UNIVERSITY OF KWAZULU-NATAL

Information Assurance within Supply Chains' Structures and Processes

By
Ajayi Nurudeen Abimbola
209510551

A thesis submitted in fulfilment of the requirements for the degree of Doctor of Philosophy (Information Systems and Technology)

School of Management, IT and Governance
College of Law and Management Studies

Supervisor: Prof Manoj Maharaj

December 2017

DECLARATION

I, Nurudeen Abimbola Ajayi declare that

i. The research reported in this thesis, except where otherwise indicated, is my original work.

ii. This thesis has not been submitted for any degree or examination at any other university.

iii. This thesis does not contain other persons' data, pictures, graphs or other information, unless specifically acknowledged as being sourced from other persons.

iv. This thesis does not contain other persons' writing, unless specifically acknowledged as being sourced from other researchers. Where other written sources have been quoted, then:

   a) Their words have been re-written but the general information attributed to them has been referenced;

   b) Where their exact words have been used, their writing has been placed inside quotation marks, and referenced.

v. Where I have reproduced a publication of which I am an author, co-author or editor, I have indicated in detail which part of the publication was actually written by myself alone and have fully referenced such publications.

vi. This thesis does not contain text, graphics or tables copied and pasted from the Internet, unless specifically acknowledged, and the source being detailed in the thesis and in the References sections.

Signed:

[redacted]

Ajayi Nurudeen

Date: 22/12/2017

ACKNOWLEDGEMENTS

Firstly, I wish to thank God Almighty for giving me the ability, wisdom and strength to commence and conclude this dissertation work.

I also wish to express my deepest gratitude to Professor Manoj Maharaj for all his support and guidance. His valuable supervision is highly appreciated. I also wish to express my sincere gratitude to my colleagues and staff of the discipline of Information Systems & Technology.

I would like to acknowledge and express my immense gratitude to Junaid Amra and Abdulbaqi Badru.

I also wish to express my distinguished and unfathomable appreciation to my parents, siblings and friends, for all their unconditional support, words of encouragement and understanding.

Finally, my heartfelt appreciation goes to my wife and children, for their understanding, support and encouragement. You are all appreciated.

ABSTRACT

Organisations are challenging the traditional linear-based market model which is characterised by a straight line movement of goods and services. As a result, they are increasingly forming and moving towards a value web of supply chain network that connects a whole ecosystem of trading partners. These networks, which are mostly complex and dynamic, are creating a global market environment in which organisations no longer focus only on their immediate suppliers and customers, but also on the optimization and the smooth flow of information, funds and materials, within their respective direct and remote trading networks.

The large number of participants within most supply chain networks has necessitated that these networks be agile and resilient. For supply chain networks to be agile and resilient, and for supply chains' structures, processes and resources to be synchronized and integrated, the organisations within the supply chain must share information. Hence, in today's supply chains, interests are moving towards obtaining the most benefits from information. In order to obtain these benefits from information, organisations are making use of information systems and their related technologies to acquire, process and adequately share information. These systems are making it possible for organisations to form strategic partnerships within the supply chain networks.

The global market environment is causing supply chains to expand, and the expansion is exposing information to various security vulnerabilities and risks. The exposure of information to different vulnerabilities and risks is forcing trading partners to seek assurance that the information within their supply chain network is adequately protected and also performs as advertised. To understand how the assurance sought by trading partners can be provided, this study investigated information and information systems' security within supply chains' structures and processes. The study also investigated how information assurance objectives (i.e. confidentiality, integrity, availability, authentication and non-repudiation) can be achieved optimally within supply chains. Finally, the study proposes an information assurance model, which if adopted by decision makers, could enable them sustain their respective functions and processes within the supply chain network.

In order to achieve the objectives of this study, the exploratory design and the case study approach were adopted in this study. The study also adopted the qualitative research method, and hence, semi-structured interviews were conducted, and served as the primary means of data collection. Participants in this study were drawn from two categories of organisations, which are supply chain and logistics organisations, and Information Technology (IT) consulting organisations. Therefore, the purposive sampling method was adopted in this study. An inductive approach was adopted in the analysis of data, and as a result, thematic analysis was adopted as the analysis method. The main outcome of the study is the proposed information assurance model that can enable decision makers sustain their respective functions and processes within the supply chain network.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS

API - Application Programming Interfaces

AWS - Amazon Web Services

CAS - Complex Adaptive System

CCA - Continuous Compliance Assurance

CEDI - Collaborative Electronic Database Infrastructure

CIO - Chief Information Officer

COBIT - Control Objectives for Information and Related Technologies

CPFR - Collaborative Planning Forecasting and Replenishment

CR - Continuous Replenishment

CRM - Customer Relationship Management

CRP - Continuous Replenishment Program

CSP - Cloud Service Provider

ECR - Efficient Consumer Response

EDI - Electronic Data Interchange

EDP - Electronic Data Processing

ERP - Enterprise Resource Planning

GE - General Electric

GM - General Motors

HDR – High Dynamic Range

HRM – Human Resource Management

HTTP – Hypertext Transmission Protocol

IA – Information Assurance

ICMP – Internet Control Messaging Protocol

ICT - Information and Communication Technology

IDS - Intrusion Detection System

IEC - International Electro technical Commission

IMIS - Integrative Manufacturing Information System

IP – Internet Protocol

IS - Information Systems

ISO - International Organisation for Standardisation

ISP - Internet Service Provider

IT - Information Technology

ITCO - Information Technology (IT) Consulting Organisations

ITIL – Information Technology Infrastructure Library

JIT - Just-in-time

MES - Manufacturing Execution Systems

MRP - Material Requirements Planning

MRP II - Manufacturing Resource Planning

PDM - Product Data Management

PII - Personal Identifiable Information

QCA - Qualitative Comparative Analysis

QDAS - Qualitative Data Analysis Software

QR - Quick Response

RAT - Routine Activity Theory

RFID - Radio Frequency Identification

SCDI - Supply Chain Design Information

SCIRM - Supply Chain Information Risk Management

SCLO - Supply Chain and Logistics Organisation

SCM - Supply Chain Management

SDK - Software Development Kit

SETA - Security Education Training and Awareness

SIEM - Security Information and Event Management

SOA - Service-oriented Architecture

SOD - Segregation of Duties

TCP - Transmission Control Protocol

TV - Television

UDP - User Datagram Protocol

VAN - Value-Added Network

VICS - Voluntary Interindustry Commerce Standards

VMI - Vendor Management Inventory

WMS – Warehouse Management System

CHAPTER 1: INTRODUCTION

1.1 Introduction

The world is experiencing an intense and global trading era where one of the most difficult challenges faced by organisations is the management of resources, such as information, funds and materials, among geographically dispersed trading partners (Piderit, Flowerday, & Von Solms, 2011). The intense and global trading era is also making organisations face fiercer and increasing competition. The increasing competition is forcing organisations to improve their internal operations and integrate their trading partners. According to Mizgier, Wagner, & Jüttner (2015), this increasing competition, coupled with increasing consumers' demands are also causing an increase in the pressure on organisations to make their business processes more efficient and responsive. To achieve these, organisations are increasingly demanding for an integrated production and distribution process, and also, for a consumer-oriented trading network that can facilitate the smooth running of business processes, so as to meet the consumers' demands (Gunasekaran, Lai, & Edwin Cheng, 2008; Stevens & Johnson, 2016).

The demand for an integrated process by organisations, led to the creation of supply chains, which has been described by Yu, Ting, & Chen (2010) as a network that is made up of all the stages (e.g. purchasing, manufacturing, inventory control, distribution etc.) involved in the production and delivering of finished goods and services to consumers. Supply chains are made up of different structures and processes that are dynamically interrelated (Ivanov, Sokolov, & Kaeschel, 2010). These structures can be likened to an organisational structure, which involves decision-making activities that relate to the division of authorities, tasks and set of coordination mechanisms. The processes, on the other hand, involve the activities that include the planning, sourcing, manufacturing, delivering and returning of products (McCormack, Wilkerson, Marrow, Davey, Shah *et al.*, 2008). To make supply chain processes work optimally and their structures function efficiently, information must be acquired and shared.

Information is an essential component for improving the performance of supply chains because it provides organisations with the ability to better match supply with demand (Fu & Zhu, 2010; Seth, Goyal, & Kiran, 2015). It also serves as the foundation upon which decisions regarding the structure and processes of supply chains are made. According to Cherdantseva & Hilton (2013), performing organisational transactions and activities requires the sharing of information among trading partners. Hence, supply chain trading partners are increasingly sharing information among themselves, especially because of the realisation that when there is sufficient information within the supply chain network, the organisations within the network can make better decisions which bring about an improved operational performance. Also, ensuring a smooth transition of resources within supply chains and being able to manage the complexities involved in the production of goods and services requires that information is exchanged within the supply chain network.

For information sharing to be effective, organisations are using information systems such as Vendor Management Inventory (VMI), Electronic Data Interchange (EDI), Customer Relationship Management (CRM), Enterprise Resource Planning (ERP) etc. that can enable and enhances supply chain relationships and the acquisition, sharing, use and management of information (Gunasekaran *et al.*, 2008; Piderit *et al.*, 2011). Currently, there is a global increase in the dependency and use of information systems. This is because information systems have become globally connected, and hence, are making it possible for organisations to merge information from various sources for the purpose of making informed decisions, improving the integration of trading partners and increasing the responsiveness of the supply chain (Seth *et al.*, 2015). However, the global interconnection of information systems is also causing an increase in the vulnerability of information to attacks by globally dispersed threats (Fuchs, Pernul, & Sandhu, 2011; Hamill, Deckro, & Kloeber Jr, 2005).

The information shared in today's supply chain networks is getting complex and also becoming exposed to risks that pose a huge challenge to the performance of supply chains (Ho, Zheng, Yildiz, & Talluri, 2015). Organisations are continuously looking for means of reducing information risk. They are also increasingly seeking assurance on information and information systems so as to sustain the processes and activities of their businesses (CESG, 2010). This is because, when assurance of information and information systems are provided, accurate and complete (as much as possible) information and reliable information systems are made available to decision makers. According to Bunker (2012), organisations are still, however, faced with the challenge of using an approach that is practical and cost-effective in the management of information and information system risks, and in the provision of assurance on the confidentiality and integrity of information, and the reliability and performance of information systems.

1.2 Background

In the manufacturing environment of the 1980s, experts in logistics took the concept of material management a step further by incorporating transportation and distribution functions (Omar & Ballal, 2009; Tan, 2001). During this period, manufacturers also experimented with forming strategic partnerships with their immediate suppliers. The incorporation of transportation and distribution functions and the forming of partnerships by manufacturers resulted in the formation of integrated logistic processes (Tang, 2006). These processes, however, brought about changes that intensified the already existing competition among organisations. As competition intensified, markets started becoming global, organisations then began to realise that delivering the best values with minimal cost to consumers is not associated with their internal functions, structure or processes only, but also involves their trading partners (Prajogo, Oke, & Olhager, 2016). They also became conscious of the fact that their survival in the competitive market requires the seamless sharing of raw materials, money and information with their trading partners.

The realisation of organisations that it is important to share resources among trading partners, led to the formation of an integrated sourcing, production and distribution process called supply chain (Braziotis, Bourlakis, Rogers, & Tannock, 2013; Yu *et al.*, 2010). The forming of supply chains made it possible for organisations to form trading networks that consist of interconnected components, in which the members of the network complement each other's deficiencies and share benefits and losses. Traditionally, the parties within supply chains interacted in a disconnected manner that led to the sporadic movement of resources (i.e. materials, information and funds) across the supply chain (Lambert & Cooper, 2000). McCormack *et al.* (2008) also stated that in the past, trading partners within supply chains were mostly concerned with the management of inventory and the reduction of cost. However, in the early stages of supply chain, organisations were more focused on improving their production planning and inventory management, so as to ensure the efficient utilisation of machinery and capital (Stevens & Johnson, 2016).

Over the years, supply chains has emerged or evolved for reasons such as the emergence of a new market (e.g. Smart and HDR TV), response to technological breakthrough (e.g. 3D printing and bendable displays) or the establishment of a new geographical market (e.g. China and Africa) (MacCarthy, Blome, Olhager, Srai, & Zhao, 2016). The emergence and evolution of supply chains have enabled organisations to engage profitably in trade and commerce, exploit natural resources and meet the different consumer needs. Eamonn & Kelly (2015), showed that supply chains have evolved into value webs that are helping organisations manage existing and potential risks, improve their service level and reduce their operational costs. Different factors, as seen in Figure 1.1, has been identified to be stimulating the emergence and evolution of supply chains. Some of these factors are exogenous (e.g. policies and regulations) while some are endogenous (e.g. procurement and distribution strategies) (MacCarthy *et al.*, 2016). These factors are not mutually exclusive. Hence, technology advancements may cause a supply chain to evolve while at the same time, change in policies and regulations may also be a strong factor in the evolution of the same supply chain.

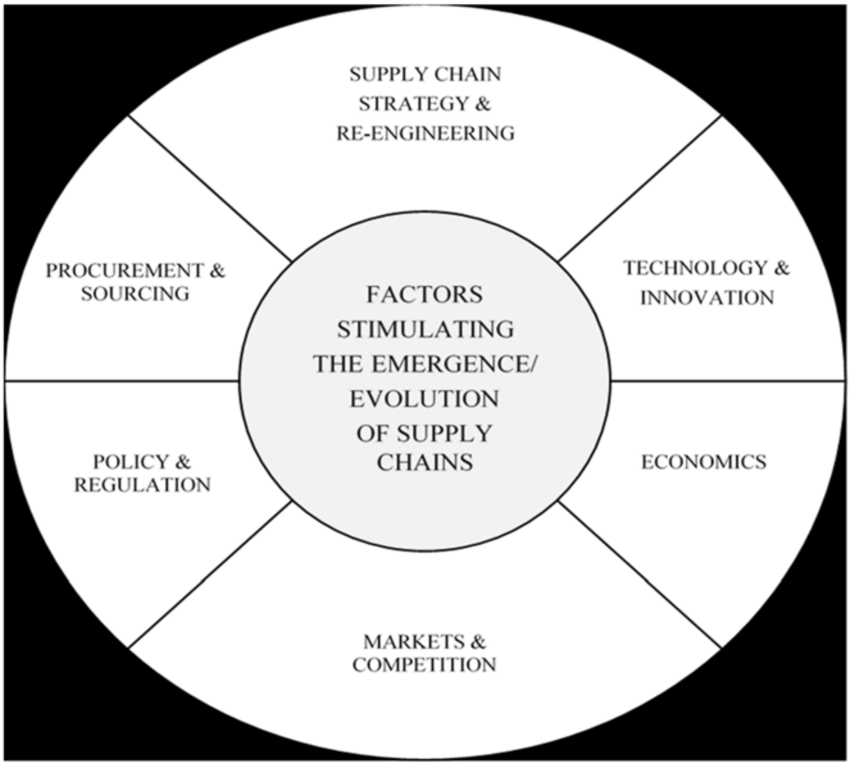


Figure 1.1: Factors stimulating supply chains' emergence/evolution (MacCarthy *et al.*, 2016)

The evolution and continuous emergence of supply chains brought in an era where suppliers, manufacturers, distributors and consumers are no more managed in isolation but as complex networks that are linked throughout the entire process involved in the acquisition of raw materials from their sources, transformation of the raw materials into finished products and the delivery of the finished product to consumers (Ardalan, Karimi, Naderi, & Arshadi Khamseh, 2016; Spekman, Davis, & Ellinger, 2016; Wang, Mastragostino, & Swartz, 2016b). According to Vilko, Ritala, & Edelmann (2014), this evolution, emergence and increasing length of supply chains have also caused an increase in the length, complexity and vulnerability of the materials, funds and information used within supply chains. Similarly, as explained by Huang, Li, & Ho (2016), the degree and level of information sharing among supply chain trading partners have increased, and this consequently, has increased the possibility and vulnerability of information to different types of distortions, disruptions and risks.

As the sharing of information and the other resources used within supply chains expanded, organisations felt the need to adopt information systems and technologies to facilitate and enhance the sharing of information, and the integration with their trading partners (Denolf, Trienekens, Wognum, van der Vorst, & Omta, 2015). Information systems played an important role in the early stages of the emergence and development of supply chains (MacCarthy *et al.*, 2016). They facilitated the separation of information from the other resources used in the production and distribution of goods and services. According to Hinkka, Främling, & Tätilä (2013), they were used to improve information quality, operational efficiency, service level and the agility of the traditional supply chain. However, as technology continued to evolve, trading partners began facing challenges of the continuous exposure of their information to different threats (Fuchs *et al.*, 2011). Trading partners are also now faced with the challenge of interconnectivity between their respective information systems (Mittelstädt, Brauner, Blum, & Ziefle, 2015).

1.3 Problem Statement

In order to provide an efficient and effective supply chain that can meet consumers' needs, the information acquired within the supply chain must be shared amongst the supply chain's trading partners, using information systems (Gunasekaran *et al.*, 2008; Ho *et al.*, 2015; Yu *et al.*, 2010). This is necessary because the performance of information within a supply chain depends on the information system that provides support to it within the supply chain (Denolf *et al.*, 2015).

Global supply chains are expanding, and this expansion is exposing the major supply chain resources (i.e. information, material and fund) to various security vulnerabilities, disruptions and risks (Hasani & Khosrojerdi, 2016). Information systems as well, have increased supply chains' complexity thus causing information to be exposed to different threats and risks (Jain, Wadhwa, & Deshmukh, 2009; Jouini, Rabai, & Aissa, 2014). If these risks are not properly managed, disruptions that endanger the overall performance, processes and structures of the supply chain may occur.

The exposure of information and information systems to different threats and risks is forcing trading partners to seek assurance that the information and information systems within their supply chain network are adequately protected and also performs as advertised (Bunker, 2012). To understand how the assurance sought by supply chain trading partners can the provided, this study investigated information and information systems' security within supply chains' structures and processes. The study also investigated how information assurance objectives (Confidentiality, Integrity, Availability, Authentication and Non-Repudiation) can be achieved optimally within supply chains. Finally, the study proposes an information assurance model that if adopted by decision makers within supply chains, could enable them to sustain their respective functions within the supply chain network. In order to ensure a proper investigation and to obtain a detailed outcome in this study, the problem statement has been further decomposed into the following sub-problems.

1.3.1 First sub-problem

Information, whether in a static state or being shared within the supply chain need to be treated as an asset, not just a commodity (Olivier, von Solms, & Cowley, 2006). To enable the continuous flow of the processes within the supply chain, and to also reduce supply chains' risks, the information collected by each organisation within the supply chain should be shared with their trading partners. For information sharing to be successful, an information system for sharing information along the supply chain is essential (Gunasekaran *et al.*, 2008; Yu *et al.*, 2010). In order to have a proper understanding of the role of information within the supply chain, and to also understand how information can adequately flow within the supply chain, supply chain information and information systems were investigated.

1.3.2 Second & Third sub-problem

The emergence of an extended manufacturing and a globally dispersed organisation has brought a new dimension to how organisations coordinate their processes that deal with information and material flow across the supply chain (MacCarthy *et al.*, 2016). The effective use of information provide supply chains with a competitive advantage, while if misused or not well managed could lead to an immense financial loss or even worse, the destruction of the overall supply chain (Ajayi & Maharaj, 2010; Olivier *et al.*, 2006; Workman, Bommer, & Straub, 2008). Fuchs *et al.* (2011) stated that the high dependence on information system is increasing the vulnerability of information to disruptions and risks. These disruptions and risks are causing organisations to seek assurance that information and information systems are adequately secured. In order to understand how the assurance of information and information systems' security within supply chains can be guaranteed;

- This study investigated information and information systems' security within supply chains.
- The study examined information assurance objectives and also investigated how they can be ensured so as to improve the various structures and processes within supply chains.

1.4 Research Objectives

The main objective of the study is:

- To propose an information assurance model that can enable organisations protect and sustain their respective information within the supply chain structures, and that can also enable them to minimise or prevent the risks that information within the supply chain processes could be exposed to.

To accomplish the main objective, the study has four primary objectives which are:

i. To understand the role of information and information systems within supply chains.
ii. To understand how information is shared, and also, the impact of sharing information within the various processes and structures of the different components of supply chains. This was done by also investigating the information systems used for sharing information.
iii. To identify and understand the issues and challenges surrounding the security of information systems, and also, information, as it moves through the various supply chain structures and processes.
iv. To understand information assurance as a concept and evaluate its objectives, and also identify how it can facilitate a smooth supply chain process and an efficient and effective supply chain structure.

1.5 Research Questions

After consulting with practitioners in the field of supply chain, and after reviewing the literature, as well as the problem statement and objectives of this study, the following key research questions were identified:

- What is the role of information and information systems within supply chains?
- How does sharing information impact on the supply chains’ structures and processes?
- How do information systems affect the sharing of information within supply chains?
- What are the security challenges faced by information systems and information, as it moves through the supply chain?
- How are information assurance objectives (availability, integrity, authentication, confidentiality, and non-repudiation) ensured within the supply chain?
- How is information assurance provision for protection, detection, reaction or restoration incorporated into the supply chain structures and processes?
- How is information assurance facilitating a smooth supply chain process and an efficient and effective supply chain structure?

