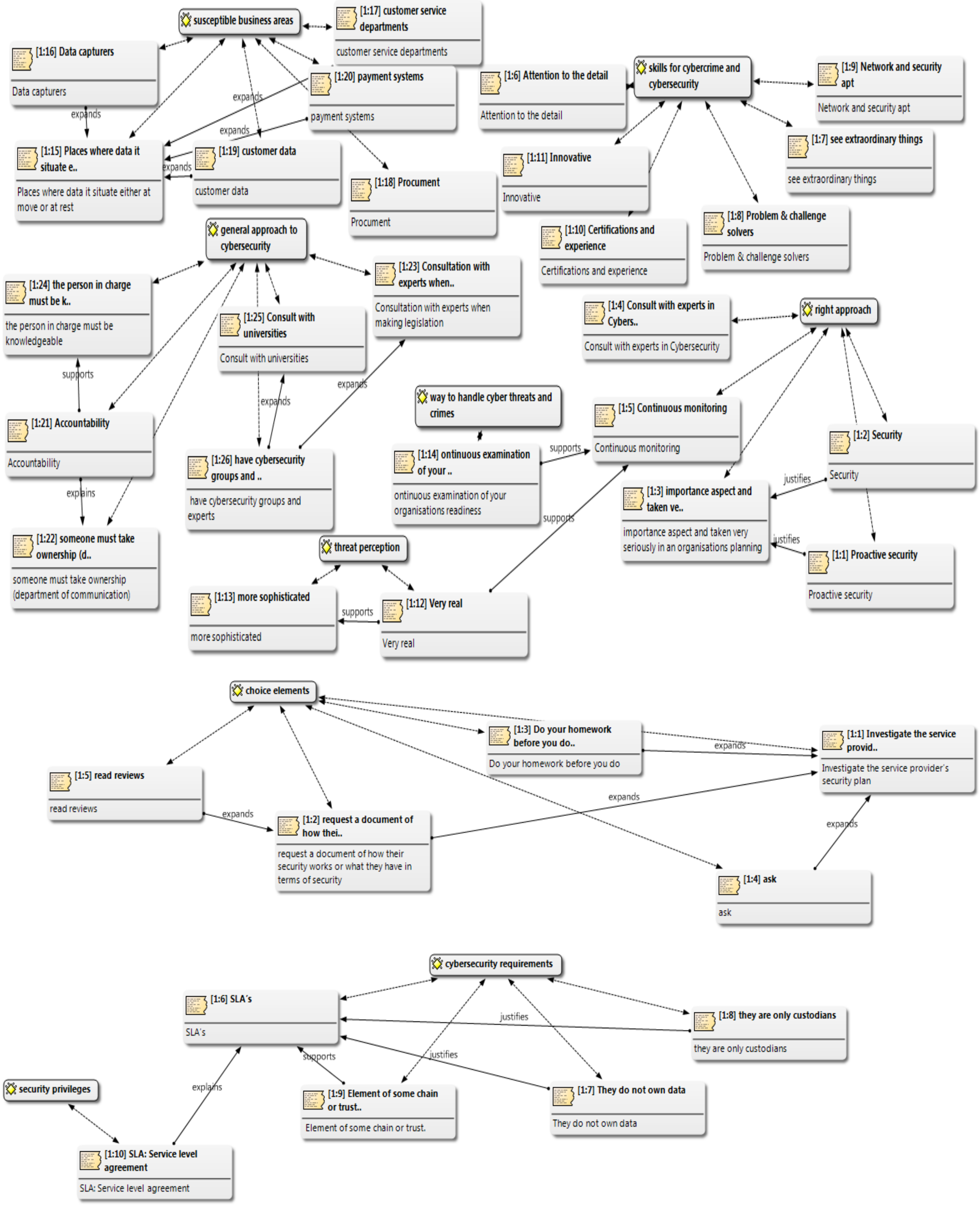
RESEARCH ETHICS COMMITTEE
INFORMATICS AND DESIGN
ETHICS APPROVAL GRANTED
2 5 OCT 2016
Cape Peninsula
University of Technology

APPENDIX C: List of participants and objectives

Participant were selected from the population IT managers, information security mangers, cybersecurity researchers and specialist, e-commerce developers.

Participant	Rank	Objectives	Status
1	E-commerce Developer	To obtain insight into their understanding of Cybersecurity and electric retail in South Africa.	Achieved
2	Information Security Manager	To obtain insight into their understanding of Cybersecurity and electric retail in South Africa.	Achieved
3	Cybersecurity Specialist	To obtain insight into their understanding of Cybersecurity and electric retail in South Africa.	Achieved
4	Cybersecurity Specialist	To obtain insight into their understanding of Cybersecurity and electric retail in South Africa.	Achieved
5	IT Manager	To obtain insight into their understanding of Cybersecurity and electric retail in South Africa.	Achieved
6	Information Security Manager	To obtain insight into their understanding of Cybersecurity and electric retail in South Africa.	Achieved
7	Cybersecurity Specialist	To obtain insight into their understanding of Cybersecurity and electric retail in South Africa.	Achieved
8	Information Security Manager	To obtain insight into their understanding of Cybersecurity and electric retail in South Africa.	Achieved
9	Information Security Manager	To obtain insight into their understanding of Cybersecurity and electric retail in South Africa.	Achieved

APPENDIX D: Sample Atlas.Ti Data Presentation


susceptible business areas
[1:17] customer service departments
customer service departments
[1:16] Data capturers
Data capturers
expands
[1:20] payment systems
payment systems
expands
expands
[1:15] Places where data it situate e..
Places where data it situate either at move or at rest
expands
[1:19] customer data
customer data
[1:18] Procument
Procument
[1:6] Attention to the detail
Attention to the detail
skills for cybercrime and cybersecurity
[1:9] Network and security apt
Network and security apt
[1:7] see extraordinary things
see extraordinary things
[1:11] Innovative
Innovative
[1:10] Certifications and experience
Certifications and experience
[1:8] Problem & challenge solvers
Problem & challenge solvers
general approach to cybersecurity
[1:23] Consultation with experts when..
Consultation with experts when making legislation
[1:24] the person in charge must be k..
the person in charge must be knowledgeable
supports
[1:25] Consult with universities
Consult with universities
expands
expands
[1:21] Accountability
Accountability
explains
[1:22] someone must take ownership (d..
someone must take ownership (department of communication)
[1:26] have cybersecurity groups and ..
have cybersecurity groups and experts
[1:4] Consult with experts in Cybers..
Consult with experts in Cybersecurity
right approach
way to handle cyber threats and crimes
[1:14] ontinuous examination of your ..
ontinuous examination of your organisations readiness
supports
[1:5] Continuous monitoring
Continuous monitoring
supports
[1:2] Security
Security
justifies
[1:3] importance aspect and taken ve..
importance aspect and taken very seriously in an organisations planning
justifies
[1:1] Proactive security
Proactive security
threat perception
[1:13] more sophisticated
more sophisticated
supports
[1:12] Very real
Very real
choice elements
[1:3] Do your homework before you do..
Do your homework before you do
expands
[1:1] Investigate the service provid..
Investigate the service provider's security plan
[1:5] read reviews
read reviews
expands
expands
[1:2] request a document of how thei..
request a document of how their security works or what they have in terms of security
expands
[1:4] ask
ask
cybersecurity requirements
[1:6] SLA's
SLA's
justifies
[1:8] they are only custodians
they are only custodians
supports
justifies
explains
security privileges
[1:9] Element of some chain or trust..
Element of some chain or trust.
[1:7] They do not own data
They do not own data
[1:10] SLA: Service level agreement
SLA: Service level agreement

APPENDIX E: Sample Interview transcript

Full interview transcript are available in the accompanying CD or on request.

Interviewer: Interesting.00:06

Interviewee: It's a firewall, i mean that's a piece of software that runs on the [unclear 00:11] which will prevent this sort of thing from happening. 00:18

Interviewer: In the case, how do we reduce the severity of that, so as to not cripple 00:29

Interviewee: The denial of service 00:32

Interviewer: Yeah, the denial of service attacks 00:32

Interviewee: Well, the best would be to my..what i would do is to make sure that you have...you separate, you don't put everything on the same network. [unclear 00:53] you perhaps split, split some of your computers so that they can't be on [unclear 00:56] networks. Because, normally, the denial of service works on the one so it spreads in the same network and could cause people not [unclear 01:08] to get into your site.01:14 . The best way is to prevent it, in my opinon that is the best strategy. By a number of ways using filtering(there are so many types), Igress & egress are there. Also simple but basic is security patches applying them. Don’t broadcast your IP never, also loadbalancing.. So many others honeypots and so on. I don’t know all