1.6 Research Methodology

In order to get the views of the personnel from all the relevant parties involved with information and information system security within supply chains, and also tap into the experience of general supply chain and information assurance professionals, a qualitative research methodology was implemented in this study. This methodology was deemed appropriate because it provides a rich account of the phenomenon being investigated (Smith, 2015), and also helps the researcher understand the topic being investigated, from the participants’ perspective (Rosenthal, 2016). The research was done using an exploratory and case study approach, and the methodology was implemented through:

- Interviews
- Desk-based research (risk profile analysis of organisations, through document analysis)

This section is covered in detail in the document’s methodology chapter (i.e. chapter 5).

1.7 Motivation for Research

The literature shows that information is one of the major components influencing the performance and success of supply chains. This is because it serves as a lubricant to other components within the supply chain and also because it increases supply chains’ process and operational efficiency (Seth *et al.*, 2015). Trading partners are increasingly sharing information within their supply chain networks so as to ensure that the different structures and processes within their supply chains are synchronised (Denolf *et al.*, 2015; Koçoğlu, İmamoğlu, İnce, & Keskin, 2011; Li & Lin, 2006). However, as information is shared, its variability increases and it gets cumulatively delayed. It also becomes vulnerable to attacks, distortions and disruptions that pose a huge risk to the supply chain’s performance. According to Stevens & Johnson (2016), information vulnerability, distortion and disruption has become a major challenge to organisations in the twenty-first century. Hence, trading partners are increasingly seeking information security assurance (CESG, 2010).

This research was motivated by the following (as identified in the literature and also in consultation with practitioners in the field):

- The need to understand and identify the factors causing the vulnerability of information to different distortions, disruptions, threats and risks, when either in a static state or when being shared within supply chain networks.
- The need to explore and understand the severity and negative impacts of supply chain information risks on the performance, processes and structures of supply chains.
- The demand by supply chain practitioners to understand how assurance (from threats and risks) can be provided for the information and information systems used within supply chains.

1.8 Significance of Study

The main objective of this study is to propose an information assurance model that can enable organisations protect and sustain their respective information within the supply chain structures, and that can also enable them to minimise or prevent the risks that information within the supply chain processes could be exposed to. To achieve this main objective, other primary objectives were considered. These primary objectives include, understanding the role of information within supply chain structures and processes, understanding how effectively information systems are used to facilitate information sharing, and understanding how assurance of information and information systems' security can be ensured within supply chains. The findings of this study is therefore of significance to supply chain organisations in the following ways:

- ➢ The study will help supply chain organisations better understand how information flows within their supply chain network.
- ➢ The study provides an understanding of how information systems can be used to effectively share information within supply chains.
- ➢ The study provides an understanding of information vulnerabilities and the threats that could exploit those vulnerabilities, and also, the risk that the threat exposes information to when shared within the supply chain.
- ➢ The study provides an understanding of how assurance of information and information systems' security can be provided or ensured within supply chains'.
- ➢ The study provides an evaluation of the impact of information, information systems and information assurance within supply chains, supply chains' structures and processes.
- ➢ Finally, an information assurance model that if adopted by decision makers within the supply chain can enable them to sustain their respective functions within the supply chain network is proposed.

1.9 Structure of the Thesis

In order to ensure a proper and detailed presentation of the literature that are related to the topic being investigated, and to also ensure a proper and detailed presentation of the findings of this study, this dissertation has been divided into seven chapters.

In *chapter 1*, an overview of the study is presented. The overview covers an introduction to the study and a brief discussion on the background of supply chains and the role of information in the expansion of supply chains. The chapter also presents the objectives, motivation and significance of the study. Furthermore, the chapter presents the problem statement, research questions and a brief description of the methodology used in the study.

The literature review on supply chains, supply chain networks, structures and processes are presented in *chapter 2*. The chapter also presents the literature review on supply chain disruptions, risks and risk management. The chapter concludes by reviewing and presenting the literature on the overall management of supply chains.

In *chapter 3*, a review of the literature on the role of information, information sharing and the information systems and technologies that support the processes and structures of supply chains are presented. The chapter also presents some common information systems and technologies and their functions in optimising the processes, structures and performance of organisations and their supply chains.

Chapter 4 presents a review of the literature on some common threats to supply chains' information and information systems. Information and information systems' risks and security within supply chains are also presented in this chapter. The chapter also presents some technical and non-technical security measures that can help in managing supply chains' information and information systems' threats and risks. The chapter concludes by reviewing and presenting the literature on information (and information system) assurance, as applicable within supply chains.

The methodology underpinning the research for this study is presented in *chapter 5*. The chapter begins by presenting the research design. This is followed by the explanation of the sequence in which the research was conducted. The chapter also presents the criteria used in determining the organisations used as the point of data collection in the study. The analysis method used in the study and how the analysis method helps in interpreting and understanding the gathered data is also presented in this chapter.

In *Chapter 6* the frameworks used to underpin the study are presented. In the chapter, the application of the frameworks to this study is also presented. The chapter concludes by explaining how these frameworks are aligned to this study's research questions.

C*hapter 7* presents the findings from the analysis of the study's transcribed interviews. The demographics of the study's participants is also presented in the chapter. This is followed by the explanation of the representation of the organisations, and the employees drawn from the organisations, to participate in this study. The generated themes (i.e. main and sub-themes) from the analysed data are also presented in this chapter. The chapter concludes by presenting the relationship between the generated themes and the study's main research questions.

The discussion of the findings of this study in relation to the objectives of the study in presented in *chapter 8*. This chapter also presents the validation and modification of a developed framework called the "Supply Chain Information Risk Management" (SCIRM) framework developed in a previous study. The proposed model of this study, to help with supply chain information assurance, is also presented in this chapter. The explanation on how the findings of the study, the modified and validated framework and the proposed supply chain information assurance model can help supply chain organisations ensure and provide assurance on information and information system within supply chains is also presented.

Finally, *Chapter 9* concludes the study. This chapter also present areas of future research in the field of information security and assurance within supply chains.

1.10 Conclusion

In this chapter, an introduction into the study is presented. The chapter presents a brief overview of supply chain, information sharing and information systems within supply chains. It also presents the background, objectives, motivation and significance of the study. From this chapter, it may be concluded that the concept of supply chain is about coordinating the processes involved in the flow of information, materials and funds among trading partners, through a common set of established structures, processes, strategies and principles (Omar & Ballal, 2009). It is apparent that supply chains are experiencing changes that are driven by changes in consumer preferences, competition among organisations, the continuous evolution of technology and the increasing globalisation of trading markets (Seth *et al.*, 2015; Stevens & Johnson, 2016). These changes are causing existing supply chains to evolve and new supply chains to emerge (MacCarthy *et al.*, 2016). In chapter 2, the literature review on supply chain and its related activities and challenges are presented.

CHAPTER 2: OVERVIEW OF THE STUDY'S CONTEXT

2.1 Introduction

Today's supply chain environment has become a global environment that has not only provided organisations with different opportunities but also, with a number of challenges such as the disruption of supply sources, distortion of information and forecast inaccuracies that are increasingly affecting the processes and structures within supply chains, and also causing serious threats and risks to the manner in which supply chain organisations conduct their businesses (McCormack *et al.*, 2008; Piderit *et al.*, 2011; Wiengarten, Humphreys, Gimenez, & McIvor, 2016). The threats and negative impacts of supply chain disruptions and information distortion on the performance, processes and structures of individual organisations and their respective supply chains has made the topic of supply chain structures and processes, and also, the issue of supply chain disruption, distortion and risk, become of paramount importance to supply chain researchers and practitioners.

This chapter presents an overview of supply chain, supply chain networks, structures and processes. It also presents an overview of supply chain disruptions, risks and risks management. The chapter concludes by reviewing and presenting the literature on the management of supply chains. The layout of this chapter is presented in Figure 2.1.

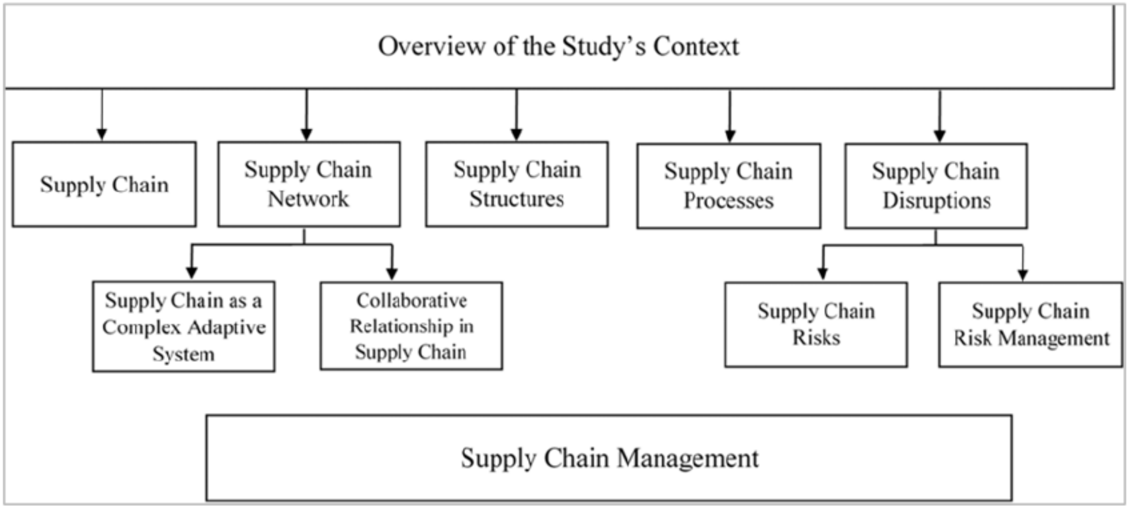

Overview of the Study's Context
Supply Chain
Supply Chain Network
Supply Chain Structures
Supply Chain Processes
Supply Chain Disruptions
Supply Chain as a Complex Adaptive System
Collaborative Relationship in Supply Chain
Supply Chain Risks
Supply Chain Risk Management
Supply Chain Management

Figure 2.1: Layout of the Chapter

2.2 Supply chain

A supply chain may be described as an integrated process wherein different organisations combine their efforts in acquiring raw materials, transforming the raw materials into finished products and delivering the finished products to the final consumers (Pop, Pintea, Pop Sitar, &

Hajdu-Măcelaru, 2015; Wang *et al.*, 2016b). It may also be described as a structure that is made up of different entities such as suppliers, production facilities, distribution centres, retailers and consumers, that are all connected through the downstream feed-forward flow of materials or services and the upstream feedback flow of information (Disney & Towill, 2003). Each of these entities has a responsibility in the planning and controlling of the movement of products or services and their related information, from one point to the other. According to Eamonn & Kelly (2015), supply chains are now being perceived as a concept that is evolving from being linear to becoming a value web (Figure 2.2) that connects the whole ecosystem of trading partners.

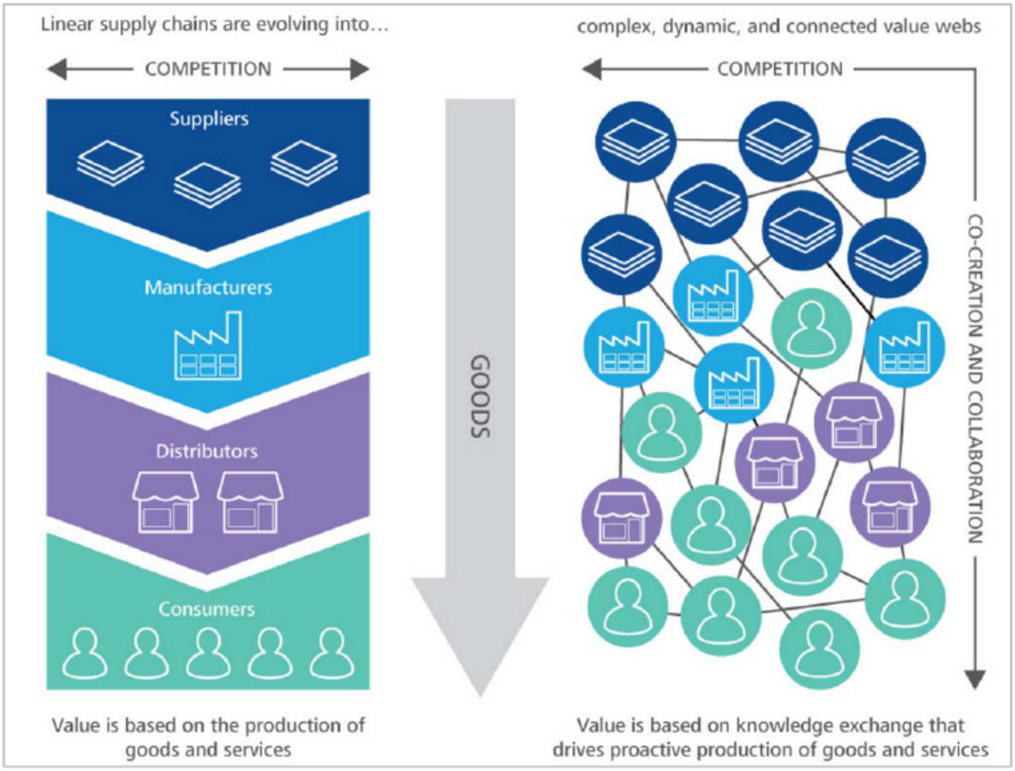

Linear supply chains are evolving into...
complex, dynamic, and connected value webs
COMPETITION
COMPETITION
Suppliers
Manufacturers
Distributors
Consumers
GOODS
CO-CREATION AND COLLABORATION
Value is based on the production of goods and services
Value is based on knowledge exchange that drives proactive production of goods and services

Figure 2.2: Linear supply chains evolving into dynamic value webs (Eamonn & Kelly, 2015)

Over the years, researchers and practitioners have developed different initiatives that have influenced or enhanced supply chains' activities, processes and practices. These initiatives, such as Efficient Consumer Response (ECR), Continuous Replenishment Program (CRP), Collaborative Planning Forecasting and Replenishment (CPFR), Quick Response (QR), Vendor Managed Inventory (VMI) etc. have been used to make information easily available to trading partners (Li, Fan, Lee, & Cheng, 2015; Pasandideh, Niaki, & Asadi, 2015; Tang, 2006). Some of these initiatives (e.g. ECR and QR) have enabled upstream suppliers to have real-time access and visibility into the point-of-sale and inventory information of the downstream retailers. While others (e.g. VMI) have enabled suppliers to determine the quantity and timing of replenishment for retailers as they (e.g. VMI) allows them (suppliers) to manage the inventory at retailers' site (Fu & Zhu, 2010).

Businesses of today are experiencing a paradigm shift in which they no longer compete amongst each other as solely an autonomous or independent entity, but instead as supply chains. Fang & Shou (2015) emphasised this paradigm shift in their study when they explained the dairy industry in China, in which, the two largest national players in the industry, China Mengniu Dairy Company Ltd and Yili Group Company, are in recent years, stiffly competing at a supply chain level. Another example of this paradigm shift can be found in the automobile industry, where Ford Motors (a U.S based automobile organisation), compete at a supply chain level against the German, Japanese and other US automobile manufacturers (Spekman *et al.*, 2016).

Over 42% of organisations manage or are involved in more than five different supply chains (Tang & Tomlin, 2008), some of which spans across the globe. This is as a result of their desire to meet up with consumers' needs. Today's supply chains have become globalised and longer, due to the continuous increase in the number of the organisations becoming trading partners. This increase in length is presenting new opportunities for trading partners. It is, however, also making supply chains become more complex and vulnerable to different types of threats, disruptions and uncertainties (Denolf *et al.*, 2015; Stevens & Johnson, 2016; Wiengarten *et al.*, 2016) that are not easy to manage or fully control (Vilko *et al.*, 2014).

Supply chain managers need to identify different supply chain alternatives that can prevent their organisation from losing integrity and value in the face of uncertainty or in the event that any of their trading partners encounter any form of disruption (Heckmann, Comes, & Nickel, 2015). The challenge though, is that there are not so many organisational practices or research that have presented supply chain alternatives or examined the relative effectiveness of the strategies adopted by organisations in the mitigation or prevention of the different vulnerabilities, disruptions and risks that supply chains are constantly being exposed to (Chang, Ellinger, & Blackhurst, 2015). Braziotis *et al.* (2013) and Govindan & Fattahi (2015) in their work, however, showed that one of the alternatives that can be implemented in mitigating or preventing supply chains' disruptions or risks is by establishing and ensuring a coherent and agile supply chain network.

2.3 Supply Chain Network

The literature shows that the traditional supply chain linear-based model has been challenged by organisations, and as a result, organisations are forming and increasingly moving towards a networked supply chain strategy that can facilitate the delivery of superior performance (Stevens & Johnson, 2016). The acceleration in manufacturing trends is also forcing supply chain trading partners to form agile supply chain networks that are adaptive, resilient and aligned to meet the needs of consumers. The forming of supply chain networks is enabling organisations to form close relationships and also increasing organisations' operational efficiency by enabling the acquisition and free flow of resources such as raw materials, information and funds, that are needed for the production of goods or offering of services to consumers (Seth *et al.*, 2015; Wang *et al.*, 2016b). These networks are, however, also causing organisations to go through intense global competition (Fang & Shou, 2015).

Organisations are transcending the boundaries of their intra-organisational processes, structure and systems and as a result, they are increasingly becoming part of an environment that is characterised by the network of trading partners and supply chains (Eskandarpour, Dejax, Miemczyk, & Péton, 2015). By forming supply chain network, organisations have been able to concentrate on their expertise and core competencies, while relying on other organisations for their non-core competencies (Gunasekaran *et al.*, 2008; Stevens & Johnson, 2016). Hence, organisations competitiveness is increasingly becoming dependent on the organisation's internal resources, external resources and the number of trading partners within the organisation's supply chain network. Similarly, the number of trading partners in a supply chain network has become a determinant of the amount of effort required in the coordination of the network's information and activities, and also a determinant in the improvement of the supply chain's performance (Denolf *et al.*, 2015).

Supply chain networks are inherently complex. This complexity is causing an increase in the amount and quality of information required to be shared among supply chain trading partners (Li & Lin, 2006). It is also impacting the establishment of a mutual relationship between supply chains' trading partners and also causing decision-making activities within supply chains to be a challenging problem (Pasandideh *et al.*, 2015). The number of participant, stages and the level of integration within supply chain networks increases the complexity of supply chains (Lemmens, Decouttere, Vandaele, & Bernuzzi, 2016). Hence, organisations such as General Electric (GE) and General Motors (GM) are reported to be reducing the number of suppliers they have, so as to reduce the complexities of their supplier network and also be able to effectively coordinate the activities with the other organisations within their supply chain network (Denolf *et al.*, 2015).

2.3.1 Supply Chain as a Complex Adaptive System (CAS)

The increase in supply chain reach has caused an increase in the number of nodes and connections within supply chain networks, and consequently, caused an increase in the exchanges and interactions among supply chains' trading partners. The exchanges and interactions that exist within the global supply chain network have made supply chains become a convoluted system to study and understand. Supply chains have been described as a complex system (Eamonn & Kelly, 2015; Holweg & Pil, 2008), and also, as a complex network (Lam, Choy, Ho, Cheng, & Lee, 2015; Li, Ji, Sun, & Lee, 2009) that comprises of many entities that are constantly interacting. The complex nature of supply chain networks suggests that supply chains have attained a level in which complex adaptive systems thinking is needed to provide additional insights into the complexities involved in the network and processes of trading partners.

One of the major challenges faced by supply chain organisations is to develop a supply chain structure that can facilitate a synchronised, flexible and adaptive behaviour in a complex and dynamic environment (Li, Yang, Sun, Ji, & Feng, 2010). By thinking of supply chain network as a complex adaptive system, organisations will be able to study and understand the dynamic behaviour and response capabilities of their supply chain network so as to learn and change from experience (Holweg & Pil, 2008). They will also be able to interpret the behaviour of the members of the network in a complete manner so as to develop interventions that will be efficient and effective. However, organisations should be cautious in the adoption of this thinking because according to Li *et al.* (2010), complex adaptive networks are difficult to understand because of the amount and level of interaction between its constituent entities.

Organisations' effort to manage supply chains has been frustrating because supply chain managers have struggled with the complex and dynamic nature of supply chain networks, and also, with the inability to easily control or predict their trading members (Choi, Dooley, & Rungtusanatham, 2001). Hence, authors such as Li *et al.* (2009), Li *et al.* (2010) and Capaldo & Giannoccaro (2015) suggested that there is a need to recognise and treat supply chain networks as a complex adaptive network. This is because complex adaptive systems are dynamic systems that can easily evolve and adapt to a changing market environment (Glenn-Mann, cited in Iñigo & Albareda, 2016). They are also considered systems "that emerges over time into a coherent form and adapts and organises itself without any singular entity deliberately managing or controlling it," (Holland, cited in Choi *et al.*, 2001, p.352). Treating supply chain as a complex adaptive system can help generate and improve the understanding of how to manage the overall supply chain network.