Interviewer: Okay, any remediation strategies. How do we recover from such, an occurrence of such an attack. 01:24

Interviewee: Pretty what you have to do is to take the site off-line. Then of course, they can't attack. There will be some downtime required, so you have to put down your website or e-retail site and then you fix the...[unclear 01:48] that's a weak point somewhere in your firewall, so you have to fix it and then you can bring it back on-line. 01:55

Interviewer: Okay, third category drive by download, this has to do with things downloaded off the Internet, distribution by flash drives or through the network. Drive by download. Any preventative strategies that you know that we could [unclear 02:14] 02:15

Interviewee: Yeah, you have most of the anti-virus software [unclear 02:16] these days. You can actually block anything you plug into your USB port. So it may pick up something is plug in and then it will tell you "Please clean this first" or it won't allow you to actually use the USB drive. So that's something. But if it is downloaded from the Internet of course, that is a bit difficult. But once again, most anti-virus software will cater for that. It would actually block it and quarantine the file if it picks up it's a malicious file. 02:52

Interviewer: Okay, social engineering, social media, very big thing now. Social media in terms of attacks through social media where social sites, password, keyboard hacks. How do we prevent against that. 03:18

Interviewee: Yeah, well, once again you know, the..that's why your firewall is important. In that you specify what is allowed, what is not allowed and [unclear 03:33] stuff like blacklist, white list, and certain sites will be allowed, certain sites will not be allowed. So it will be in your configuration of your firewall, that's where you will determine what is allowed, what can be done, what cannot be done. 03:49 . Also awareness is important. Normally attackers learn and understand their victim before an attack happens. So victims should ensure they safeguard their information: I think that is sear-phishing. Also take note of reverse social engineering

Interviewer: And to reduce the severity in case it's already happening, how do we reduce 04:04

Interviewee: Well, the best will be to [unclear 04:05] block access from social media. Definitely these firewalls and software that you put in place, you can specify a particular category of access. So you can [unclear 04:21] block all social media access until you fix the problem. [unclear 04:27]04:27 . Bare in mind the channel of social engineering attacks matters

Interviewer: Okay, recovery methods or procedures? 04:32

Interviewee: There are a lot. That's the same as i explained the other one is you clean up the website and you restore from a clean copy.04:46

Interviewer: Moving on to the broad question around ecosystem and banking supply. So these will be fairly general in nature. It could be national but not really as technical as the other ones. So what do you think should be the right approach to cybersecurity within an e-retail organisation, because security is very important today. We have had so many cases of ransom where companies are being asked for...seized their data and asked for money. So in an organisation, what should be their approach to security? Should it be something taken important or what do you think? 05:30.

Interviewee: Yeah, definitely, security is...in an IT environment, very important. So i think it's should be taken very seriously and when you decide to start a new system or a new website, you must [unclear 05:47] one of the first things to consider. What is the security around this site? And best is to call the expert, because there are people that are experts in cybersecurity. So, consulting with some of them would be a good idea. And in terms of general measure that you should take is to make sure you download the latest version of patches, you know, of Windows update. I know from these previous ransomware that came in maybe wannaCry and those ones attack could have been prevented if people had the latest versions of Windows installed and the patches that are sent by Windows or Microsoft. That normally help you to protect you against that and also to have anti-virus software installed and actively running. Yeah, so [unclear 06:53] when you design a particular e-retail solution you must make sure that you have factored in [unclear 07:00]. Get the consultant in perhaps and to make sure you've got anti-virus and the service provider you use is ...you can trust that he would also do what he's supposed to do to protect you. 07:13

Interviewer: In an organisation, what skills should those dealing with security have? If you have a security section, what are the security skills they should have in terms of both certifications and qualifications? 07:30

Interviewee: Yeah, of course they are courses that you could send these people to. But i think the important thing is attention to detail. That is the important thing and they must be able to see extraordinary things that comes up. Definitely you will see warning signs that...of things coming up. That's typical of your anti-virus software will do is to go through all files or emails or stuff that contain details of your organisation and check...as well as the one coming on USB devices that are plugged in and...they must be able to solve problems. They must be problem solvers. They must be able to work after hours, typically you need somebody that...well [unclear 08:25] people. That sort of narrows [unclear 08:28] because it can be quite technical some of the security things that you need to know. So they have to know the networks and because most things happen over the network, there must be network experts, good problem solvers as i said and have a good general knowledge of IT in general. 08:49

Interviewer: Okay, within an organisation, what business areas...because there are specific things either in your purchasing, manufacturing, if the e-retail is a [unclear 09:02] setting. What business areas do you think are more prone to cyber attacks? Like customer data, the company that handles processing and what areas do you think within business are very susceptible to cyber attacks? 09:18

Interviewee: Well, i would say it could be your data capturers are the people that are working with data or your customer service department who typically receive calls or emails from customers and perhaps your marketing people, they also...well in our organisation for instance, they work a lot on social media, they interact with customers and...yeah so people who are in contact customers...i would say, that's the people that would be most vulnerable [unclear 09:58] . Also those that handle customer raw data 09:58

Interviewer: ..And nationally, what would you like to see in terms of cybersecurity, from a national level, in terms of legislations, or directives or policies an e-retail should follow? What do you think should be the general...10:18

Interviewee: Well, that actually also counts for other parts of the government and so the first thing is accountability. Somebody must take ownership of [unclear 10:31] that is the first thing. Currently that falls under the department of communications if i am not mistaken. So you need somebody that's knowledgeable, that knows the industry and they must...when they do the legislation, they must make sure that they speak to the knowledgeable people. One area perhaps that...one thing that i would do differently if i were say the minister, for example is to speak to the experts for example, many universities have got special departments or groups that look after cybersecurity or that does research in cybersecurity so you must have a knowledge of people that can help you to put together the legislation. 11:24

Interviewer: Okay in general, what is the acceptable way in an organisation to handle, is it proactive thing or reactive thing...in an organisation. Do we wait for it to happen and certainly do things or if it's proactive, what are the things we should take [unclear 11:41] 11:41

Interviewee: Well, proactive is definitely integral...and i have got these [unclear 11:47] you have software, especially anti-virus software and things that are installed on your firewall to protect you. And then also you need somebody to just check because definitely you will get report of attacks so you have the software that's installed which will prevent it from coming into the organisation and then you must have somebody, some administrator or somebody that actually checks the attacks, the reports of the attack. So....sometimes it [unclear 12:21] and it stops by the software or it does not stop then obviously [unclear 12:27] able to come through then that person must immediately act and then...what you often do is to take that PC for example, take it off the network, you just unplug it from the network so it can't spread further into the rest of the organisation. A continuous examination of your organisations readiness, you can do it yourself or employ an external testing team if I may call it 12:45

Interviewer: Okay, that's that. Thanks for the e-retail...thank you. Now, the other one is the banking. The bank, banking or finance plays an important role in e-retail. That's where payment go through, card payment system as well as customer data goes through there. So as a retailer or e-retailer as the case may be what role does the bank play in your business typically? 13:17

Interviewee: Well, because the bank has got it's own legislation and stuff which is very strict, and they must also outsource certain system [unclear 13:25] what typically happens is that you employ or you make...you get the services of what we call the payment gateway. So that's [unclear 13:35] by the payment gateway. So the payment gateway is a company such as [unclear 13:40] is a one big company that does that. [unclear 13:43] they are called a payment gateway...and there are others as well. [unclear 13:48] payments for example, i can't remember some of the others but some of [unclear 13:54] which is a payment gateway. So they act as the middle man between the e-retail and the bank. So bank [unclear 14:03] takes the money the bank is still the place where the money is deposited by the customer through his credit card but the thing with gateway you could annul the transactions on behalf of the e-retailer so typically when you purchase on-line and it's time to checkout and pay and so on, the payment gateway thing will pop up so you don't talk directly to the bank. The payment gateway company will handle that, and they will process the transaction, they will make sure that the credit card is...that the information is not leaked somewhere in a language that is secure and they will send it through to the bank and the bank will then speak to say for example Visa or MasterCard [unclear 14:48] this is a valid card, it's the right password and stuff, comes back and then it typically it will give a message back to e-retail [unclear 14:56] this transaction has been approved by the bank and then it carries on from there. 15:02