As explained in the work of Iñigo & Albareda (2016), complexity and systems-thinking have grown over the years to become an important concept and body of knowledge applied to the analysis of organisations' complex networks and systems. According to Capaldo & Giannoccaro (2015), a complex adaptive system comprises of a network of interacting and adaptive agents. "In the case of supply chain systems, the agents interact by exchanging information and physical goods" (Holweg & Pil, 2008, p.399). According to Choi *et al.* (2001) and Day (2014) as well, a complex adaptive system focuses on the co-evolution and interplay between a system and the environment in which the system operates. In the supply chain context, a system is regarded as a network of organisations that collectively share information and provide resources, products or services to a buying organisation, while an environment is regarded as the market space or sector in which the organisations operate.

2.3.2 Collaborative Relationship in Supply Chain

To increase supply chains' efficiency and competitiveness, supply chain trading members must establish a mutually beneficial collaborative relationship. Similarly, to create a supply chain network in which information is adequately and smoothly shared, Braziotis *et al.* (2013) and Kembro & Selviaridis (2015) explained that the supply chain trading partners should establish a collaborative network of relationship that closely links the different organisations within the supply chain. The collaborative relationship in supply chains is a potential differentiator that enhances forecast accuracy and the adequate sharing of information (Syntetos, Babai, Boylan, Kolassa, & Nikolopoulos, 2016). It can, however, be difficult to achieve because it comes with challenges that include establishing the criteria for selecting the organisations to collaborate with, and also, developing and maintaining the activities and relationships involved in the collaboration (Gunasekaran *et al.*, 2008).

Today's global supply chain environment is causing organisations strategic orientations to shift from being only competitive to also becoming collaborative. Since the mid-90s, practitioners and academics have strongly advocated for collaboration within supply chains (Ryu, Tsukishima, & Onari, 2009). This is because they understand that the supply chain that focuses on collaboration is in most cases more capable of implementing appropriate strategies that can help in the management of information and supply chain risks. Collaborative network and activities engage trading partners and facilitate the development of a responsive supply chain and the joint planning and processing of trading activities. This subsequently leads to an increased visibility of the supply chain's operational activities, and an increased free exchange of information within the supply chain (Koçoğlu *et al.*, 2011).

In order to induce collaborative relationships between manufacturers and retailers, the "Voluntary Interindustry Commerce Standards (VICS) association developed an initiative called Collaborative Planning, Forecasting and Replenishment (CPFR)" (Tang, 2006, p.478). Under the CPFR initiative, the retailer and the manufacturer are expected to jointly develop an information sharing mechanism, and also, a demand forecast process, that is mutually agreeable to both parties. Other initiatives such as Continuous Replenishment (CR) and Vendor Managed Inventory (VMI) have also been developed, so as to facilitate collaboration between supply chain trading partners (Ryu *et al.*, 2009). These initiatives often require commitments from trading partners.

They also require collaborating organisations to willingly and freely share information and to form a collaborative network and relationships that can enhance the delivery, design and conception of products and services (Braziotis *et al.*, 2013).

Organisations should adopt and establish collaborative relationships among themselves. This is because a collaborative relationship approach can be used as a supply chain risk management strategy that can help in the management of distortion to information and disruption to material flow (Braziotis *et al.*, 2013). It can also be used in facilitating the optimisation of supply chain processes. According to Li *et al.* (2015), the collaborative relationship and network adopted by organisations should be characterised by a long-term orientation and low levels of goal conflict. It should also be characterised by some level of outsourcing so that organisations can concentrate on their core competencies, so as to increase their competitive edge (Tuncel & Alpan, 2010). As explained in the study of Zhu (2016), outsourcing often requires the sharing of some private information with third party organisation. This information, if not properly managed could create uncertainties that may eventually cause or increase supply chain risks.

2.4 Supply Chain Structures

In the traditional supply chain structure, retailers have the responsibility of acquiring customers and at the same time take risks such as inventory risks, distribution risks etc. (Netessine & Rudi, 2004). However, with initiatives such as VMI and drop-shipping, the supply chain structure is changing. It is now expanding beyond organisations' processes, to include the organisations' trading partners (Hugos, 2010). According to Huang *et al.* (2016), supply chain structures should be built as a model that can evaluate the level of services offered to customers, with the aim of improving information performance and exchange between trading partners. Syntetos *et al.* (2016) presented a framework (Figure 2.3) that proposes a four-dimensional structure (i.e. location, product, echelon and time) for supply chains. The location dimension is essential in helping to provide information and forecast about transport planning, the product dimension is useful in transport planning as well as in warehouse planning, the echelon dimension is important in addressing all forecasting information and problems relating to inventory management, while the time dimension is important for all forecasting challenges, not just those relating to inventory.

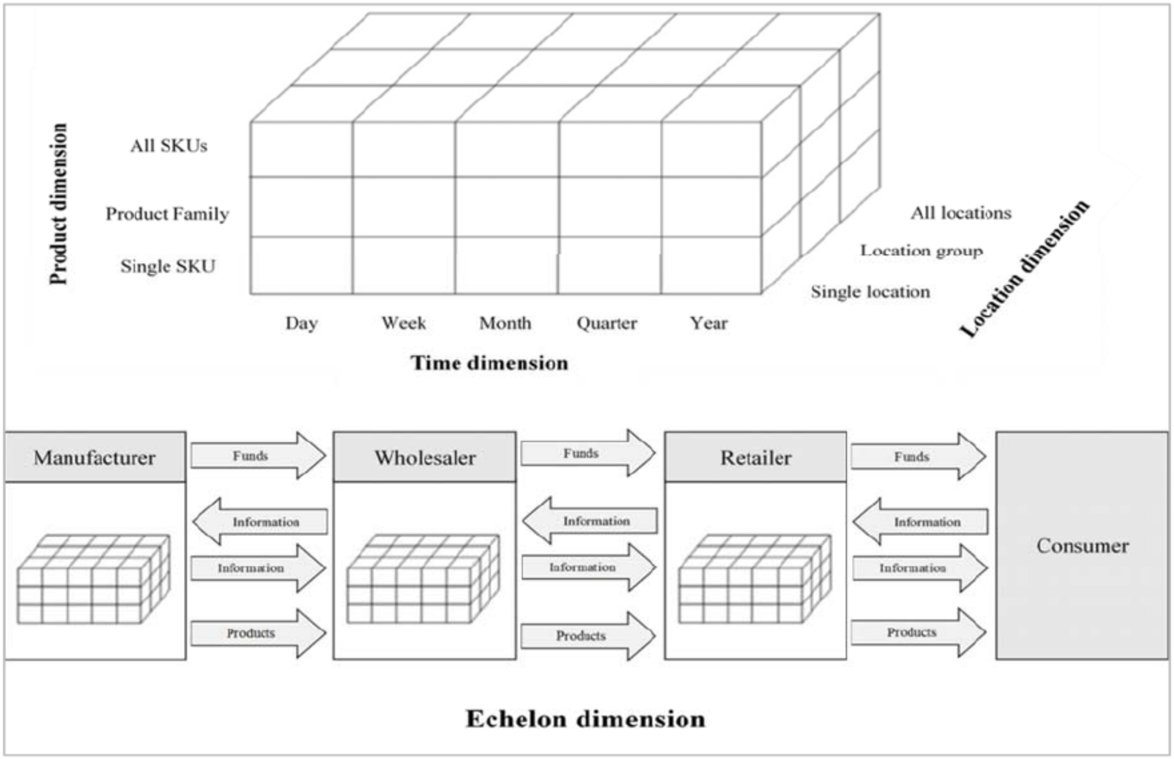


Figure 2.3: A Framework for Supply Chain Structure, adopted from Syntetos *et al.* (2016)

The supply chain structure has been described by Netessine & Rudi (2004) as a system in which the different organisations within the supply chain network make decisions concerning their respective functions within the supply chain. That is, manufacturers will be primarily concerned with decisions relating to production, while, wholesalers will be primarily concerned with decisions relating to inventory and retailers will be primarily concerned with decisions relating to consumers' acquisition. Hence, the level and how well a supply chain operates is a function of the structure of the organisations within the supply chain network. As stated in the work of Eckstein, Goellner, Blome, & Henke (2015), the structural flexibility of organisations is an important factor in the supply chain's ability to access resources and manage costs. However, according to Koçoğlu *et al.* (2011), the efficiency of the supply chain structure depends on the adequate sharing of information among the organisations within the supply chain network.

There are challenges in supply chains that are affecting the structural behaviour of the different supply chain components, and also making organisations re-evaluate and make changes to their supply chain structures (Neureuther & Kenyon, 2009). As explained in the study of MacCarthy *et al.* (2016), the structures of supply chains are being affected by economic and political factors, regulatory frameworks, strategic choices and technological drivers. Similarly, in the study of Wang & Disney (2016), sourcing, shipping and distribution activities were identified to complicate the structure of supply chains. The geographical dispersion of supply chain members has also been identified as a factor affecting supply chains' structures (Ivanov *et al.*, 2010; Piderit *et al.*, 2011; Syntetos *et al.*, 2016). This is because the geographic location of organisations influences how information is shared, how responsibilities are allocated and how decisions are made within supply chains.

According to Karimi & Davoudpour (2016), supply chain structure can be divided into the parallel and serial structure. In the parallel structure, each organisation within the supply chain works as a separate individual towards performing its functions and achieving its own objectives. While in the serial structure, each organisation performs part of each other's job functions so as to achieve the objectives of the different organisations within the supply chain. Serial structures are often high in complexity because of the inter-dependencies and inter-relation of trading members. Stevens & Johnson (2016) in their study also identified another structure called the centralised organisational structure. In this structure, organisations support the central goal of a networked supply chain. This structure, however, often leads to an inflexible structure that makes it difficult for organisations to cope with the challenges and turbulence of today's market environment (Braziotis *et al.*, 2013; Stevens & Johnson, 2016).

In the work of Lambert & Cooper (2000, p.71), supply chain structure has also been divided into horizontal and vertical structures. According to them (p.71), "Horizontal structure represents the number of tiers available across the supply chain. While the vertical structure refers to the number of suppliers and consumers represented within each tier." Ivanov *et al.* (2010) in their work also divided supply chain structures into different types, which are; organisational structure, functional structure, information/technological structure, financial structure, product structure and geographical/topological structure. According to them, these structures are all interrelated.

The prominent structures within supply chains that were identified in the literature are briefly described below:

Organisational Structure: This is associated with the structure of workers e.g. the directors, managers, workers etc. within an organisation. It is also concerned with the structure of the different trading partners that are members of a supply chain network. Organisational structure influences the environment in which supply chain trading partners operate. However, according to Denolf *et al.* (2015), supply chain organisations often have incompatible organisational structures that need to be properly integrated and managed, so as to operate in a coherent manner.

Functional Structure: In the work of Lambert & Cooper (2000), it was explained that organisations often emphasise the importance of functional structure. Functional structure relates to the structure of the business processes and management functions within the supply chain (Ivanov *et al.*, 2010). It is also concerned with the processes involved in the manufacturing and delivering of products or services to meet consumers' demands.

Product Structure: This is the structure that deals with the design and development of products, product variety, bill-of-material, demand etc. (Ivanov *et al.*, 2010). It also involves the network structure for sourcing, production and distribution across the supply chain (Lambert & Cooper, 2000).

Financial Structure: This is the structure that deals with the movement of funds within the supply chain. It also deals with costing, expenditure and the generation of profits (in some instances, loss) within the supply chain (Ivanov *et al.*, 2010). It is one of the structures that other structures depend on.

Informational Structure: Another important structure that other structures depend on, is the information structure. This structure involves the coordination strategy put in place by organisations to ensure that information is adequately and continuously shared between them and their trading partners (Ivanov *et al.*, 2010). It is also concerned with the frequency of information flow among supply chain trading partners (Lambert & Cooper, 2000).

The agility of supply chains in terms of structure impacts directly on an organisations ability to respond to consumers' needs (Eckstein *et al.*, 2015). It is, therefore, important for organisations to form an agile and coherent supply chain structure, because an agile and coherent supply chain structure help organisations attain an adaptive, resilient and responsive supply chain network (Eamonn & Kelly, 2015; Gunasekaran *et al.*, 2008; Lambert & Cooper, 2000). An agile supply chain structure is also important in determining how risks relating to the different supply chain components can be expressed. Furthermore, it is also crucial in influencing the selection of the strategy that can be used in the management of information and supply chain risks. However, according to Gunasekaran *et al.* (2008), the level of complexity in terms of processes, products and networks can significantly hinder the ability of organisations to form an agile supply chain structure. Also, according to Wiengarten *et al.* (2016), when rules are less specified and enforced, the supply chain and its structures are likely to be less agile.

2.5 Supply Chain Processes

A supply chain has been described as a complex network that integrates different business processes, such as distribution, manufacturing and procurement, so as to create value in the form of goods or services to consumers (Lam *et al.*, 2015; Li *et al.*, 2009). While supply chain management has been described as the management of the internal and external processes of an organisation's operations (Prajogo *et al.*, 2016). The literature shows that each supply chain has its own set of processes and operational activities. Davenport cited in Lambert & Cooper (2000, p.76) defined a process as “a structured and measured set of activities designed to produce a specific output for a particular customer or market.” Processes are an important determinant of how resources such as information, material and funds will flow within the supply chain, and also, how responsive a supply chain can be.

The agility of supply chain processes determines the ability of the supply chain’s trading partners to respond to consumers’ needs. Hence, today’s supply chain organisations are increasingly improving their business processes, internal operations and process control (Prajogo *et al.*, 2016). Business processes are fundamental links to the activities of all the trading partners within a supply chain network. In order to remain competitive, organisations, through supply chain innovations, are transforming their business processes and models (MacCarthy *et al.*, 2016). They are also increasing the efforts to improve and align their processes so as to meet the demanding expectations of today’s marketplace. The processes within an organisation and between the organisation and its trading partners have also been identified by Kolkowska & Dhillon (2013) as an important factor in determining how business values and norms are achieved.

One of the important issues that have gained attention among supply chain practitioners and researchers is the integration of processes (e.g. procurement, manufacturing, delivery etc.) within the supply chain network (Karimi & Davoudpour, 2016). The integration of processes within the supply chain is important because supply chain performance and competitiveness can be improved significantly if the processes within the supply chain network are properly integrated (Cherdantseva & Hilton, 2013; Denolf *et al.*, 2015; Yu *et al.*, 2010). According to Wiengarten *et al.* (2016), when the processes within the supply chain network are adequately integrated, information exchange among the trading partners is improved and thus, the flow of material and funds. Also, according to Stevens & Johnson (2016), an efficient supply chain performance can easily be achieved when processes are interacting and improving in an integrated manner, and not when isolated processes are improved or optimised.

Supply chain processes include performance measurement, customer relationship and service quality management, distribution, manufacturing, procurement and product development (Marinagi, Trivellas, & Sakas, 2014; Pérez-Aróstegui, Bustinza-Sánchez, & Barrales-Molina, 2015). These processes must be integrated in order to achieve an optimal supply chain performance. However, according to Lambert & Cooper (2000), integrating all the processes within a supply chain is probably not a good practice. This is because some processes within supply chains are more delicate than the others and organisations with such processes could lose a lot if anything goes wrong with the integrated processes. In the work of Wiengarten *et al.* (2016), it was also explained that integrating supply chain processes could be a problem because the tighter and more integrated the supply chain processes are, the more the severity of any disruptions that might affect the supply chain will be. Hence, according to Stevens & Johnson (2016), integration should be driven by information, behaviour and insight and not just by processes.

2.6 Supply Chain Disruptions

Over the years, civil unrest, economic crisis, earthquakes, tsunami, viral diseases (e.g. SARS and Ebola) etc. have caused repeated disruptions to the ways organisations conduct their businesses, and consequently, to the ways the activities and processes of supply chains are being performed (McCormack *et al.*, 2008; Mizgier *et al.*, 2015; Tang, 2006). According to Foulds (2015), disruptions are activities or events that interrupt the flow of information and materials between suppliers, producers and consumers. Similarly, supply chain disruption has been described by Porterfield, Macdonald, & Griffis (2012) and Chang *et al.* (2015) as the events or activities that interrupt the normal flow of resources such as information, materials and funds (within a supply chain) and products or services (to consumers). According to Wagner & Bode (2006), supply chain disruptions may also be described as unintended events or situations that often lead to the exposure of the organisations within the supply chain to different risks.

Global supply chains are getting longer and complex and hence more vulnerable to different uncertainties and disruptions. According to Mizgier *et al.* (2015), it is difficult to make predictions about disruptions that could occur in today's global supply chains. This is because of the dispersion of the sources of disruptions, the dynamic nature of supply chains and the growing expectations and demands of consumers. According to Chang *et al.* (2015), the length, complexity and dynamic nature of a supply chain determines the extent of disruptions that information, material and knowledge could experience as they travel through the supply chain. In a shorter supply chain, information and material have a lesser chance of getting delayed, distorted or disrupted, while in a longer supply chain, the chances of information and material getting disrupted, distorted or delayed are very high.

Disruptions can have a serious impact on the performance of the overall supply chain. This can be seen in the case of Japan's global merchandise, which fell by 14.5%, when the country was hit by tsunami, in 2011 (Hasani & Khosrojerdi, 2016), and also in the case of computer manufacturers whose hard discs supply chains (based in Thailand) was disrupted, when the 2011 flooding of Thailand happened (Ho *et al.*, 2015). The impact of disruptions in supply chains can cause organisations to lose out on customers, operational costs and shareholders' value (Li *et al.*, 2015). The financial performance of organisations can be adversely affected by supply chain disruptions. These, for example, can be seen in the loss of 400 million Euros by Ericsson, after Philip's (their semiconductor supplier) plant caught fire (Ho *et al.*, 2015; Li *et al.*, 2015), and also, in the loss of customer orders by Apple during a DRAM chips supply shortage that was caused by an earthquake that hit Taiwan in 1999. These organisations (Ericsson and Apple) were negatively affected both in the short-term and long-term manner.

According to Clemons & Slotnick (2016), even with ample warning, it is difficult to prevent or completely avoid supply chain disruptions. Sources of supply chain disruptions can either be internal, that is, within the supply chain network (e.g. unreliable supplier, uncertain demand, sharing of inadequate information, etc.) or external, that is, outside the supply chain network (e.g. strikes, civil unrest etc.). It could also be as a result of unstable consumer demands, uncertain economic cycles, manmade disasters, or the use of unskilled labour to perform the operations and activities of the supply chain (Ryu *et al.*, 2009). As shown in the work of Gunasekaran *et al.* (2008), the factors affecting supply chains' exposure to disruptions also include: the number of transportation mode, the extent of geographical areas that the supply chain covers, the borders and political areas included in the supply chain network, and the degree of usage of technical infrastructure for managing the supply chains' information.

It is important for trading organisations to establish adequate strategies that can help deal with supply chain disruptions. However, not so many organisations have detailed strategies, plans or measures in place to deal with disruptions in supply chains (Shao, 2013). To deal with supply chain disruptions, organisations should implement strategies that include having alternative or multiple sources of supply, holding safety stock or purchasing insurance (Clemons & Slotnick, 2016; Hasani & Khosrojerdi, 2016). Authors such as McCormack *et al.* (2008), Mizgier *et al.* (2015), Foulds (2015) and Lemmens *et al.* (2016) have also suggested that, to deal with supply chain disruptions, trading organisations should create resilient supply chains that can anticipate disruptions and risks, limit the impact of disruptions and risks, and quickly return the activities and processes of the supply chain to their previous or even a better state.

2.6.1 Supply Chain Risks

Organisations are reacting to the opportunities of globalisation by engaging in various global practices such as outsourcing, collaboration and partnerships that are increasing supply chains' exposure to different vulnerabilities, threats and risks (Vilko *et al.*, 2014; Wiengarten *et al.*, 2016). Hence, today's supply chains are increasingly and continuously being exposed to different supply chain risks. Supply chain risk has been described as "the likelihood and impact of unexpected macro and/or micro level events or conditions that adversely influence any part of a supply chain, leading to operational, tactical, or strategic level failures or irregularities" (Ho *et al.*, 2015, p.5035). It has also been described as the negative deviation caused by disruptions that threaten the regular activities and processes within a supply chain (Chang *et al.*, 2015). The detrimental consequences of supply chain risks are intense on supply chain organisations.

It is important to have a good understanding of the inherent risks that supply chains could be exposed to (Mizgier *et al.*, 2015). Similarly, organisations are realising that it is important to understand the varieties and interconnectedness of the different types of risks that their supply chain could be exposed to, as this will enable them to develop effective risk management strategies that can be tailored to suit the overall supply chain (Chopra & Sodhi, 2004). This realisation is also making practitioners and researchers pay more attention to supply chain risks and their impact on the performance and operational continuity of supply chains (Li *et al.*, 2015). Mizgier *et al.* (2015) noted that the increasing attention being paid to supply chain risks by practitioners and researchers is as a result of the rise in the disastrous events (natural and human) happening around the globe and that are causing distortion to information and disruptions to global supply chains.

Three aspects of supply chain risk were identified in the literature, and they are:

Operational risk – Operational risks are the inherent uncertainties in the day-to-day operations of supply chains. According to Vilko *et al.* (2014), the operational failure of information system and supply chain is an increasing concern to logistics and supply chain organisations. Uncertain supply and consumers' demands, internal unrest, failure or loss of key supplier, product quality problems are examples of risks that may have severe impacts on the operations and performance of supply chains (Chang *et al.*, 2015).

Cost risk – According to Lemmens *et al.* (2016), this is the type of risk incurred in the running of the supply chain processes and activities. It is also sometimes referred to as financial risk. Franca *et al.,* as cited in Lemmens *et al.* (2016) described the financial/cost risks associated with supply chains as the likelihood of the objectives of cost or profit not meeting their target level. According to Ho *et al.* (2015), there is still a research gap in the domain of financial risk, especially within supply chains.

Reputational risk – According to Roehrich *et al.,* cited in Petersen & Lemke (2015, p.498), reputational risk is "the cumulative likelihood that events stemming from exogenous or endogenous sources can occur and negatively impact stakeholder perceptions of the firm's behaviour and performance". If the reputation of any organisation within the supply chain is affected, it could potentially affect the holistic supply chain in a manner that poses a threat to all the members of the supply chain. Hence, it is important for today's organisations to have a clear visibility of the integrity and activities of their trading partners, so as to avoid reputational demand.

Ho *et al.* (2015) categorised supply chain risk into two, and they are; the micro-risk and macro-risks. According to them, the micro-risks are the recurrent risks such as operational risks (e.g. supply and demand risk) that originate directly from an organisation's internal activities or its relationships with other organisations within the supply chain. While macro-risks are the external events such as natural risks (e.g. tsunami and earthquakes) and man-made risks (e.g. political instability, terrorism and war) which have greater negative and adverse impact on organisations. Mitroff and Alpaslan, cited in Wiengarten *et al.* (2016), also identified three categories of risks to supply chains, and they are; the normal risks (e.g. technology breakdowns or failure), the abnormal risks (e.g. ill-will by outsiders or insiders) and the natural risks (e.g. earthquakes, fires etc.).

Supply chain organisations are constantly being exposed to different risks, and according to Hamill *et al.* (2005, p. 472), "a risk accepted by one is a risk imposed on all." Supply chain practitioners are therefore emphasising that there is a need for an effective strategy that can facilitate the anticipation, identification, assessment and management of risks. Chopra & Sodhi (2004) stated that organisations like Motorola, Toyota and Dell have created strategies of identifying and managing their supply chains risks. These strategies, however, are dependent on the likelihood and severity of the risks events. The risks that exist throughout supply chains have made decision-making a challenging problem, to such an extent that, supply chain practitioners now consider decision making regarding the management of supply chain risks an integral part of their job (Li *et al.*, 2015). As explained in the work of Wiengarten *et al.* (2016), organisations are now investing in contingency plans and implementing mitigating practices that can facilitate the management of the various types of risks that their supply chain could be exposed to.

2.6.2 Supply Chain Risk Management

Supply chain risk management is one of the most important topics to supply chain practitioners and researchers because it has become an important domain that continues to present global challenges to organisations and supply chain managers (Chang *et al.*, 2015). It has, however, also become important because it helps organisations proactively mitigate risks or reactively respond to them by facilitating the implementation of appropriate actions that can help contain or avoid vulnerabilities and threats in supply chains (Vilko *et al.*, 2014). Supply chain risk management is described by McCormack *et al.* (2008, p.8) as "the systematic identification, assessment, and quantification of potential supply chain disruptions with the objective to control exposure to risk or reduce its negative impact on supply chain performance." It is also described by Narasimhan & Talluri (2009) as the strategic management activities that can affect the operational performance of organisations, if not properly implemented.

Tang (2006) stated that management of supply chain risks requires the adoption of strategies that can help with supply management, demand management, product management and information management, and also, that can help with the coordination of upstream partners so as to ensure an efficient supply of materials, and downstream partners so as to influence demand and demand information on a regular basis. However, as stated in the work of Li *et al.* (2015), differences in organisational goals and information asymmetry could jeopardise the strategies used in the management of supply chain risks. To reduce risks and increase the effectiveness of supply chain trading partners, the activities within the supply chain network should be balanced and coordinated. one of the ways of coordinating supply chain activities is by having a written contract that will explicitly define the roles and responsibilities of each organisation within the supply chain (Denolf *et al.*, 2015).

The less specified or complete a contract is, the less successful the attempt at managing supply chain disruptions and risks may be. According to Koçoğlu *et al.*, (2011) and Eamonn & Kelly (2015), one of the factors that can help in strengthening contracts and their duration among trading partners is the establishment of a trust-based relationship. In the work of Li *et al.* (2015), two supply chain risk management practices were identified. These practices (described below) often requires the development and use of contracts such as revenue sharing contracts, quantity-base contracts etc., by supply chain trading partners.

Risk Information Sharing: This practice requires that organisations and their trading partners share their respective supply chain risk information in an accurate and timely manner. This practice helps organisations identify possible vulnerabilities within the supply chain and develop the possible corresponding measures. Also, when actual supply chain risk occurs, this practice provide organisations with accurate and timely information on the status and possible impacts of the risk. This practice also helps ensure visibility within the supply chain.

Risk Sharing Mechanism: This practice involves a situation in which an organisation aligns to the obligations and incentives among the supply chain trading partners, regarding how the duties to manage supply chain risks is shared and how they (the organisation and its trading partners) face the consequences of supply chain risks. This practice involves the use of formal policies and arrangements (e.g. contracts).

Chang *et al.* (2015) stated that organisations should devote resources to the management of risks, however, they should ensure that the benefits of doing so outweigh cost. Managing supply chain risk leads to the reduction of uncertainties and the impact of disruptions. It also helps in the improvement of supply chain operation and performance. However, to manage the risks that supply chains faces, supply chain trading partners "need to be adaptive to market dynamics," (Tang & Tomlin, 2008, p.15). The management of supply chain risk can be approached in three phases (Lam *et al.*, 2015; McCormack *et al.*, 2008), and in the work of Tuncel & Alpan (2010), a fourth phase (i.e. *risk monitoring*) was added. According to Ho *et al.* (2015), these phases (Figure 2.4) should ensure that disruptions, micro-risks (majorly, operational risks) and macro-risks (majorly, catastrophic risks) – explained in section 2.6, are monitored and managed. Also, that the risks to supply chains' resources (i.e. information, material and funs) and activities are quickly identified and managed appropriately. The supply chain risk management phases are explained after the Figure 2.4.

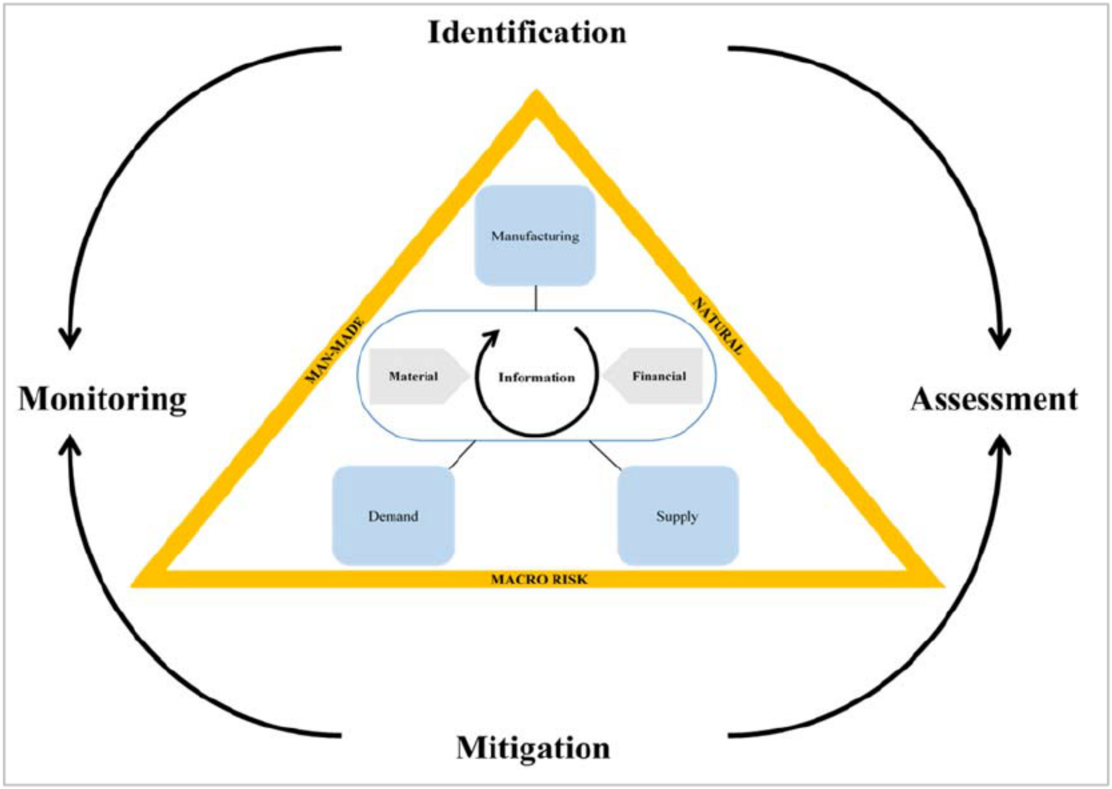


Figure 2.4: Supply Chain Risk Management Phases, adopted from Ho *et al.* (2015)

<u>*Risk Identification*</u>: This phase of supply chain risk management involves creating a list of possible incidents that could cause disruptions to the supply chain's operations, performance and resources (i.e. information, materials and funds) (Ho *et al.*, 2015; McCormack *et al.*, 2008). It is important to identify and understand the risks affecting the business before deciding on any risk management strategy. Risk identification should be on an ongoing basis as this enables organisations to create plans that can help in managing risks before their occurrence (Tuncel & Alpan, 2010). It also helps organisations save cost because when organisations react rather than prevent adverse events, they tend to use more resource. With risk identification, questions such as; what is uncertain, what can go wrong, etc. are often asked by organisations (McCormack *et al.*, 2008). Risk identification methods include geo-mapping/supply chain mapping, information audits, looking at historical problems, site

visits, etc. (McCormack *et al.*, 2008). After risks have been identified, the next step is to quantify the identified risks through risk assessment.

Risk Assessment: This phase deals with understanding the possibility of a potential risk happening, and the impact the risk could have on the overall structure, processes and information of the supply chain. According to Narasimhan & Talluri (2009), before developing risk mitigation strategies, it is important to quantify and classify the nature of the risks affecting the business. The quantification of risks helps in determining the strategies that can best fit for mitigating the identified risks. The risk assessment phase enables organisations to prioritise the resources that are/will be used for managing risk. It also helps organisations in understanding and clarifying the risk nature, the frequency at which the risk events has occurred or is expected to occur and the conditions leading to the risk events. It usually involves two measures which are; likelihood (the possibility that a risk event will happen) and impacts (the consequences faced by an organisation if or when a risk event happens) (Tuncel & Alpan, 2010; Vilko *et al.*, 2014). While conducting a risk assessment, questions often asked include; what is the likelihood of the risk happening, what impact the risk would have on the organisation if or when it happens, etc. (McCormack *et al.*, 2008).

Risk Mitigation: As stated in the study of Tuncel & Alpan (2010) and Chang *et al.* (2015) risk mitigation in supply chain refers to an organisation's actions intended at reducing the probability of occurrence and the negative impacts of risks. In this phase, the appropriate measures for controlling, mitigating or preventing the occurrence or effects of risks are being chosen and implemented. According to McCormack *et al.* (2008), supply chain risk mitigation methods includes; having alternative suppliers, the adoption of Collaborative Planning Forecasting and Replenishment (CPFR) initiative, establishing strategic partnerships, etc. Risk mitigation also deals with questions such as; what approach should be used to monitor risks, what approach should be used to control risks, etc. (McCormack *et al.*, 2008). Chang *et al.* (2015) classified the strategies that can be used in mitigating supply chain risks into two categories which are; ***flexibility*** – focuses on building capabilities that can sense threats to supply chains and respond to them quickly, and ***redundancy*** – focuses on reducing the negative impacts of risk by ensuring product availability.

Risk Monitoring: This is considered the last phase in the management of risks. In this phase, the implemented measures for mitigating, preventing or controlling risks are being supervised. This phase could also help to detect risks before and when they occur. According to Ho *et al.* (2015) however, not so much attention is being given to this phase of risk management.

Risk management is an integral part of any business. Chang *et al.* (2015) stated that supply chain risk may be classified as acceptable, unacceptable and tolerable, and based on this classification organisations can implement strategies that can best help manage risks. According to Tang (2006), the management of risks in the supply chain requires that the partners within the supply chain network are able to access different types of private information that are available to the different partners within the network. Communication across the supply chain's functional units has also been identified by McCormack *et al.* (2008) as being fundamental in the identification of risks and also, in the determination of appropriate measures and actions that can be taken in the management of risks. Ho *et al.* (2015) stated that communication within supply chains' functional units can be easily established only when there is a clear definition of the roles of the respective supply chain members, and also, only when an adequate information sharing mechanism is established within the supply chain.

2.7 Supply Chain Management

Today's global and competitive market environment has caused an increase in the level of attention being paid to the material, funds and information being shared among supply chain trading partners. It has also made supply chain management become an important issue to trading partners. According to Lambert & Cooper (2000, p.66), supply chain management "is the integration of key business processes from end user through original suppliers that provides products, services, and information that add value for customers and other stakeholders". The management of supply chain has become an important strategic issue for organisations because when supply chains are properly managed, the activities starting from the creation of demand up to its fulfilment are properly controlled (Pedroso & Nakano, 2009). However, when supply chains are not properly managed, valuable resources such as funds and information could be wasted (Lambert & Cooper, 2000).

Since the 1990s, supply chain management has been receiving a lot of attention and definition from academics and different industrial practitioners (Gunasekaran *et al.*, 2008; Zhang & Chen, 2013). According to Pasandideh *et al.* (2015), it is still receiving attention from several organisations because it is considered an essential activity required for meeting consumers' demands. It is also considered a key determinant in achieving competitive advantage and performance. According to Yu *et al.* (2010), a successful supply chain management can be achieved when there is commitment of trading partners to the sharing of real-time information. This is because, supply chain management incorporates the movement of goods and the exchange of information between suppliers, manufacturers, distributors, retailers, consumers and any other organisations within the extended supply chain network (Gunasekaran *et al.*, 2008).

Supply chain management practices help with the management of the financial, information and material flow across the entire supply chain. They also help with the planning, controlling and monitoring of the supply chain network's activities, so as to achieve consumers' satisfaction and at the same time maximise profit. These practices provide the support needed by organisations in becoming collaborative and responsive. They also play an important role in minimising the inherent uncertainties within supply chains (Stevens & Johnson, 2016). According to Tuncel & Alpan (2010) however, supply chain management practices that do not put into consideration, vulnerability and risk issues, may have to deal with the inconsistent processes and flow of resources, that could lead to sub-optimal results.

In recent years, numerous research that investigated and suggested solutions on the major challenges and trends in the management of supply chains have been published. Results from these research show that the rapid transformation in business environments, the diversity in consumers' demands and the severe competition in today's markets are causing organisations to face challenges in the management of supply chain. The cost involved in the management of supply chains has also been identified by Gunasekaran *et al.* (2008) as a challenge facing organisations in the management of supply chains. In order to address the challenges faced in the management of supply chains, Li *et al.* (2015) suggested that supply chain organisations should work in an integrated manner, as this ensures the continuity of the management strategies put in place within the supply chain.

2.7.1 Supply Chain Integration

Supply chain management has seen a shift in focus from inter-functional integration to information and process coordination and inter-organisational integration. Hence, successfully managing the activities of the different organisations involved in the acquisition of information, funds and materials, and in the production and distribution of goods or services, requires the integration of the processes of the different organisations within the supply chain network (Lambert & Cooper, 2000; Wang *et al.*, 2016b). As explained in the work of Wiengarten *et al.* (2016), when the processes within the supply chain network are adequately integrated, the organisations within the network are able to access the capabilities and resources embedded within the other organisations in the network, and subsequently, able to increase their visibility and innovativeness. According to Stevens & Johnson (2016), having visibility within the supply chain network can help in the identification and management of potential threats and risks to the organisations within the network.

Supply chain integration may be referred to as the adoption and use of standards, practices, technology and information systems, among supply chain trading partners for the purpose of establishing a timely flow of information, funds, materials and finished goods and services (Koçoğlu *et al.*, 2011). According to Wiengarten *et al.* (2016), it is the extent to which an organisation strategically aligns and interconnects with the trading partners within its supply chain network. While, according to Stevens & Johnson (2016), it may be referred to as the coordination, linkage and alignment of information, processes, strategies and people across all points of contact within the supply chain, so as to ensure the effective and efficient flow of information, funds and materials, in response to consumers' needs. Supply chain integration has been categorised into three different types by Stevens & Johnson (2016), and they are:

Supplier integration: helps improve the operations of organisations and their supply base, by facilitating the sharing of information, streamlining the flow of products and enabling a collaborative relationship between organisations and their supply base.

Distribution integration: helps improve the management of resources and product flow, by increasing demand information visibility. With an integrated distribution, the organisational focus does not only include the efficient management of transport but also includes the development, planning and controlling of an effective forward and reverse storage and flow of products and their related information amongst the trading partners.

Customer integration: help organisations collaborate with customers so as to develop an agreeable forecast of demand and supply that can meet the needs of customers. Customer integration can be operationalised by CPFR.

Integration can be from an internal perspective, that is, when the different functional areas within an organisation's boundaries are integrated, or from an external perspective, that is, when the activities and processes of an organisation and its trading partners are integrated (Shao, 2013; Wiengarten et al., 2016). It is important to manage both the internal and external integration of an organisation, so as to facilitate the smooth flow of resources. According to Khalifehzadeh, Seifbarghy, & Naderi (2015) however, one of the most difficult challenges still facing today's supply chain is the integration of production and distribution activities among the trading partners. To manage these challenges, Steven cited in Stevens & Johnson (2016), suggested that organisations should progress through different supply chain developmental stages. These stages as shown in Figure 2.5 starts from a baseline of independent functional silos, and then moves gradually until the stage of full internal and external integration is achieved, where there is a seamless flow of resources among the supply chains' trading partners.

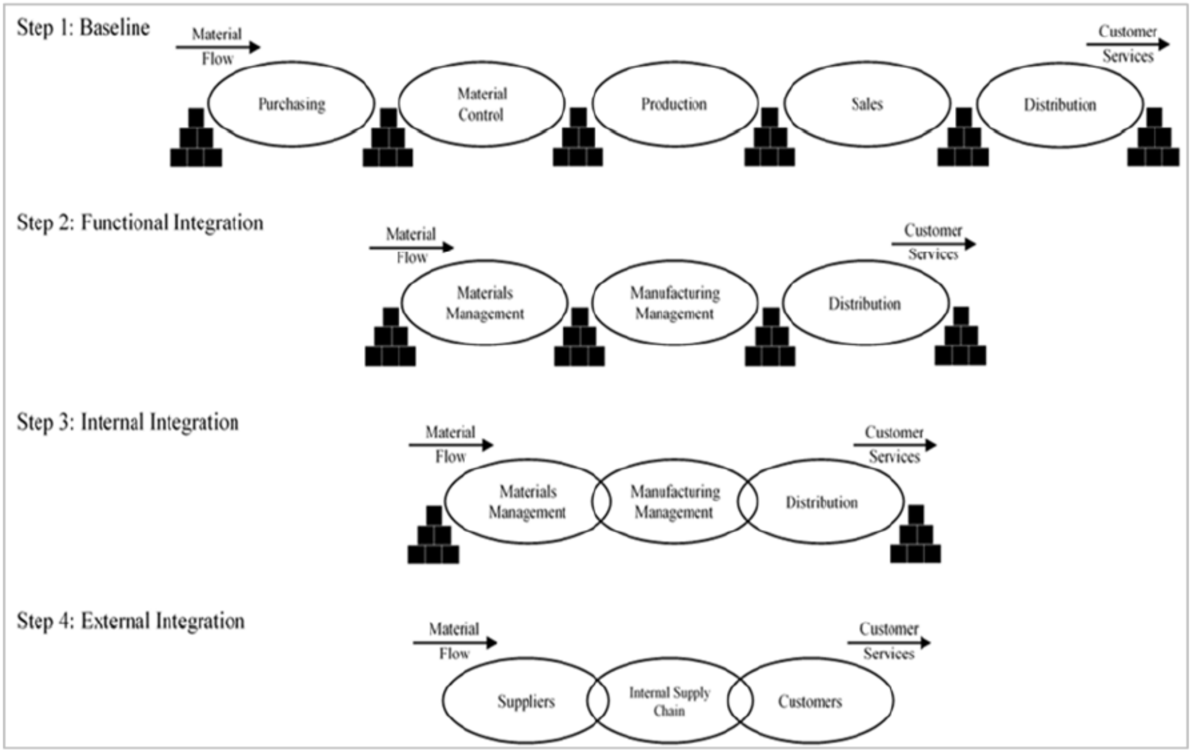


Figure 2.5: Supply Chain Developmental Stages, adopted from Stevens & Johnson (2016)

Previous studies have shown that supply chain integration is a difficult multidimensional construct. To address the difficulties involved in achieving supply chain integration, Stevens & Johnson (2016) suggested that the scope of supply chain integration should include establishing an effective and efficient organisational structure, relationship management, performance management, information sharing mechanism, business strategy and governance. Likewise, Prajogo et al. (2016) suggested that the scope of supply chain integration should include the integration of resources, sharing of information and the collaboration and coordination of the operations and activities within the supply chain network. Also, according to Surana, Kumara *, Greaves, & Raghavan (2005) and Gunasekaran et al. (2008), appropriate methodologies and strategies that involve the availability of timely and accurate information and communication, education and training, should be adopted so as to ensure an effective integration of supply chain activities and processes.