Interviewer: Okay, thanks. In terms of cybersecurity, what do you as a retailer impose on the banks. You've mentioned that the banks' legislation is quite strict which i also agree with, but what requirements do you place or before choosing a bank, if i may put it, what are the things you should look out for in terms of security? 15:25

Interviewee: Yeah, well you see....definitely as i said it depends on how [unclear 15:41] interactive the bank because in our case, we...the banks and the bank account are chosen by the financial department. The financial manager typically would work with the banks and they would open accounts and so on and so on and obviously...and then they also use Internet banking for example to [unclear 16:01] transactions. But when it links to the e-retailing part the security is actually more important on the payment gateway company. So..in terms of whole cybersecurity in terms of e-retailers, your payment gateway that link between your bank and business is actually more important than the bank itself. Because the bank only accepts your money. The money is only deposited in that account, so the security, of course it will be the normal for banking security so the security in terms of what you....that's not the main thing that you have to decide on when you decide on a bank, you'd rather...it's more important to have a good payment gateway. 16:53

Interviewer: Okay, what cyber attacks could happen from the bank that could affect you as the e-retailer? Because there are so many attacks that don't...are not targeted at the e-retailer. Though the target is the e-retailer, but it comes through the other channels it has. 17:15

Interviewee: Yeah, see what definitely...[unclear 17:18] that happens is that somebody might...if they have been [unclear 17:23]...it doesn't happen often but a criminal might intercept if the security is not in place, you know he might intercept credit card details for example, of a customer so while he's busy doing his payment on the transaction, somebody might intercept his details and then use that to buy other stuff or to sell, but normally, if the payment gateway is in place properly and everything is installed the way it should be then it should not be able to [unclear 18:00] but i mean there is insurance if you don't do it the right way. So the criminals, the cyber criminals, they would steal identity, they might also steal the ID number of people, or tax [unclear 18:15] and credit card number, that's the most important thing. So one thing that you also should not do as a retailer and i think that is governed by legislatures is you not suppose to store the credit card numbers of your customers because then it becomes a risk. There could be [unclear 18:35] or the could be fraudulently used by somebody may be even in the organisation if it's in some database, somebody can get access to [unclear 18:46] they can use it or give it to their friends or somebody else. 18:49

Interviewer: Thanks, we are on to the next point, legislation and you've touched a bit on that. Okay, what role does legislation play? Also legislation has to do with framework, if you are familiar with the NIST framework then... 19:02

Interviewee: Nope i am not familiar with it. 19:05

Interviewer: Okay, there are so many...so what...in terms of legislation, both policies and framework, what role does it play in cybersecurity in e-retail? 19:15

Interviewee: Yeah, see like with many other parts of IT, security is governed by what you call the best pratices and standards that's been put together by organisations such as ITIL is one big framework that is used by many people, COBIT is another important framework...that...so [unclear 19:50] it gives you if you read through those frameworks it gives you a guideline on how you should do your business governed by these practices. So legislation also suppose to look at these things, to make sure that legislation adheres to these best practices, frameworks that [unclear 20:19]. So a lot of them...most of them are already been published, it is available, you can do a [unclear 20:25] you can download it, you can subscribe to these organisations. They will give you guidelines that has been designed over many years to make sure that it is the best practices, best way of doing things, the most secure way of doing things. 20:43

Interviewer: Okay, you have answered my next question, but let's...what legislation or frameworks are available to the e-retailer? You've mentioned [unclear 20:53] and [unclear 20:54] are there other any specific to the e-retailer which a retailer could refer to in terms of starting? 21:01

Interviewee: I don't know...i think a South African context, you know, you have to look at the...well there are different acts related to IT 21:16

Interviewer: POPPI/POPPI, ECT? 21:17

Interviewee: Yeah the ECT act would be a good one to start with. The PUPPY is more about protection of personal information. These days of course, that's also something you have to look at to make sure that you don't make it possible for people to steal your customers' personal information. Yes, so that would be a starting point, the ECT act and the...and also the [unclear 21:43] reports...you must have [unclear 21:50]. So that would also be a good starting point if you read through those legislation. 21:56 . There are also international ones ISO standards

Interviewer: How is legislation measured? or will i say compliance to legislation within an organisation? Because as a e-retailer, there are so many legislation around ECT, PUPPY, e-commerce act...how does an organisation or yours, if i may ask, measure it's compliance to it? Is there any policing of it or what? 22:28

Interviewee: Yeah, not specifically. So what we actually do have is that we...annually, we have the auditors come in. So in our case it is Deloitte and [unclear 22:42] they come in and then they have IT risk assessment that they do. So that will be the measure that they do, it's normally....then they bring experts, they bring IT experts and security experts and then [unclear 22:58] with me and sometimes support staff to ask...to sort of to determine whether we are compliant to these practices and legislation. 23:10

Interviewer: Thank you. The supplier, this is one of the major component 23:17

Interviewee: Is that not the supplier of the product..[unclear 23:19]

Interviewer: Could be...yes, the supplier...yeah, what safeguards are in place? Because some attacks...because there are some suppliers that have certain access to a company where they maybe upload [unclear 23:37] 23:37

Interviewee: Yeah [unclear 23:38] technically [unclear 23:39] 23:41

Interviewer: What safeguards are in place to make sure no attack comes from the side of the supplier? 23:52

Interviewee: Yeah, well that will be...there's no special security, the normal internal security that you do, for example you typically use a...well there are two ways these days to get files and catalogs across. One will be FTP which is the old way of doing things, and FTP...you can do a secure FTP server for uploading and stuff or what more people these days do is to use webservices which is a way of two different serves to communicate with each other and in a webservice, you need credentials. So people can't upload stuff without you knowing it and without...yeah some [unclear 24:40] credentials and the way it is designed, you know the webservice that we use, it is designed in such a way that it is one-to-one communication. It is not open to the Internet. It goes through a secure tunnel if you like. 24:58

Interviewer: Okay, what requirement should an e-retailer place before choosing...i want if i go in to become an e-retailer, what requirements should i take in place before choosing a supplier in terms of security, there are many other things you should consider, but in terms of security...25:17

Interviewee: Tell me, are you talking digital products or physical products? 25:20

Interviewer: Yeah, both. It ranges from...25:23

Interviewee: Yeah because physical products, i mean it's not gonna attack your network computer system but i mean so obviously you need to make sure that the system that the supplier use are also secure, you know, so when you choose it you must talk to say the IT support person of that company to make sure that, you know when you interact with them through your systems...it depends how you are integrating...because definitely...it depends, if you are fully integrated for example, when you...when a customer place a order and you must now process the order, do you just print it out and fax it through or do you take it to them or..by hand or 26:10

Interviewer: Or do they see it there? 26:12

Interviewee: ...or do you...was it fully integrated? Remember the order is placed and the money is received, a digital proof, notification goes to the supplier it says please provide these products and then it's gonna depend on how it's done. Is it done through email or an integrated systems that talks directly to their system or [unclear 26:33] the email message that they get. So normally if you send the order to the supplier through email, that is quite secure, depending on your email provider. But if it is a direct integration, normally the security is also set up when you do the integration to make sure that there is a secure connection between you and your supplier. 26:55

Interviewer: Also, what privileges when we talk about fully integration, should a supplier be given? 27:04

Interviewee: Well, you see...well, once again, it depend on your agreement with the supplier, but typically he must be able to receive orders obviously, and then he must be able to send back acknowledgements that he did receive...there will have to be a two-way communication. But typically, he would not change or change anything on your side. So he will only receive stuff. So the only stuff he will send back will be acknowledgement to say yes, i received the order or there is a delay in the order or whatever other status updates there might be in terms of suppling the products. 27:49

Interviewee: Okay, last section. The service provider...many e-retail organisation outsource their web design or their data or their storage to third parties as the case may be. So what should be...what element should be taken into consideration in terms of security when outsourcing some of your business areas...websites? 28:22