2.8 Conclusion

Findings from the literature show that organisations are experiencing a new era of intense competition in which supply chains are used as the centre point of competition, as against business versus business. Hence, most supply chains now have their own unique structure, set of processes, operational activities, market demands and also challenges. The literature also shows that this new era of intense competition is forcing organisations to form networks that are of close knitted collaborative relationships. These networks are inherently complex, have greater distances and consequently, have more uncertainties and are faced with more vulnerabilities, disruptions and risks (Chang *et al.*, 2015; Tuncel & Alpan, 2010; Wiengarten *et al.*, 2016). These disruptions and risks are adversely impacting on the information, operations and performance of supply chain organisations (Foulds, 2015; Ho *et al.*, 2015). Hence, supply chain practitioners and researchers are emphasising that trading organisations should establish and implement agile and resilient supply chain management practices that encourage information sharing, anticipates disruptions and risks, limit the negative impacts of disruptions and risks, and at the same time help organisations maintain an acceptable service level and cost reduction (Day, 2014; Lemmens *et al.*, 2016; Wang *et al.*, 2016b).

CHAPTER 3: INFORMATION & INFORMATION SYSTEMS WITHIN SUPPLY CHAINS

3.1 Introduction

Supply chains have evolved from dealing with only material flow to a much broader perspective that encompasses integrating the financial, material and information flow of trading organisations (Siddiqui & Raza, 2015). In today's supply chains, interests are moving towards using and obtaining the most benefits from information. Hence, it has become important for information to be presented clearly and in a manner that can be easily understood. To achieve this (presenting information in an easy to understand manner), information systems and their related technologies are being used by organisations (Pérez-Aróstegui *et al.*, 2015). These systems and technologies are making it possible for organisations to share resources, collaborate and form strategic partnerships within the supply chain.

This chapter discusses the literature on information, information sharing and information systems and technologies that are being used to enhance supply chains' structures, functions and processes. The compressed layout of the chapter is presented in Figure 3.1.

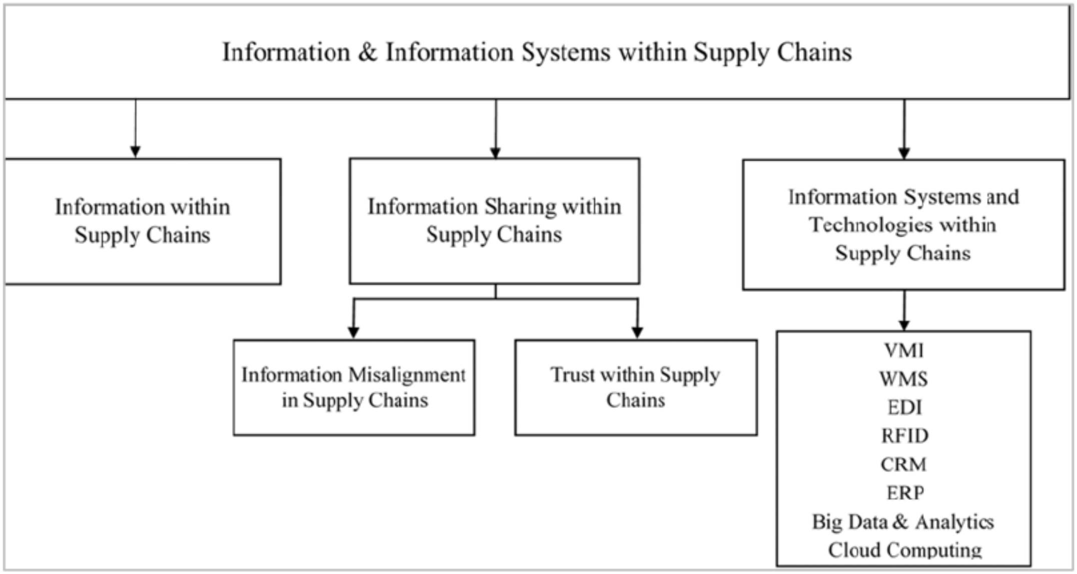

Information & Information Systems within Supply Chains
Information within Supply Chains
Information Sharing within Supply Chains
Information Systems and Technologies within Supply Chains
Information Misalignment in Supply Chains
Trust within Supply Chains
VMI
WMS
EDI
RFID
CRM
ERP
Big Data & Analytics
Cloud Computing

Figure 3.1: Layout of the Chapter

3.2 Information within Supply Chains

Supply chains are made of series of organisations and activities in which information and material move on their way to consumers (Vilko *et al.*, 2014). As shown in Figure 3.2, information is often considered one of the major components that flows in supply chains. It is a vital component needed for the smooth running of business operations and relationships. Likewise, it is an important component that is required in facilitating the transition of resources between trading partners, and in enhancing the ability of trading partners to effectively manage the supply chain (Tatoglu, Bayraktar, Golgeci, Koh, Demirbag *et al.*, 2016). The proper use of information can help organisations make competent decisions, and can also enable a coordinated and integrated supply chain. However, according to Miller & Drake (2016), the information that flows in a supply chain can also be a source of the supply chain's trading partners becoming vulnerable to different threats.

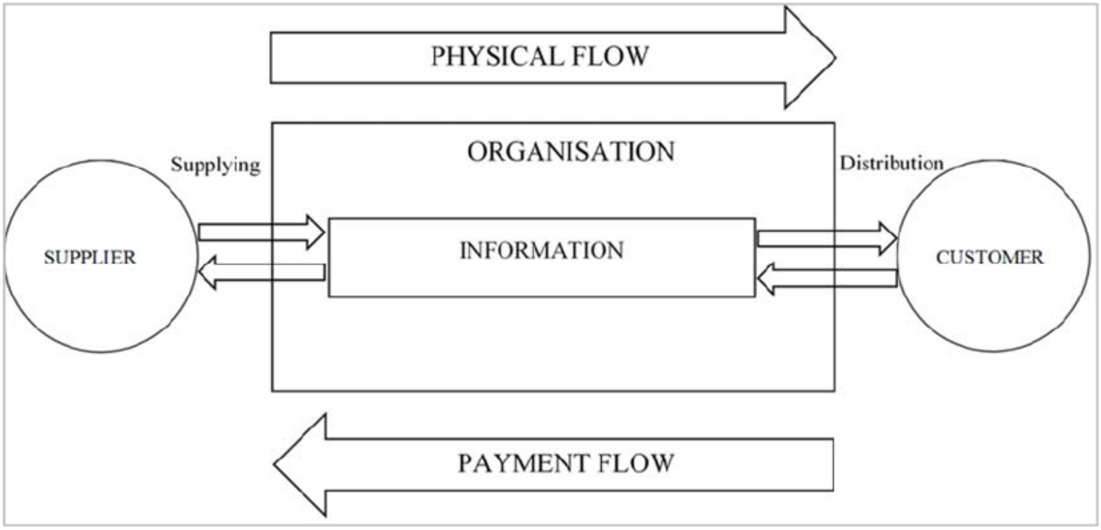


Figure 3.2: General Supply Chain Scheme showing material, fund and information flow, adopted from Regattieri & Santarelli (2013)

Organisations are increasing the effort to align and integrate information throughout the entire supply chain. This is because of the realisation that achieving organisational objectives and greater supply chain performance requires the use of integrative practices that includes information alignment and integration (Hariga, Gumus, & Daghfous, 2014; Huang *et al.*, 2016). Also, because the alignment and integration of information are crucial and central to the conversion of consumers' orders (through manufacturing operations and raw material acquisition) into final products that satisfy the needs and expectations of consumers (Pawar & Rogers, 2013; Spekman *et al.*, 2016). Successful information alignment, integration and flow throughout the supply chain is, however, dependent on the complexities of the supply chain (Gunasekaran, Subramanian, & Rahman, 2015; Lei, Chen, Wei, & Lu, 2015).

The design, processes and operations of supply chains depend on the availability of relevant and reliable information. According to Qrunfleh & Tarafdar (2013), the availability of information encourages collaboration and the involvement of the collaborating organisations in the design and integration of supply chain structures, processes and products. It, however, also determines the dimension of the uncertainties a supply chain could be exposed to (Thomé, Scavarda, Scavarda,

& Thomé, 2016). According to Simchi-Levi, Kaminsky, & Simchi-Levi (2004), when relevant and reliable information are made available within the supply chain, the trading partners are able to prevent out of stock situations, avoid problems such as the bullwhip effect (Angeles, 2009), ensure accurate planning, forecasting and production (Yu *et al.*, 2010), and also enhance their respective decision making processes (Mitchell & Kovach, 2016).

Studies on the flow of information in supply chain have been mostly about demand information (Wang & Disney, 2016). Hence, information regarding demand is considered one of the most critical information needed by trading partners. When trading partners have the complete knowledge of the consumers' demand information, they are able to make effective decisions. According to Isaksson & Seifert (2016), demand information, when shared accurately, improves inventory management. It, however, can also cause harm to organisations, especially when leaked to competitors. Insufficient demand information can also be a cause of an increase in the manufacturers' production cost, and an unreliable demand forecast, which can negatively affect the inventory planning capacity of trading partners (Wang, Lu, Feng, Ma, & Liang, 2016d).

The quality of information that the different organisations within a market have about each other is an important determinant of each organisations' behaviour in the market. It is also a determinant of the benefits derived by organisations when information is shared (Dai, Li, Yan, & Zhou, 2016). According to Kembro & Selviaridis (2015), organisations are often faced with the challenge of deciding on the quality of information to be acquired or shared within the supply chain. The factors affecting the quality of any acquired or shared information are the divergent interests of supply chain partners and the sharing of asymmetric information across the supply chain (Zhu, 2016). When information is shared or distributed asymmetrically, it opens the door for opportunistic behaviours.

Information asymmetry has become a vital issue for supply chains because it creates uncertainties for decision makers and often increases supply chain risks. According to Tong & Crosno (2016), information asymmetry is caused by organisations deliberately distorting the information that is communicated not only to their competitors but also to their trading partners. When information is deliberately distorted, the benefits to be derived from such information is often minimal. Information asymmetry is often amplified when trading partners fail to share real-time information (Dai *et al.*, 2016). To mitigate information asymmetry, organisations should adopt control mechanisms that include the careful selection of trading partners and the establishment of trust with the selected trading partners (Miller & Drake, 2016).

Acquiring information can be costly. According to Huang *et al.* (2016, p.1519), "the more detailed the information is, the greater the cost of collecting it." One of the major concerns of organisations with regards to acquiring information is the accuracy of the acquired information. This is because, when inaccurate information is acquired, it can cause coordination failure in supply chains. According to Ryu *et al.* (2009), there seems to be an inherent reluctance by organisations to disclose accurate or more than minimal information to their trading partners. This is because of the fear that the disclosed information may leak to their competitors. Yu *et al.* (2010), however, stated that if organisations are made to understand the benefits they will derive from sharing accurate and reliable information, they will be willing to disclose the necessary and accurate information that is required for the success of the supply chain.

3.3 Information Sharing within Supply Chains

The topic of information sharing has been on the agenda of both supply chain practitioners and researcher for decades and has also become a topic of debate and interest among supply chain organisations (Rached, Bahroun, & Campagne, 2015). For supply chains' structures and processes to be synchronised, the organisations within the supply chain must share information. Similarly, in order to establish a resilient and agile supply chain, information must be shared among the supply chains' trading partners (Gunasekaran *et al.*, 2015). Information sharing has been described in the study of Tong & Crosno (2016) as the proactive and timely exchange of useful information among trading partners, and in the study of Li and Lin (2006) as the degree to which relevant and proprietary information is shared among trading partners. It has also been described in the study of Dai *et al.* (2016) as the practice in which inventory and consumers' demand information are being communicated to all the parties within the supply chain. According to Yu *et al.* (2010), information sharing can be divided into three different scenarios which are:

Scenario 1: No information is shared between the parties in the supply chain network
Scenario 2: Partial information is shared between the parties in the supply chain network
Scenario 3: Full information sharing happens between the parties in the supply chain network

Not sharing information within the supply chain might render trading inefficient (Miller & Drake, 2016). However, according to Yu *et al.* (2010), not sharing information within the supply chain is in some cases better than sharing partial information. For example, when only information such as inventory or capacity level is shared but demand information is not shared, interference with production may be caused and sales forecast may be misrepresented. Increased information sharing among trading partners may also not always be favourable. This is because, for example, when excess raw downstream data are sent to upstream partners, it may result in inaccurate assimilation or misrepresentation of data (Kembro & Selviaridis, 2015).

There is a growing body of literature on the study of the incentives that can be derived from sharing information within supply chains (Fu & Zhu, 2010; Li *et al.*, 2015; Rached *et al.*, 2015).

Sharing information helps supply chain members in responding rapidly to market changes (Chang *et al.*, 2015), reducing supply chain complexities and uncertainties (Gunasekaran *et al.*, 2015) and ultimately, in satisfying consumers' needs (Kenyon, Meixell, & Westfall, 2016; Spekman *et al.*, 2016). Hence, the sharing of information should be encouraged between supply chain members. Koçoğlu *et al.* (2011) in their study outlined some means of encouraging the sharing of information among supply chain members. The means are:

Inter-organisational integration: In order to improve their performance, organisations are encouraged to undertake supply chain initiatives such as outsourcing, collaboration and inter-organisational integration (Kenyon *et al.*, 2016). Inter-organisational integration allows for the sharing of information, responsibilities, resources, rewards and risk among the supply chains' trading partners. Hence, according to Koçoğlu *et al.* (2011), when inter-organisational integration is established, information can be adequately shared, and an efficient and effective supply chain operation can be easily achieved.

Provision of Incentives: Incentive schemes can be used to facilitate information flow and information access management within supply chains (Koçoğlu *et al.*, 2011; Siddiqui & Raza, 2015). Although, according to Lei *et al.* (2015), incentive conflicts can lead to failure in supply chain coordination. The result of the study of Rached *et al.* (2015) on the gains of sharing different types of information, shows that incentive mechanisms are important in encouraging the sharing of different types of information within the supply chain. Hence, incentive mechanism should be established across the supply chain network, so as to facilitate the prompt and complete sharing of information.

Establishing a Trust-based Relationships: The issue of trust is a determinant in the reluctance of organisations to share information with their trading partners (Koçoğlu *et al.*, 2011). Organisations in a high trust relationship are often more willing and less reluctant to share information. This is because, in a trust-based relationship, the information being shared between the supplier and retailer is believed to be credible and reliable (Fu, Dong, Liu, & Han, 2016), and the organisations in this type of relationship do not expect their trading partners to behave opportunistically. However, according to Prajogo *et al.* (2016), it takes time to build trust in supply chain relationships and among trading partners.

Adoption of Information Technology (IT): Information technology is a resource that enables the acquisition, storage, sharing and use of information (Bian, Shang, & Zhang, 2016; Eamonn & Kelly, 2015; Koçoğlu *et al.*, 2011; Pérez-Aróstegui *et al.*, 2015). Hence, the adoption of IT and its infrastructures such as the different hardware, software, shared technological service etc. enables and facilitates the smooth diffusion of real-time information among trading partners. According to Rached *et al.* (2015) however, the pervasiveness of IT is also creating a significant challenge to real-time information sharing.

The willingness of most organisations to share information is a function of the information revelation behaviour of the other organisations within their supply chain network (Zhang & Chen, 2013). Lack of trust, inability to link inter-organisational information systems, improper handling of confidential information and fear of loss of bargaining power are some of the issues preventing organisations from willingly sharing information. Irregular demand patterns, lead-times and information sharing direction (i.e. upstream or downstream) has also been identified by Wang & Disney (2016) as factors affecting the sharing of information, willingly. Shao (2013) and Singh & Teng (2016) however, stated that establishing a collaborative relationship and trust often facilitates and ensures information is willingly shared among trading partners.

Achieving the benefits of information sharing within supply chains may be difficult. Hence, Zhang and Chen (2013), Denolf *et al.* (2015), Lei *et al.* (2015), Lee, Cho, & Paik (2016), and Protopappa-Sieke, Sieke, & Thonemann (2016) suggested that supply chain trading partners must sign coordinative contracts such as compliance contracts, revenue-sharing contracts, VMI contracts, service level contracts etc. that will make certain that each member in the supply chain share relevant information adequately. Furthermore, McCormack *et al.* (2008) suggested that the process, format, frequency, and technology used for sharing information must be agreed upon by the supply chain trading partners, as this will reduce the supply chains' overall risk, enable consistency and consequently, encourage the supply chain members to participate in the sharing of information.

One of the ways of reducing the probability of risks occurrence and the severity of disruptions is by sharing information among the supply chain trading members. Hence, Supply chain partners are encouraged to openly and frequently share information about their production processes, marketing activities and general consumer information. According to Schoenherr (2010) and Piderit *et al.* (2011), openly and frequently sharing information increases the level of inter-organisational relationship and trust, decreases uncertainties and reduces the impacts of the risks inherent in supply chains. This is because, as explained in the work of Shao (2013), organisations that openly and frequently share information concerning disruptive activities will enable their trading partners to proactively prepare and make possible plans for reducing the negative impact of such disruptive activities.

3.3.1 Information Misalignment in Supply Chains

One of the effects of not sharing information adequately, as found in the literature, is the misalignment of information. The misalignment of information, especially the demand and supply information, causes an effect called the "bullwhip" effect, in supply chains. The bullwhip effect is one of the main causes of distortion to upstream inventory (Wang *et al.*, 2016d). It is caused by inaccuracies or inconsistencies in inventory information and records (Bruccoleri, Cannella, & Porta, 2014), the lack of information visibility within the supply chain network, and the delays in information sharing among trading partners (Wang & Disney, 2016). According to Bruccoleri *et al.* (2014), human factors or employees' behaviour towards information, such as inventory information, is also another important contributing factor to the misalignment of information within supply chains.

The lack of information and the misalignment of information, are some of the forces contributing to the disruptions happening in today's volatile globalised supply chains. Similarly, supply chain members' inability to access demand information or make demand forecast, and the lack of timely and precise information about the true point of sales data are also contributing factor to the misalignment of information happening within supply chains (Mitchell & Kovach, 2016; Pedroso & Nakano, 2009). Dai *et al.* (2016) explained that the shrinkage in the quality of shared information is also another contributing factor to information misalignment with supply chains. They further explained that when statistical information rather than real-time information is being shared within the supply chain, the bullwhip effect can also be created or magnified.

To overcome the misalignment of information and also reduce the impact and consequence of bullwhip effect, Zhang & Chen (2013), Sabitha, Rajendran, Kalpakam, & Ziegler (2016) and Bian *et al.* (2016) suggested, as a measure, the adequate sharing of information among supply chains' trading partners. According to Kembro & Selviaridis (2015), several other authors have also shown that the frequent and adequate sharing of information, such as demand and inventory information, help minimise information misalignment. However, according to Wang & Disney (2016), information sharing can sometimes also be a cause of information misalignment, especially when there is a lack of trust and when information is not adequately and accurately shared among the information sharing partners (Miller & Drake, 2016).

3.3.2 Trust within Supply Chains

Trust and shared vision between supply chain trading partners are identified to be of huge influence on the quality of shared information within supply chains (Denolf *et al.*, 2015). They have also been identified as major factors that could prevent an organisation or supply chain's growth and performance. Trust within supply chain has been described in the study of Koçoğlu *et al*. (2011, p. 1633) as "the extent to which a firm believes that its partner with whom exchange takes place, is honest and/or benevolent and is considered to be a salient buffer of long-term stability and success of inter-organisational relationships." It has also been described by Seth *et* *al.* (2015) and Spekman *et al.* (2016) as the belief that an organisation's trading partners will act in a reliable and consistent manner, and deliver on what they have said they will do.

Trust is an important enabler for information sharing and process integration among supply chain trading partners. This is because it makes it possible for organisations to make decisions that will not be harmful to the other members of the supply chain network. It also serves as a mitigating factor to the information users' potential loss (Fu *et al.*, 2016). In the study of Piderit *et al.* (2011), it was stated that for supply chains to remain competitive and integrated, the organisations within the supply chain must build trust among themselves so as to allow for an improved information sharing. Similarly, according to Choo (2011), for supply chain to remain integrated, the organisations within the supply chain must have a trusted and secure information sharing mechanism that facilitates the timely sharing of information. This is because a trusted information sharing mechanism within the supply chain will help ensure the commitment of trading partners to the information sharing activities of the supply chain.

Trust, privacy and security, are complex issues that have transcend the traditional market environment, and have moved into the modern electronic geographically dispersed market environment. Organisations are therefore increasingly being advised to trust each other so as to be able to reduce the challenges affecting information sharing, and still be able to effectively manage the processes within their supply chain network (Shao, 2013; Singh & Teng, 2016). The existence of trust between trading partners is a determinant of how successful, information systems will be used to facilitate the sharing of information. It is also a determinant of the level of confidence that organisations will have in each other's shared information. Trust, however, is still considered a major challenge affecting the sharing of information among trading partners and also a major contributor to supply chain failures (Singh & Teng, 2016).