Interviewee: Yeah well, so obviously you have to make sure from the service providers that they have measures in place. So this is for them to perhaps give you a diagram of how their security works so then you can evaluate if what they do is secure. So i would definitely investigate the service providers' security plan if you like, to make sure that they comply to what you have to do and once again, like i said from the beginning, make sure that you choose reputable service providers, for example, if you get a call from somebody saying "yeah could you please host your website with me, i am gonna give you a special price", then it's something on his PC or some place where it is not secure. So best is to work with one of the biggest suppliers, the well known suppliers for example, the big one these days that you get...Amazon web services, Microsoft or Google or even some of the local suppliers like we for example for our website we use [unclear 29:41] which is well know hosting company and also other companies such as Vodacom and Telkom, Afrihost. They all host websites and services for other people. So best is to choose one that is known in the industry as reliable and trusted provider. So..i would say the important thing is to do your homework before you choose one is to also ask other people, other references say for example you'd ask [unclear 30:18] give me a reference to one of your customers, and you will call that customer and ask what is your experience with this provider? Are you happy? Is security in place? Stuff like that. 30:31

Interviewer: Okay between the service provider and the e-retail, what agreement are in place in terms of divulging of information, [unclear 30:40] rights and what should be...? 30:43

Interviewee: Yeah, see the thing is that you need to make sure that the supplier is...the service provider is aware of is that your data, even though they keep it, they are...it's not their data. The data still belongs to you, even though they are custodians, they must make sure that the data is kept secure on their server...so you must have some service-level agreement. I think the best is to...well you actually have to, you don't have a choice but to put together a service-level agreement with your service provider where security measures will also be explained. So typically, in a service-level agreement you will have what services are provided by your service provider and what is the responsibility of you the customer and then also that service-level agreement must say what is the security that's in place. In our case for example, we outsourced the development of our website as well as the hosting of the website. That's all handled by the developers of the website so they have full control over the server where the website is hosted and our service-level agreement with them would describe exactly what is required. 32:11 . Chain of trust in terms of securing one anothers data

Interviewer: Okay, you've answered the last so...that is the privileges or what they should...[unclear 32:18] 32:18

Interviewee: Yeah, that'll be in the service-level agreement.32:22

APPENDIX F: Survey instrument

Name of Respondent	Designation	Company	Email	Contact details

Questions will be asked based on a taxonomy of cyberattacks and an e-Retail ecosystem diagram below: see appendix below

Category	Question	Comments
Online fraud	What are the preventative measures should be taken to prevent online fraud?	
	In the event your organisation is a victim of such what interventions can be taken to reduce the severity and consequences of the attack?	
	What measures/actions are required to reverse or stop these attacks from occurring?	
DDoS	What are the preventative measures should be taken to prevent denial of service attacks?	
	In the event an organisation is a victim of such what actions can be taken to reduce the severity and consequences of the attack?	
	What actions are required to reverse or stop these attacks from occurring?	
Drive by download	What are the preventative measures to be taken to prevent drive by download attacks?	

	In the event an organisation is a victim of such what actions can be taken to reduce the severity and consequences of the attack?	
	What actions are required to reverse or stop these attacks from occurring?	
Social engineering	What are the preventative measures to be taken to prevent social engineering attacks?	
	In the event an organisation is a victim of such what actions can be taken to reduce the severity and consequences of the attack?	
	What actions are required to reverse or stop these attacks from occurring?	

Niche area	Question	Comment
e-Retail	What is the right approach to cybersecurity within an e-Retail organisation?	
	What are the skills requirements to handle cybercrime and cybersecurity?	
	How do you perceive the threats posed by cybercrime?	
	What should be the acceptable way to handle cyber threats and crimes?	
	What are the business areas in e-Retail that are susceptible to attack?	

	What should be the general approach to cybersecurity of e-Retail on a national level?	
Banking	What role does the bank play to e-Retail?	
	What cybersecurity requirements does your company impose on banks?	
	What are the cyber threats posed by banks and how do they affect the e-Retailer?	
Legislation	What role does national and international legislation play in terms of cybersecurity?	
	What legislation or frameworks for cybersecurity are available to e-Retail?	
	How is the compliance to legislation measured and reported?	
Supplier	What cybersecurity safeguards should be in place to restraints attacks from supplier?	
	What are the requirements for choosing a secure supplier?	
	What security privileges should be granted to the supplier?	
Service Provider	What elements should be taken into consideration when choosing a service provider to partner with?	
	What are the cybersecurity requirements of your organisation and the ISP when dealing with service providers?	