3.4 Information Systems & Technologies within Supply Chains

In the present knowledge economic era, information systems and their related technologies have become an indispensable tool for the daily operations of businesses, and in the management of knowledge. They are making it possible for business information that was only accessible when in the office, to become accessible from anywhere in the world. Hence, they are increasingly being used as a tool to coordinate supply chains' structures, to increase the visibility of supply chains' operations and processes (Lam *et al.*, 2015), and to facilitate the provision of accurate information in real-time to trading partners. However, to achieve these benefits (offered by the use of information system), the information systems used within supply chains must be user-friendly, accessible and reliable (Seth *et al.*, 2015). There functionalities and capabilities must also be accessed and utilised to their capacity (Montesdioca & Maçada, 2015).

The sharing of information is being facilitated by the integration of different information systems (Singh & Teng, 2016). Hence, when organisations are planning the adoption and implementation of information systems, they should consider the systems that can integrate easily with the systems of their trading partners. Integrated information system makes it possible for organisations to make the necessary information related decisions (Lee *et al.*, 2016). However, according to Pérez-Aróstegui *et al.* (2015), the integration of information system must be in alignment with the organisational strategy. This is because the degree of information system integration with an organisation's strategy is an important determinant of the competence and capabilities of the overall information systems used within the organisation. Tatoglu *et al.* (2016), also alluded to the fact that non-alignment of information system and organisational strategy, prevents the full integration of information system into the organisational processes.

Information systems have evolved from the early legacy systems that were less sophisticated, to more advanced information management systems. They now act as one of the major difference between the traditional supply chains and modern supply chains (Marinagi *et al.*, 2014). Every aspect of modern supply chains is being affected by the pervasiveness of information systems and technologies (Singh & Teng, 2016). Hence, supply chain organisations are forced to, now more than ever, adopt information systems and their related technologies. This adoption is, however, giving those with criminal intention the motive and desire to develop newer ways of compromising information within supply chains. Choo (2011) stated that the global adoption and use of information systems present those with criminal intentions, the opportunity to perform their criminal activities. It also makes the efforts to guarantee the security of information within supply chains more challenging.

The availability, accuracy and reliability of information and the performance of supply chains are now being significantly improved by leveraging on information system and technology initiatives such as Efficient Consumer Response (ECR), Quick Response (QR), Vendor Managed Inventory (VMI), Radio Frequency Identification (RFID), etc. These initiatives, however, requires substantial investments which not all parties within the supply chain might be able to afford (Costantino, Di Gravio, Shaban, & Tronci, 2015). Hence, authors such as Stefansson (2002); Fu and Zhu (2010) suggested that in the presence of the overhead cost associated with this different information system and technology initiatives, it is worthwhile to examine the technology need and use of all trading partners in order to determine if it is an economically attractive option for the supply chain to invest in any technology initiative.

In the next sections, some of the information systems and technologies, as identified in the literature, being used to acquire, process, store and share information within supply chains are presented.

3.4.1 Vendor Managed Inventory (VMI) System

The VMI system, according to Mateen & Chatterjee (2015), is a supply chain coordination mechanism. The literature shows that the performance of supply chain increases when VMI system is implemented to facilitate information sharing activities and practices between suppliers and their retailers. This is because VMI system makes it possible for all trading partners in a supply chain to have access to the consumer demand information. It also provides tools that help with the synchronous management of information and the update of information in real-time. With the VMI initiative, the level of coordination and collaboration among trading partners is such that there is a total visibility of information (Costantino *et al.*, 2015). Klein *et al.* cited in the study of Angeles (2009) explained that, with VMI, buyers and retailers are expected to share operational information with the respective suppliers in their trading network. They are also required to share inventory and demand information (Dai *et al.*, 2016; Wang & Disney, 2016).

The VMI system is a widely used supply chain initiative that was launched to help suppliers and manufacturers plan the ordering and replenishment of the inventory of their retailers or customers in general (Lee *et al.*, 2016; Tang, 2006). It is a system that is gaining a lot of attention from organisations. This is because, with it, trading partners benefits from the reduction of the risk of information distortion and decision echelons. It is also because, it performs better than the traditional system of inventory management (Lee *et al.*, 2016). In the traditional system of inventory management, the retailer manages its own inventory and inventory information, and when the inventory is low, the retailer places a replenishment order with the supplier. But, with VMI, the vendor or supplier automatically replenishes the retailers' inventory, because the retailers' inventory information is under their (i.e. vendor or supplier) surveillance (Wang & Disney, 2016). This means that, under the VMI initiative or agreement, the vendor or supplier is allowed direct access to the information regarding inventory.

The implementation of a VMI system involves having a centralised information sharing system that helps with inventory and replenishment management capabilities. According to Sabitha *et al.* (2016), the implementation of VMI also often comes with challenges and operational difficulties. These challenges include the number of retailers under the VMI, the lack of information visibility between suppliers and retailers, the misalignment of information and the increase in organisational cost (Mateen & Chatterjee, 2015). To manage these challenges, it is explained in the study of Lee *et al.* (2016) that suppliers and customers should sign a VMI contract that specifies proportional and fixed penalties for overstocking or lack of information sharing, and that also specifies a maximum inventory level. Mateen & Chatterjee (2015) also stated that managing VMI challenges requires the institutionalisation of incentive mechanisms in which the parties experiencing challenges are compensated. The alignment and commitment of trading partners to their process of forecasting, information sharing, planning and replenishment can also help reduce the challenges of the adoption of VMI (Costantino *et al.*, 2015).

3.4.2 Warehouse Management System (WMS)

Warehouse play a pivotal role in the activities of any supply chain (Accorsi, Manzini, & Maranesi, 2014). According to Atieh, Kaylani, Al-abdallat, Qaderi, Ghoul *et al.* (2016), the main role of a warehouse is to manage the flow and storage of goods in the most effective and efficient manner. Today, however, the requirements for warehousing operations have significantly increased due to the consumers' needs in terms of order accuracy and response time. It has also increased as a result of the global market trends such as e-commerce (Accorsi *et al.*, 2014). Hence, as identified in the literature, the traditional manually managed warehouse is deemed insufficient in today's business environment. In agreement, Alyahya, Wang, & Bennett (2016) also explained that the traditional manually operated warehouse is often faced with challenges such as a consistent increase in the cost of labour, a poor efficiency of material handling and also, a high frequency of human errors, which could negatively impact the overall supply chain. The desire of organisations to overcome these challenges have necessitated the need for warehouse automation.

The advancement of technology and its implementation and integration into today's supply chain structures, processes and activities has created opportunities and demonstrated great improvement for warehouses in terms of a better inventory control and shorter response time. It has also enabled the development of the Warehouse Management System (WMS), which as described by Jomaa, Monteiro, & Besombes (2013), is a software that is used to control and monitor the operations and activities within a warehouse. These operations and activities include space optimization, real time product tracking, shipping and receiving, planning, scheduling, warehouse consumption forecasting and inventory management. According to Atieh *et al.* (2016), Warehouse Management System (WMS) is a necessary component and approach for today's warehouse facilities. This is because it facilitates an automated warehousing system that provides more efficient and reliable results compared to the traditional warehouse management approach. It also requires less effort in the tracking and management of stock.

The WMS, just like any other system comes with its own challenges. Of these challenges, one of the most prominent is it cost of acquisition (Accorsi *et al.*, 2014). Other challenges with the adoption of WMS includes, the skills required in the implementation and integration of the system into the existing organisational warehouse processes and structures and the skills required in operating the system so as to perform optimally. To manage some of the challenges with WMS, Atieh *et al.* (2016) suggested that the software (for the WMS) to be adopted by organisations must be chosen based on the needs of the warehouse.

3.4.3 Electronic Data Interchange (EDI) System

Using electronic aids to facilitate data processing and information exchange has been a practice by organisations for decades. However, according to Pfeiffer (2012), towards the end of the 1970s, the use of computer-based information systems for facilitating data processing and information exchange became pervasive. One of such computer-based information system used is the EDI System. EDI facilitates the intra- and inter-organisational computer-to-computer exchange of information and documentation, in a computer-processable and structured format (Ramdeen, Santos, & Chatfield, 2011). Jardini, Kyal, & Amri (2016) explained it to be the transfer of structured data from one computer to another, by means of agreed messaging standards that are acceptable to the trading partners. Similarly, Tatoglu *et al.* (2016) explained it to be the electronic exchange of documents and information in real-time. The data from EDI systems are usually preformatted, and their exchange mostly relies on the Internet, although, they can also be exchanged through peer-to-peer networks and serial links (Margaret, Sharon, & Jeff, 2014).

The EDI technology has been in existence for a long time (Gunasekaran *et al.*, 2008; Stefansson, 2002). But before its existence, organisations used Electronic Data Processing (EDP) systems that are designed to automate labour intensive and repetitive processing tasks (Pfeiffer, 2012). But with the advances in technology, EDI was developed as an initiative for linking suppliers and consumers, and for sharing and integrating the information within supply chains. EDI is a technology that is being increasingly adopted by supply chain organisations to suit their business needs, budget and capabilities, and to also support the interaction with their global partners. Although, according to Gunasekaran *et al.* (2008), some organisations are not adopting it at a significant rate. This, according to Musawa & Wahab (2012) is because they believe that EDI, just like most other information systems and technologies, often have a limited impact on their operations, as a result of their under-utilisation.

EDI enables a shared information platform that facilitates easier communication among trading partners. It also enables the processing of information and the facilitation of interaction and communication between trading partners. Furthermore, it enables the automatic exchange of information between remote applications, especially in cases where those applications belong to different organisations (Pfeiffer, 2012). With EDI, organisations benefit from reduced time and effort required to share information and perform transactions (Macharia & Ismail, 2015). They also benefit from reduced transaction cost, improved information quality, improved customer service and enhanced operational efficiency. The adoption of EDI, however, also comes with challenges. According to Romi (2014), establishing EDI and its value-added network (VAN) services between trading partners often requires that the trading partners have compatible ICT infrastructure, and this is not always the case between trading organisations.

The skills and cost involved in the adoption and implementation of EDI is a challenge to organisations (Musawa & Wahab, 2012). According to Jain *et al.* (2009), another challenge to EDI is that data can only be exchanged with pre-arranged partners. This is a challenge because it means that organisations cannot share or access data without having a prior agreement on messaging standards that are acceptable to their trading partners. The time and processes involved in reaching such agreement are often a challenge to most organisations. Hence, organisational complexities and readiness should be considered when planning to adopt EDI.

Jardini *et al.* (2016) stated that organisations should consider the merging of the EDI technology with the Just-in-time (JIT) production system. This, according to them is because the exchange of information using the two systems can contribute to a close collaborative relationship between trading partners. The JIT principle is a management philosophy that ensures that the demands of consumers are met, in good time and with enhanced quality (Patil, 2016). According to Jardini *et al.* (2016), it is a system that ensures that any malfunction in production is identified and eliminated. Hence, the use of EDI and JIT together will provide an efficient practice that can help in the reduction of waste, elimination of stocks, and the management of physical and information flow within the supply chain.

3.4.4 Radio Frequency Identification (RFID) Technology

Tracking is one of the important components of supply chain management, and it has been made possible by technologies such as the barcode and RFID. With barcode, computer readable codes are placed on items, so as to facilitate an efficient tracking and information retrieval of such items (Tatoglu *et al.*, 2016). RFID technology has similar functionalities with the barcode technology. The difference, however, according to de Mel, Herath, McKenzie, & Pathak (2016) is that RFID offers additional functionalities and advantages. These functionalities and advantages include loss and theft prevention capabilities, potential to provide real-time information and inventory reports, and also minimise unnecessary handling of the information regarding products. According to Jain *et al.* (2009), RFID is used within supply chains to access information about the shipment of goods from the point of origin to destination, and also, to track and manage inventory and warehouse information regarding stocks (Dai *et al.*, 2016).

The RFID technology is making it possible for supply chain trading partners to adopt a common information acquisition and exchange standard. Hence, it is changing the manner in which information is acquired by trading partners, and also increasing the availability and visibility of real-time information within supply chains. According to McCarthy *et al.*, cited in Ko, Pan, & Chiou (2013, p.446), the RFID technology "is a wireless sensor technology based on electromagnetic signal detection". It consists of a transponder (also known as a tag), an interrogator (also known as a reader) and an antenna. It uses the tags, which are attached to items, to store information about items and to track the movement of items in real-time, by means of radio waves (Jain *et al.*, 2009; Tatoglu *et al.*, 2016). The radio waves help with the exchange of data between the tags and readers. Although, according to Hinkka *et al.* (2013), the use of RFID and the benefits derived from its use, depends on the type and level of technology that is used in developing it.

RFID is considered a tool that can help minimise the challenges of inaccuracies in inventory information (Lei *et al.*, 2015). Its adoption, however, also has its own challenges which include the inter-organisational integration of the different tracking systems used by the different organisations within the trading network. According to Ko *et al.* (2013), another challenge to the use of RFID is that radio communications are often affected by nearby radio signals. Ko *et al.* (2013) further pointed out that the facilities in which RFID systems are used are also another challenge to RFID systems. This is because, these facilities often contain metal parts, such as panels, doors and windows, which reflects radio signals and thus, influences the RFID systems' effectiveness. Wu & Subramaniam (2011) in their study also highlighted trading partners' readiness, technology complexities and top management support as challenges and predictors to the adoption and successful utilisation of RFID in supply chains.

3.4.5 Customer Relationship Management (CRM) System

To attain and sustain a substantial competitive advantage, organisations require information that provides insight about their customers. This is because, customers are the most important possession of any organisation, and are also a major source of an organisation's profit and the future growth of any supply chain. Their "position is shifting from a passive receiver to an active influencer" (Triznova, Maťova, Dvoracek, & Sadek, 2015, p.956). Hence, creating and managing a strong relationship with them have become an important responsibility and challenge for organisations (Thakur & Workman, 2016). To meet up with this challenge and responsibility, organisations are adopting CRM systems that promote a scientific method of identifying new customers, and establishing and maintaining a good relationship with them, so as to retain them and ensure their loyalty (Krishna & Ravi, 2016; Soltani & Navimipour, 2016). CRM is enabling organisations to sell more effectively to customers and integrate supply chain functions.

CRM system became popular in the mid-90s, but before then, it was a concept referred to as database marketing (Elena, 2016; Sulaiman, Baharum, & Ridzuan, 2014). It is now perceived as the strategy, processes and technology that can be used to provide organisations with information about the past, present and possible future customers (Triznova *et al.*, 2015). Hence, it has now become an indispensable tool for processing customers' information, so as to establish a relationship with them. Today, CRM systems are integrated into (and also supported by) the organisations' information system and technology platform (Triznova *et al.*, 2015). This platform is enabling CRM systems to become a system that can collect and process customers' information. It is also providing organisations with the capability to enhance their marketing strategies, by providing them with the information required to customise their products and services, in a manner that suits the customers' needs and expectations (Krishna & Ravi, 2016).

In recent years, CRM system has attracted a lot of attention from the field of information technology (IT) (Ghalenooie & Sarvestani, 2016). This is because, it offers technological solutions that facilitate the building and management of customers' relationship, in an integrated manner (Elena, 2016). According to Triznova *et al.* (2015), a CRM system uses technology that depends on high quantity and quality of customer information. The technology helps in predicting customers' behaviours. It also helps in transforming acquired customer information into corporate knowledge that is used to take advantage of market opportunities. To reap the benefits offered by CRM systems, Erdil & Öztürk (2016), however, suggested that the CRM system must be aligned and integrated with the organisations' strategy, processes, technology and people.

CRM Systems are facing challenges that are making them difficult to implement. These challenges stem from the fact that their implementation often requires extensive ICT infrastructure, resources, skills (both social and IT skills) and knowledge (Tatoglu *et al.*, 2016). As explained in the study of Erdil & Öztürk (2016), one of the common mistakes made in the adoption and implementation of CRM systems is that organisations often focus only on technology, process and people components, but pay less attention to the strategies involved in the implementation and use of CRM system. According to Ghalenooie & Sarvestani (2016) and Triznova *et al.* (2015), organisations should not focus only on technology when implementing CRM system, they should also focus on establishing a customer-centric culture and strategy that can be deeply rooted in the different people in the organisation.

3.4.6 Enterprise Resource Planning (ERP) System

In the early 1970s, Material Requirements Planning (MRP) was developed to help manufacturers plan production and help warehouses plan inventory (Jain *et al.*, 2009). The widespread adoption and use of MRP within the manufacturing sector prompted the development of Manufacturing Resource Planning (MRP II) (Jain *et al.*, 2009). The desire of organisations to gain greater visibility across their business operations and with their trading partners also necessitated the evolution of MRP into MRP II (Stevens & Johnson, 2016). MRP II expanded and built upon MRP, by integrating it (MRP) into organisations' financial system, and by incorporating it into manufacturing organisations' resource planning and scheduling activities. MRP II was used for manufacturing planning and control, and for coordinating organisations' order fulfilment processes (Tatoglu *et al.*, 2016). It achieved this by ensuring that the availability of resources such as materials and information matches the market demands.

By the late 1980s, there was an increasing need to integrate the information of all the different functional units within organisations so as to facilitate decision making, enhance productivity and increase profits (Jain *et al.*, 2009). This need prompted the development of Enterprise Resource Planning (ERP) systems. The limitation and evolution of MRP and MRPII also added to the need for the development of ERP systems. Kandananond (2014) described ERP systems as an integrated system designed to integrate and automate business information and processes. Similarly, Tatoglu *et al.* (2016) described it as an integrated application that is designed and developed to address information fragmentation within and across organisations. According to Denolf *et al.* (2015, p.17), it is "a complex inter-organisational management system," because it covers a wide array of organisational processes and functions that are in some instances located at different places across the globe.

The adoption of ERP systems by organisations hoping to establish interconnected links within their value chain is growing. Over 60% of the Fortune 500 organisations have adopted and implemented an ERP system (Jayawickrama, Liu, & Hudson Smith, 2016). This is because ERP systems are making it easier for them to control business processes, coordinate the flow of information, material and funds, and to integrate the functional areas within organisations (Seth *et al.*, 2015). These systems are also facilitating the access to integrated databases that facilitates communication between organisations, and generate reports that are often used in decision making, forecasting and production (Marinagi *et al.*, 2014). These systems, in addition, also ensures the management of information in a uniform manner, thereby preventing expenses and reducing the irregularities associated with the movement of information from one point to another (Marinagi *et al.*, 2014). Furthermore, according to Tatoglu *et al.* (2016), they are also enhancing the ability to generate accurate and real-time information that can be collaboratively shared among trading partners.

Since the 1990s, the implementations of ERP systems have been widely investigated for three reasons (Denolf *et al.*, 2015). The first reason is because of its ability to integrate information flow across the functional units (e.g. finance, sales, HR, etc.) within an organisation. The second reason is because of the high failure rate of its implementation (Kandananond, 2014), and the third reason is because of the huge cost that ERP systems absorb from the organisations adopting it (Denolf *et al.*, 2015). Another reason for the wide investigation of ERP systems' implementation has been because of the challenges faced by trading partners in trying to integrate their existing systems with the ERP systems. Greasley & Wang (2016) in their study also mentioned that ERP systems implementation is being investigated so as to understand how to improve their performance (ERP) and also understand how to increase their alignment with organisational systems, processes and needs.

To address some of the challenges facing the adoption and implementation of ERP systems, Kandananond (2014) suggested that before the implementation of ERP systems, organisations should conduct a proper process mapping that will help them investigate and determine how thoroughly their business processes has been mapped to the current information and supply chain system. This will help them determine the suitability of the ERP system to the organisational processes. Kandananond (2014) further suggested that organisations should also consider and address four critical factors before the implementation of ERP systems. These factors are: defining the business case for the ERP system, preparing the users, stabilising the business operations and finally, continuously maintaining and upgrading the ERP system. Also, as suggested by Marinagi *et al.* (2014), to address ERP systems implementation challenges, ERP vendors are now providing integrated packages that make it possible for organisations to easily interconnect and integrate their respective existing enterprise systems to ERP systems.

3.4.7 Big Data & Analytics

The information systems within supply chains generate a lot of data and information that are captured through manual interactions or from automated sources (Jain *et al.*, 2009). Likewise, trading partners are continuously and increasingly accumulating a huge amount of data and information that are stemming from transactions (e.g. EDI transactions), information systems and technologies (e.g. ERP systems, RFID systems) and mobile devices (Wang, Gunasekaran, Ngai, & Papadopoulos, 2016a; Yaqoob, Hashem, Gani, Mokhtar, Ahmed *et al.*, 2016). The quantity of data being communicated and produced over the Internet is also continuously increasing. Thus, the quantity of information in their various forms, being acquired, used and shared by organisations and within supply chains are increasing tremendously. This increase has caused the generation of the term big data. According to Yaqoob *et al.* (2016), the term “Big data” has been coined as a result of the need for organisations to understand and analyse the large amount of data being continuously and increasingly acquired and accumulated.

In recent years, big data has emerged as a new paradigm. According to Wang *et al.* (2016a, p.99), it is referred to as “the ability to process data with the following qualities: velocity, variety and volume”. Yaqoob *et al.* (2016) stated that a fourth quality referred to as veracity, has been added by Microsoft and IBM, and another quality referred to as value, has also been added by McKinsey & Co. These qualities define big data and they are often referred to as the 5Vs of big data. The term velocity is used to describe the speed of incoming and outgoing data, the term variety is used to describe the sources and types of data, and the term volume is used to describe the size of the data (Philip Chen & Zhang, 2014). Veracity, on the other hand, is used to describe the trustworthiness of data, and value is used to describe the worth of the concealed information inside the data (Hiba, Ammar, Sarah, & Azizahbt, 2015; Yaqoob *et al.*, 2016).

Big data cannot be easily managed by traditional data processing technologies and systems. This is because the processing of big data exceeds the processing power of the traditional data processing technologies (Wang *et al.*, 2016a). Only advanced storage techniques and data mining techniques can make the storage, analysis and management of big data possible. Big data analytics is one of the major technique that can be used to process and manage big data (Gunasekaran, Papadopoulos, Dubey, Wamba, Childe *et al.*, 2016). In the study of Wang *et al.* (2016a, p.99), it was explained that the analytics in big data analytics "involves the ability to gain insight from data by applying statistics, mathematics, econometrics, simulations, optimisations or other similar techniques". In the same study, it was also reported that Accenture conducted a survey that showed that a large number of organisations are willing to, or already have initiatives in place to have analytics deployed in their logistics and supply chain.

Big data analytics techniques have seen a huge advancement, and as such, now offer supply chain organisations the necessary tools that are used for analysing the huge amount of data being acquired through information systems within the supply chains. It is increasingly receiving attention from supply chain practitioners and researchers because of its identified role in improving the flexibility, visibility, resilience, robustness and integration of the global logistics and supply chain processes (Gunasekaran *et al.*, 2016; Wang *et al.*, 2016a). It is also receiving attention because of its role in the in-store behaviour analysis of retail organisations, the forecasting of demand and the sales support it offers manufacturing organisations (Hiba *et al.*, 2015). Although, according to Gunasekaran *et al.* (2016), the impact of big data analytics on organisations' supply chain performance has not been thoroughly investigated.

The development and management of big data are organised around capturing, integrating and finding relevant information. According to Yang, Huang, Li, Liu, & Hu (2016) however, the development and use of big data and big data analytics also come with challenges. Hiba *et al.* (2015) explained that the challenges with big data can be divided into two categories which are: semantic and engineering. According to them, semantic challenges deals with determining meaning and patterns from big data, while engineering challenges deal with data management activities that include storage and querying of data efficiently. According to Yaqoob *et al.* (2016), finding patterns that are relevant and are of interests from big data is also challenging due to the complexity and massiveness of big data. Data capturing, storage, analysis and visualisation are also challenges to big data (Philip Chen & Zhang, 2014). The security of data is also another challenge that comes with big data (Yang *et al.*, 2016).

3.4.8 Cloud Computing

Enterprise applications and supply chain systems such as Enterprise Resource Planning (ERP), Manufacturing Execution Systems (MES), Product Data Management (PDM) etc. rely on a central database. However, with the advances in Internet technology and the advent of mobile devices, these applications and systems are able to use Internet-mediated IT platforms, functionalities, capabilities and infrastructure to rapidly deploy computing powers (Son, Lee, Lee, & Chang, 2014). These Internet-mediated platforms, infrastructure and technology trend, coupled with the development of distributed storage, multi-core processors, decentralised computing, web service and virtualisation has led to a new type of computing model called cloud computing (Avram, 2014; Zhang, Yan, & Chen, 2012). This model provides and delivers IT resources as a utility that can be released to users on a need basis, through the Internet.

Cloud computing delivers computing as a utility, with the features of on-demand access, pay-as-you-go functionality, pooled resources, broad network access, elasticity and self-service functionality (Mell and Grance, cited in Wang, Liang, Jia, Ge, Xue *et al.*, 2016c; Yang *et al.*, 2016). It is a technology model that offers supply chains access to highly scalable and agile global information system and technology platforms in real-time. It eliminates the issues of software licenses and hardware infrastructure, and also, enhances disaster recovery and simplifies scalability (Bruque-Cámara, Moyano-Fuentes, & Maqueira-Marín, 2016). It also offers the latest technology and off-the-shelf IT functionalities and capabilities that can be instantly deployed and easily used regardless of location and time (Jede & Teuteberg, 2015; Son *et al.*, 2014). According to Singh, Mishra, Ali, Shukla, & Shankar (2015), the different deployment models of cloud computing has made its adoption easy for any type of organisational sector. As shown in the literature, cloud computing has four major deployment models, which are described below:

Private cloud: This is used to describe a cloud infrastructure or service which is owned and used by a single organisation (Bruque-Cámara *et al.*, 2016). According to Chen, Liang, & Hsu (2015), private cloud is also referred to as internal cloud, and with it, data, processes and infrastructure are managed within the organisation. It is considered to be a suitable approach for organisations focusing on data security and privacy. It is mostly used by large organisations. The downside of private cloud computing is that its implementation can be costly, time-consuming and complicated (Chang, Walters, & Wills, 2013; Jede & Teuteberg, 2015).

Public Cloud: Public cloud computing is used to describe a cloud infrastructure or service that is open and can be used to the general public (Bruque-Cámara *et al.*, 2016). According to Chen *et al.* (2015), the public cloud is also referred to as external cloud, and with it, resources are dynamically provided by a third-party service provider, over the Internet. The challenges of organisations with regards to public cloud computing include conflicts concerning ethical and legal issues, data loss and the security of data in a public domain (Chang *et al.*, 2013).

Community Cloud: Community cloud computing may be described as the cloud resources or services provisioned for exclusive use by a community of users or organisations that share similar interest or concerns such as policy, compliance, security requirements, mission etc. (Bruque-Cámara *et al.*, 2016; Gupta, Seetharaman, & Raj, 2013). The community cloud may be housed, operated and managed by any one of the members of the community or a third party organisation, not belonging to the community. The challenge with this deployment model is that it often takes several years to establish a working community that is willing to share information and resources (Chang *et al.*, 2013).

Hybrid Cloud: Gupta *et al.* (2013) described hybrid cloud as a combination of private and public cloud, while Bruque-Cámara *et al.* (2016) described it as the combination of any two or more of the other deployment models (i.e. private, public and community). Hybrid cloud virtualises a network of dispersed processes and resources in the supply chain, but allows the systems of the individual trading members to perform as a functional department of the organisation within the cloud environment. Also, according to Bruque-Cámara *et al.* (2016), when two or more deployment models combine to form a hybrid cloud, the individual/respective models maintain and retain their unique entity within the hybrid cloud, but they are bounded together by proprietary or standardised technology that enables application and data portability. The literature shows that when a hybrid cloud platform is integrated into supply chain functions, support for collaborative supply chain is provided for the individual organisations within the supply chain network. The downside of hybrid cloud computing is the difficulty involved in integrating different architecture (Chang *et al.*, 2013).

Cloud computing is service-oriented, and a combination of different pre-existing technologies (Avram, 2014). Its infrastructure and resources are often kept in distributed environments that are usually geographically dispersed (Bruque-Cámara *et al.*, 2016). Its resources and services are also usually shared and allocated using virtualisation technique (giving it virtually unlimited capabilities in terms of processing power and storage) that allows the execution of multiple Operating Systems (OSs), provides high server utilisation and facilitates fault-tolerance through the simultaneous deployment of infrastructure, software and platforms (Díaz, Martín, & Rubio, 2016). These resources and services "are delivered through industry standards such as service-oriented architecture (SOA)" (Singh *et al.*, 2015, p.464), and they can be accessed through application programming interfaces (API) (Xing, Qian, & Zaman, 2016), and web-based technologies on an on-demand basis (Bruque-Cámara *et al.*, 2016; Chen *et al.*, 2015).

Cloud computing can be adopted within supply chains as an IT paradigm and provision model to address the growing issues of information, information systems and business integration. It can also be adopted to support mass information sharing, management and cross-organisational collaboration in supply chains (Xing *et al.*, 2016). However, according to Avram (2014), the adoption of cloud computing is more complex than imagined, especially in the areas of system integration and interoperability. Cloud computing offers services that can be divided into three major models, which are: Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS) (Al-jawazneh, 2016; Bruque-Cámara *et al.*, 2016; Gupta *et al.*, 2013). These models have become relevant in enhancing the structures and processes involved in the management of supply chains, through the help of specialised supply chain management (SCM) applications that have been designed to be used with cloud computing infrastructures and services (Figure 3.3) (Khan, Li, & Yu, 2015). The models are described below:

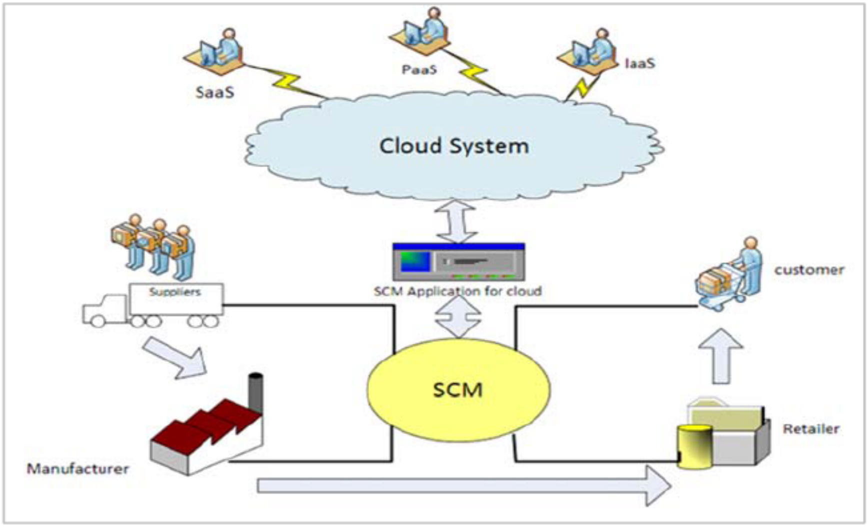


Figure 3.3: SCM Structural Design in Cloud Computing (Khan *et al.*, 2015)

Software as a Service (SaaS) model: With this cloud service model, the capability provided to users is to use the applications running on the cloud service provider's platform (Bruque-Cámara *et al.*, 2016). So, instead of installing applications or software on a client's machine and updating it with patches, the applications and software are made available over the Internet for the client's consumption (Gupta *et al.*, 2013). With this model, supply chain software and applications such as ERP and CRM are made available to users over the Internet, without the users having to install them on their machine (Gupta *et al.*, 2013). Hence, SaaS has made it easier for software and systems such as the ERP system, to outperform their similar traditional IT offerings.

In the systematic literature review done by Jede & Teuteberg (2015), it was stated that SaaS is the most common of the service models because it is considered the front-end for most end-users. SaaS is making it possible for IT software and applications to be accessible from any location through either a program interface or a thin client interface e.g. a web-based email (Bruque-Cámara *et al.*, 2016). This model is also making it possible for cloud services to support software and applications that are built and deployed over the Internet, by the cloud service provider. Examples of SaaS vendors are Microsoft Office Live, Salesforce.com, Google Apps, Gmail, Yahoo Mail, Cisco WebEx web conferencing, TurboTax Online, SuccessFactors (HRM tool) etc. (Al-jawazneh, 2016; Gupta *et al.*, 2013).

Platform as a Service (PaaS) model: With this cloud service model, the capability provided to users is to create applications (using programming languages, tools, services and libraries that are supported by the cloud service provider), that are run or deployed on the cloud service provider's infrastructure or platform (Bruque-Cámara *et al.*, 2016), through the use of middleware, application programming interfaces (APIs) etc. (Xing *et al.*, 2016). So, instead of buying platform licenses such as that of a software development kit (SDK) or tool (e.g. Python, .NET, Java etc.), they are made available to users over the Internet.

This model packages a computing platform that includes operating systems, web servers, databases, programming languages etc. (Chen *et al.*, 2015). Using PaaS for supply chain management helps minimise the cost of development and integration. Examples of PaaS are Microsoft Azure, Google AppEngine, Amazon Web Services (AWS), Rackspace cloud sites etc. (Al-jawazneh, 2016; Gupta *et al.*, 2013; Philip Chen & Zhang, 2014).

Infrastructure as a Service (IaaS) model: This refers to physical devices such as networks, storage devices, and servers that are physically located at a central location (usually data centre), and that are used and accessed over the Internet. With this cloud service model, the capabilities provided to users include to provision networks, storage, processing and other important computing resources, that enables a user to run and deploy software and applications (Bruque-Cámara *et al.*, 2016). This model uses an integrated environment of computing resources delivered over the network (Chen *et al.*, 2015). It also uses a virtualisation techniques to ensure efficient use of resources (Xing *et al.*, 2016). Examples of IaaS are Rackspace cloud server, Simple Storage Service (S3), Amazon EC2 (Elastic Compute Cloud), Terremark etc. (Al-jawazneh, 2016; Gupta *et al.*, 2013; Philip Chen & Zhang, 2014).

Organisations such as SAP, GT Nexus etc. are offering different cloud computing services and technologies for coordinating and enhancing different supply chain related IT processes (Jede & Teuteberg, 2015). These services and technologies are creating an environment that is making it possible for risks to be shared among supply chain partners (Goel, 2015). They are also providing organisations with the platform, software solutions and infrastructure to easily integrate their decentralised global supply chains (Jede & Teuteberg, 2015). Hence, if properly implemented, cloud computing can improve the agility and responsiveness of supply chain trading partners, especially under the condition of high and intense security challenges (that can be caused by the economic, political and technical differences between the regions in which trading partners are operating) (Jede & Teuteberg, 2015).

The adoption and migration to cloud computing by organisations is still in its infancy, and has also been slow (Wang *et al.*, 2016c). Likewise, the concept of cloud-based supply chain management is still new and hence considered to be at an infancy stage (Casey *et al.* cited in Al-jawazneh, 2016). Unstable and slow broadband network speed is hindering the adoption and diffusion of cloud computing in some countries. The availability, reliability and quality of service offerings, data lock-in, interoperability and the capability of the cloud service provider are also challenges affecting the adoption of cloud computing (Bruque-Cámara *et al.*, 2016; Díaz *et al.*, 2016; Son *et al.*, 2014; Wang *et al.*, 2016c). According to Díaz *et al.* (2016), information security is also a major reason most organisations are unwilling to adopt cloud computing. While, according to Philip Chen & Zhang (2014), privacy, with regards to the storage and hosting of data and information on servers that are publicly accessible, is also another challenge facing the adoption and diffusion of cloud computing.

3.5 Conclusion

Supply chain activities require the flow of information, cash and materials. However, organisations' ability to be competitiveness and also adapt to environmental changes is dependent on their ability to obtain market or customer information. The literature shows that accurate and timely information is required by organisations in order to effectively manage their supply chains' structures and processes. However, for information to be meaningful, it must be shared among the supply chain trading partners (Yu *et al.*, 2010). Information systems and technologies have made the sharing of information between trading partners more efficient and effective (Seth *et al.*, 2015). Hence, organisations are implementing and adopting information systems and technologies such as VMI, EDI, RFID, CRM, ERP, Big Data, Cloud Computing etc., to facilitate the sharing of information and the integration of their supply chain structures and processes. According to Denolf *et al.* (2015) however, implementing information systems across any supply chain network is complex (because of the number of participating actors involved in supply chains), and often comes with security challenges and risks. The next chapter presents the literature on information and information systems' security challenges and risks.

CHAPTER 4: INFORMATION SECURITY & ASSURANCE WITHIN SUPPLY CHAINS

4.1 Introduction

The need for information in enhancing the flow of material and fund within supply chains has made information become of great importance to supply chains. Likewise, the use of information systems for acquiring, storing, processing and sharing information has made information systems become an important tool in today's supply chains. Information and information systems have become important assets within supply chains. However, their security and management are continuously getting more challenging, as a result of the increasing amount of threats, disruptions and risks that they are constantly and continuously being exposed to (Lam *et al.*, 2015).

The adverse outcome caused by threats, disruptions and risks is causing a rise in the need for assurance that, the threats and risks to the information and information systems of individuals, organisations and supply chains, will be properly managed (Hamill *et al.*, 2005; Roy & Kundu, 2012). This chapter presents the literature on information (and also, information systems) threats, risks, security and assurance within supply chains. The compressed layout of the chapter is presented in Figure 4.1.

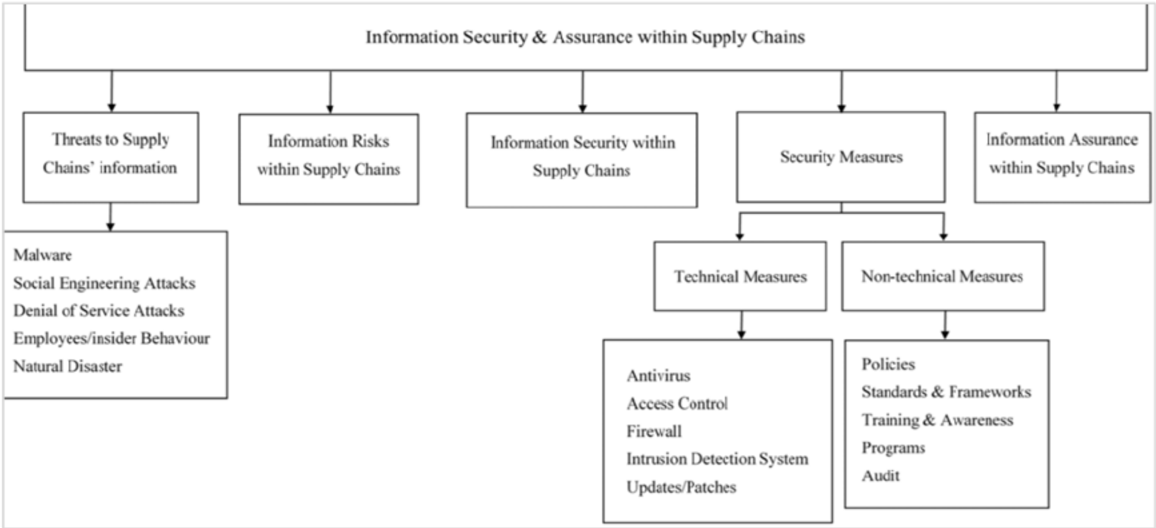

Information Security & Assurance within Supply Chains
Threats to Supply Chains' information
Information Risks within Supply Chains
Information Security within Supply Chains
Security Measures
Information Assurance within Supply Chains
Malware
Social Engineering Attacks
Denial of Service Attacks
Employees/insider Behaviour
Natural Disaster
Technical Measures
Non-technical Measures
Antivirus
Access Control
Firewall
Intrusion Detection System
Updates/Patches
Policies
Standards & Frameworks
Training & Awareness
Programs
Audit

Figure 4.1: Layout of the Chapter

4.2 Threats to Supply Chains' Information

As explained in the study of Hamill *et al.*, (2005, p.472), threat is "any circumstance or event with the potential to harm an information system or the information within, through unauthorised access, destruction, disclosure, modification of data, and/or denial of service.'' The threats to information and information systems are caused by different unexpected sources, and they are increasingly becoming more complicated and sophisticated. One of the causes of threats to the information and information systems within supply chains is the drive towards the establishment of an efficient global supply chain network. This drive is causing an increase in the length of supply chains and subsequently, causing supply chains to become vulnerable to different information threats (Wolden, Valverde, & Talla, 2015). According to Windelberg (2016), counterfeiting or tainting of information systems or any of their components (i.e. hardware, firmware, software etc.) is also a cause of threat to the operations of supply chains, because they lead to the compromise or the violation of the integrity of the information flowing within the supply chain.

Another source of increased threats to information and information systems within supply chains are the users of the information and information systems (Jouini *et al.*, 2014; Sindhuja & Kunnathur, 2015). Users' actions directly or indirectly cause security threats to information and information systems. Hence, according to Montesdioca & Maçada (2015), the dissatisfaction of users is a problem and threat to organisational information and information systems. The users' actions that directly or indirectly causes security threats to information and information systems has been divided into two categories, which are: Intentional (e.g. espionage, sabotage, theft etc.) and Unintentional (e.g. using a simple password, carelessly accessing compromised websites, floods, hurricanes, earthquakes etc.) (Crossler, Johnston, Lowry, Hu, Warkentin *et al.*, 2013; Speier, Whipple, Closs, & Voss, 2011). According to Speier *et al.* (2011), unintentional threats can also be a result of mad-made causes. An example of this is an accident (e.g. injury or transport oriented) that causes information distortion.

Threats adversely affect the confidentiality and integrity of information and the availability of information systems (Hamill *et al.*, 2005; Jouini *et al.*, 2014). Unfortunately, the degree and amount of security breaches, threats and attacks on information and information systems are continuously increasing. According to Hunton (2012), one of the reasons for the increase is financial gains, which, unfortunately, often leads to significant financial losses or organisational reputational damage. According to Sindhuja (2014) also, another reason for the increase in threats to information is the unparalleled trust and reliance on information systems. This is so because malicious attackers often capitalise on the reliance of users on information systems, as this serves as a major influence and factor for them to carry out their malicious acts.

In order to ensure the protection of information and information systems, there is a need for organisations and their employees to possess up-to-date skills and knowledge about vulnerabilities and threats, and also about ways of preventing, mitigating or managing them (i.e. the vulnerabilities and threats) (Choo, 2011). There is also a need for the categorization of threats, their causes and their impacts (Amoo Durowoju, Kai Chan, & Wang, 2012; Jouini *et al.*, 2014).

This categorisation makes it easy for organisations to develop strategies and measures that can help in the prevention of threats and the mitigation of their impacts. Similar to what was presented in the study of Jouini *et al.* (2014), the section below describes a hybrid threat categorization, which combines both the techniques (i.e. threat techniques) used by attackers and the effects of the techniques on information and information systems.

4.2.1 Malware

Malware has been consistently ranked as one of the most common form of security threat to individuals, organisations and government. Examples of malware are; ransomware, bot, spyware, adware, viruses, worms etc. (Martin & Rice, 2011; Stokes, Karampatziakis, Platt, Thomas, & Marinescu, 2014). They are considered to be a great danger, mostly to organisations, especially those that uses modern information systems and technologies. They usually contain instructions that when executed, provides malicious programs that can affect the performance of information and information systems within supply chains (Nishat Faisal, Banwet, & Shankar, 2007), by acquiring sensitive information within the supply chain. The instructions that malware contain can cause loss of privacy, unauthorised access to information, data theft etc. Hence, according to Lysne, Hole, Otterstad, Ø, Aarseth *et al.* (2016), the ability to distinguish between malware-infected and malware-free code is important in today's business environment.

Modern malware can be broadly categorised into two types, which are; the generic and customised information-stealing malware. Generic malware targets the general population while customised information-stealing malware targets specific individual, organisation or government. An example of generic malware is the "bot malware" which exploits vulnerabilities on the systems of individuals, organisations or government (Choo, 2011). This type of malware are hosted on servers, and when unsuspecting users connect to such servers, their system(s) may become infected and controlled by the manager of the botnet, often referred to as Botmaster (Bottazzi & Italiano, 2015) – this activity is also referred to as a "drive-by attack" (Choo, 2011). Systems infected with botnet are often turned into "zombies", that is, compromised systems waiting to be activated, through some command-and-control servers (C&C) and other various communication channels (Bottazzi & Italiano, 2015).

Customised information-stealing malware, as described earlier, is a targeted type of malware, and an example of it is the Zbot malware (Caballero, Grier, Kreibich, & Paxson, 2011). This malware can be purchased and then customised to build a different variant of malware. Choo (2011) explained that some customised information-stealing malware often has a phishing-based keylogger component in them. A phishing-based keylogger is a program that is designed to monitor users' activities such as keystrokes, and to harvests login credentials, account numbers, etc. to a collection server (Chauhan, Singh, & Chandra, 2013; Issac, Chiong, & Jacob, 2014). Once this information is collected, funds, for example, can be transferred from an account, using the harvested information, and by disguising as the legitimate user/owner of the account. The customised information-stealing malware can also be used to penetrate organisations and their supply chain network, in a way that allows access to workstations or servers within the organisation and also across the supply chain network.

Malware poses threat to the operations of supply chains by allowing the illegal transfer of the supply chain's proprietary information to competitors (Nishat Faisal *et al.*, 2007). According to Roy & Kundu (2012) and Bottazzi & Italiano (2015), the use of the Internet and emerging technology concepts such as cloud computing, for supply chain operations, has brought about an increase in the proliferation of malware onto the information and information systems of trading partners, and has also increased malware's potential as threats to the operations of supply chains. According to Nishat Faisal *et al.* (2007), amongst other things, the lack of information security policy within most supply chains, has not made the proliferation of malware attacks easy to manage. It (i.e. the lack of information security policy) has unfortunately become one of the common reasons for supply chain organisations' exposure to threats, and susceptibility to malware attacks.

There are no standard methods of detecting malware, in fact, some malware are almost impossible to detect, but, their negative impact can be limited. A signature-based technique that utilises fixed-code patterns to identify malware can be used to determine malware-infected and malware-free code (Issac *et al.*, 2014; Lysne *et al.*, 2016). This technique extracts the semantic and syntactic features and patterns of codes, and then subsequently create unique signatures that can match particular malware (Hsieh, Wu, & Kao, 2015). The weakness with this technique, however, is that its main purpose is to identify known malware, that means, new malware are never detected with this technique. Another technique that can be used to identify malware or infiltrate the C&C is the use of reverse engineering (Caballero *et al.*, 2011), which is a process of understanding how executable code was designed and what executable code does. This technique makes it possible to find faults in the executable codes, so as to limit their impact.

4.2.2 Social Engineering Attack

It is explained in the study of Choo (2011) that attacks on information, information systems and networks can either be syntactic, semantic or a combination of the two - often referred to as blended attack. A syntactic attack is the type of attack that exploits technical vulnerabilities in hardware and software, in order for a crime to be committed (Hathaway, Crootof, Levitz, Nix, Nowlan *et al.*, 2012). An example of this type of attack includes the installation of malware (described in section 4.2.1) on information systems, so as to gain access to information. Semantic attacks, on the other hand, are the attacks that exploit social vulnerabilities, so as to gain access to personal information (Heartfield & Loukas, 2013). These types of attacks (semantic) are carried out using social engineering techniques such as phishing, baiting, tailgating etc. Blended attacks, which is a combination of both syntactic and semantic attacks, are the attacks that are carried out "using technical tools to facilitate social engineering in other to gain privileged information" (Choo, 2011, p.724).

Social engineering attacks are mostly used to extract privileged and private information from victims, so as to cause problems such as identity theft and financial fraud (Issac *et al.*, 2014). Identity theft is a prevalent issue facing individuals, organisations and most supply chain networks. "One form of identity theft crime that has become a lethal security threat is phishing" (Issac *et al.*, 2014, p.1). Phishing is described in the study of Chauhan *et al.* (2013) as the luring of unsuspecting people into disclosing sensitive information such as their personal and/or financial information, for the purpose of identity theft or fraud. It uses unsolicited messages (delivered through emails, websites etc.) masquerading to originate from legitimate or trustworthy individuals or organisations, to deceive people into providing sensitive information that is used to facilitate and commit crimes (Choo, 2011; Li, Yin, & Chen, 2016).

Distributed spam, phishing and pharming attacks are all gaining notoriety and hence, increasing attention from individual organisations and their respective supply chain network members. Another attack gaining attention among organisations is session hijacking, which when conducted with the aid of social engineering is often referred to as session fixation (De Ryck, Nikiforakis, Desmet, Piessens, & Joosen, 2012). In this type of attack, the attacker lures the user to use sessions created by him/her, so as to allow for the takeover of the user's session after authentication. Also, in this attack, malicious software, in the form of browser component, are often installed by the attacker, such that when the user log in to perform a transaction, the installed malicious software takes over the user's session, once the user's credentials are proved to be correct with the transacting website (Issac *et al.*, 2014).

Encryption technique in java that saves the passwords of users in a database, and in an encrypted form, can be used to reduce the effects of social engineering attacks (Chauhan *et al.*, 2013). The use of a strong firewall and also looking out for the padlock symbol and "https" protocol in the address bar before entering any sensitive or personal information can also be helpful in preventing against falling prey to social engineering attacks (Issac *et al.*, 2014). According to Martin & Rice (2011), organisations can also reduce social engineering attacks and their impacts by installing security codes of practice, and by also monitoring electronic and physical access to sensitive information. Other means of managing social engineering attacks include users' education, training and awareness, implementing authentication mechanisms, and the patching of operating systems (O/S).

4.2.3 Denial of Service (DoS) Attack

Supply chain organisations are putting in place tight security measures to protect the information within their supply chain network. However, malicious individuals and organisations are using the vulnerabilities found in information systems to commit crimes such as DoS attacks, defacement, web hacking etc. against information systems, and consequently, against information (Wolden *et al.*, 2015). DoS attack is an attack that is designed to consume a reasonable amount of its target's available resources (e.g. network bandwidth, disk space, processing power or memory) so as to cause some form of service disruption (Chauhan *et al.*, 2013; Yuvaraj, 2015). This attack is used by malicious users to intentionally disrupt or slow down servers' services and operations, such that the legitimate users of such server(s) are denied access to the server's network and resources. Similarly, in supply chains, this attack interrupts the legitimate access of organisations to the supply chains' network, services and resources, hence, causing an interruption in the overall operations of the supply chains' member organisations (Nishat Faisal *et al.*, 2007).

One of the most common external attacks on supply chains is the DoS attack, which can be set up using bots (explained in section 4.2.1) (Lin, Hsu, & Cheng, 2015; Martin & Rice, 2011). According to Chauhan *et al.* (2013), the DoS attack, commonly known as packet flooding attack, is being increasingly reported by organisations to be affecting their operation, and invariably, their supply chain network's operations. This attack is carried out by sending of request (mostly unwanted) incessantly or by sending of large amount of packets to a target, to such a point where network bandwidth are being consumed and the legal users of the system cannot query or access the system as usual (Lin *et al.*, 2015). The packet flooding attack used by DoS attackers often comes in different types that includes Transmission Control Protocol (TCP) flooding (streams of TCP packets with different flags are sent to the target IP address), User Datagram Protocol (UDP) flooding (streams of UDP packets are sent to the target IP address) and Ping flood/ ICMP echo request/reply (streams of ICMP packets are sent to the target IP address) (Chauhan *et al.*, 2013).

According to Lin *et al.* (2015), supply chain practitioners and researcher should pay more attention to Dos attacks, and also increase the effort put in place to withstand DoS attacks. Similarly, according to Cheah (2015), they should also pay attention to Distributed Denial of Service (DDoS) which works similarly to DoS attacks, except that it tends to target limited, shared and consumable network environment. DDoS/DoS attacks are not easy to manage, however, in order to manage them, the security measures put in place by organisations must be robust and agile enough to be able to help prevent or react to them. According to Chauhan *et al.* (2013) as well, the maintenance of log files can also help in responding to DoS attacks. Zargar, Joshi, & Tipper (2013, p.2051) however, explained in their study that when DDoS/DoS flooding attacks are detected, "there is nothing that can be done except to disconnect the victim from the network and manually fix the problem."

4.2.4 Employees/Insider Behaviour

One of the reasons why information and information system security abuse and breach incidents continue to plague organisations is because of the organisational employees who constitute an insider threat to the organisations' information, and who are considered the vulnerable link in ensuring information security. Employees are the first line of defence in protecting information and information systems, but unfortunately, they are also the weakest link and consequently, a major threat to information security (Crossler *et al.*, 2013; Sindhuja & Kunnathur, 2015). As explained in the study of Ifinedo (2014), research has shown that organisations that fail to pay attention to the individuals within their business environment, may fail to achieve and sustain success in their effort to combat security threats and attacks. Hence, a beneficial approach to protecting and safeguarding information systems' assets and resources is that organisations pay attention to their own employees' behaviour and intentions.

According to Wolden *et al.* (2015), supply chain organisations should implement security measures that will be very effective from within the organisation. To achieve this, the supply chain member organisations should implement practices that can help manage the behaviour of employees, especially the behaviours that can cause harm to the organisation's information and information systems. One of the ways organisations and their supply chain partners can influence and manage the behaviour and intention of their employees with regards to the security of information and information system is through the use of guidelines, rules and requirements that are laid out in the form of policy (Ifinedo, 2014). Another way in which organisations can manage the behaviour of their employees is by establishing practices and activities that can ensure that employees understand and adhere to the countermeasures, capabilities and limitations that are put in place to reduce or counter threats (Wolden *et al.*, 2015).

Furthermore, to reduce and manage the potential threats that can be caused by employees, Angeles (2009) suggested that the people with appropriate qualifications, experience and skills should also be employed within the organisation. Especially, those that will be responsible for the creation, maintenance and support of the information system infrastructure that is used to produce and manage the information used to support the achievement of the overall organisational strategies and objectives. Similarly, it is stated in the study of Zailani, Seva Subaramaniam, Iranmanesh, &

Shaharudin (2015) that the screening and employment of the people with the appropriate qualifications and skills is an important aspect of ensuring that security policies and practices are adequately followed and utilised. This also helps reduce the number of employees that can cause or be a potential threat to information and information systems.

The misuse and abuse of information and information systems' resources by employees has been identified as major sources of vulnerability to supply chains. Employees with low loyalty to the organisation may deliberately misuse or abuse information and information system or may undertake acts that can sabotage and impair the security activities of the organisation and its supply chain. To reduce the possibility of threats and also possibly address the information security challenges that can be caused by employees, Ifinedo (2014) suggested that organisations should adopt the following practices:

Rewards and incentives: should be used as a means of encouraging employees to become more conscious of information security issues and also become more compliant with information security measures.

Security education, training and awareness: should be used to orientate (or re-orientate) the employees that are identified or perceived to have negative perception or belief about security issues.

Regular group meeting: should be used to help enlighten and continuously remind employees of the consequences of their actions toward security breaches, threats and attacks.

Co-worker socialisation: should be established as an activity within the organisation. This activity should be used to provide an environment where employees can learn the importance of security measures through their co-worker.

Creation of knowledge environment: should be used to encourage employees to take it upon themselves to improve or develop the necessary knowledge and skills that are required in protecting and safeguarding the organisational information and information system assets.

Establishment of social consciousness: should be adopted because employees are more likely to comply with security regulations when they perceive or believe that their compliance with the regulations is a social issue that benefits everyone in the organisation.

Use of notable/influential people: notable or influential people who are capable of motivating or shaping the opinion and perception of others should be tasked within organisations to champion the cause of employees' compliance with information security measures.

4.2.5 Natural Disaster

Natural disasters such as hurricanes, tsunamis and earthquakes are a huge threat to supply chain operations because they disrupt the resources (especially information and materials) that flow within supply chains. This is a type of threat that organisations do not often put so much effort into, with regards to preventive and reactive measures. This is because this type of threat is perceived to have a low probability of occurrence (Park, Min, & Min, 2016). Although, because of occurrences of this type of threat (natural disasters), organisations such as Ericsson, Apple, Honda and Toyota have been forced to reduce or completely stop their production for a while (after the occurrence of a natural disaster), even in the plants that are unaffected by the natural disaster (Ho *et al.*, 2015; Li *et al.*, 2015; Todo, Nakajima, & Matous, 2015). Production at unaffected plants are often stopped because the supply of parts or components from the affected part would have been disrupted when the natural disaster occurs, and this affects production at the unaffected locations.

Natural disasters do not only directly disrupt supply chain information, their after effects can also have a devastating effect on the information and operations of the overall supply chain. The after effect of a natural disaster can be found in the case of the earthquake and tsunami which happened in Japan in 2011 and the flooding in Thailand which happened in the same year, in which power outage, information loss, road closure etc. prevented organisations from committing to the full restoration and quick recovery of their supply chain (Ivanov, Sokolov, & Dolgui, 2014; Park, Hong, & Roh, 2013). This subsequently affected the operations of the global supply chain. The length and extent of a supply chain network increases the vulnerability of the supply chain information to the disruptions caused by natural disasters. It can also negatively affect the IT disaster recovery plans put in place within the supply chain network. It can, however, also be of immense help to the recovery from natural disasters through the provision of extensive support from the unaffected organisations within the supply chain network (Todo *et al.*, 2015).

The effects of hurricane, tsunami, earthquake and fire on supply chains' information, structures and processes are making organisations consider the management of natural disasters as a critical capability and factor in the continuous operation of their supply chain (Ivanov *et al.*, 2014). These effects are also making organisations think seriously about data backup and mirror sites so as to keep information flow uninterrupted in their supply chain (Nishat Faisal *et al.*, 2007). Furthermore, they are also making organisations think of running (locally and internationally) integrated information systems that can help with the synchronised coordination of information sharing during crisis situations (Park *et al.*, 2013). These information systems are meant to enable supply chain organisations to react flexibly to any disruptions to information flow, which are caused by natural disasters. According to Hohenstein, Feisel, Hartmann, & Giunipero (2015) as well, organisations are also being forced into developing resilient and agile supply chain structures and processes that can quickly recover from the occurrence of disruptions and natural disasters.

Organisations should develop or adopt recovery policies for responding to natural disasters (Ivanov *et al.*, 2014). These policies should emphasise flexible collaborative reactive practices and also suggest supply chain solutions for assessing the impact of disruptions on the supply chain information. Park *et al.* (2013) presented a model called Supply Chain Design Information (SCDI) and suggested its adoption in responding to the supply chain disruptions caused by natural disasters. The model proposes the use of three elements in the management of natural disasters. The elements are; *an integrative manufacturing information system (IMIS)* – helps to respond to the needs of customers during disaster crisis, through strategic design information planning and business process integration, *a collaborative electronic database infrastructure (CEDI)* – helps with the provision of IT resources (especially information) that are needed during crisis management stages, and *portability provision in supply chain information flow* – helps with the provision of the flexible information flow that are required during unexpected supply chain disruptions and natural disasters.

4.3 Information Risks within Supply Chains

The increasing length and complexity of today's supply chains are causing an increase in the distortion of information and the disruption of the information systems used within supply chains. This increasing length, however, according to Day (2014), is also an important factor in the resilience of information to different distortions and risks. A distortion to the flow of information and a disruption in the operations of information systems often present risks to the overall information available for use within supply chains. They can also lead to service failure, increase in cost, and subsequently, cause a decline in performance. According to Thomé *et al.* (2016), the realisation of the negative effects of information distortion and information systems disruption has made risk become a concept of growing interest to researchers and practitioners. Hence, numerous studies are being done to understand the impact of information and information systems' distortions, disruptions and risks on supply chains' operations.

Organisations are continuously looking for means of managing information risk and at the same time ensuring that they meet the regulatory and governance requirements of the country or countries in which they are operating (Bunker, 2012). Managing supply chain information risk often incorporates supply chain risk management approaches. According to Wakolbinger & Cruz (2011), supply chain risk management approaches can be divided into demand management, supply management, product management or information management. They further explained that information management as a supply chain risk management approaches promotes the opportunity to implement supply chain risk management best practices that can facilitate the identification and management of the disruptions and risks to the supply chains' information and information systems.

Information risks in supply chains can be easily managed if information is shared among the trading partners. This is because, according to Wakolbinger & Cruz (2011) and Chang *et al.* (2015), information sharing allows for the identification, assessment and management of potential risks to supply chains' information. Information risks in supply chains can also be managed through collaboration among supply chain members (Nishat Faisal *et al.*, 2007; Sindhuja & Kunnathur, 2015; Wakolbinger & Cruz, 2011), and by encouraging the development and use of risk-sharing contracts among trading members (Wakolbinger & Cruz, 2011). Supply chain information systems' risks, on the other hand, can be managed by interface standardisation of information system and by allocating adequate decision rights to the IT unit of the organisations within the supply chain (Xue, Zhang, Ling, & Zhao, 2013).

The type of information systems used to share information, and how secured the information systems are, is an important determinant of the resilience of information to different distortions and risks. The use of information system to reduce risk or ensure the security of information is however, not often guaranteed. This is because, disruptions to information systems could interrupt access to the information being acquired, processed and stored by the systems (Baldini, Oliveri, Braun, Seuschek, & Hess, 2012; Windelberg, 2016). Roy, Gupta, & Deshmukh (2012) also explained that the disruptions to information system could increase the risks of potential data loss, information vulnerability, availability and intrusion, and it could also make it challenging for organisations and their trading partners to make informed business decisions.

One of the causes of potential risk to supply chains is the lack of adequate protection of the information systems used within the supply chains (Amoo Durowoju *et al.*, 2012). According to Montesdioca & Maçada (2015), the dissatisfaction or non-acceptance of information systems by users is also a cause of potential risk to supply chains. Another cause of potential risk to supply chain that mostly affects the overall supply chain information systems is the improper or inadequate implementation of the information system in any of the other organisations in the supply chain network (Xue *et al.*, 2013). This is so because the inefficiencies of such organisations' information system, affects the overall supply chain. Xue *et al.* (2013) further explained that the fact that the successful implementation of information systems requires that organisations adapt to various external constraints, which are often beyond the organisation's control, is also a cause of potential risk to supply chains' information and information systems.

The literature shows that information risk analysis is important in understanding the risks that information and information systems could be exposed to. According to Karabacak & Sogukpinar (2005), the driving force for information risk analysis is no more just technology. Policies, legal and governance factors are also now being considered as driving forces in the analysis of information and information system risks. According to Bojanc & Jerman-Blažič (2008), once risks have been identified, analysed and assessed, one of the following strategies may be chosen in order to manage the risks that information is being exposed to:

Avoidance: This risk management strategy is mostly applied when the severity of the impact of risk occurrence outweighs the benefits that are derived from acquiring information or from using an information system. This strategy is implemented by eliminating the exposure to risk or by eliminating the source of the risk. An example of avoidance as an information risk management strategy is when an organisation discontinue the collection of personal identifiable information (PII) such as credit card number or passport number, so as to avoid the risk of such information being stolen in an information security breach incidence.

Reduction: This strategy is mostly applied when mitigation is the primary objective of the risk management strategy. The strategy is implemented by reducing the exposure of information to risk. Hence, it is implemented by adopting appropriate tools and technologies (such as anti-virus systems, firewall, etc.) or by implementing appropriate security policies (such as access control, passwords, port blocking, etc.).

Transfer: This refers to transferring the risk to a third party organisation. In this case, the risk responsibility is partially shifted to another organisation. This strategy is increasing being adopted by organisations, especially in cases that involves information. An example of this strategy can be seen in the recent trend of organisations subscribing to keeping their information in the cloud infrastructure of a cloud service provider (CSP). This is so that the CSP can be responsible for the safekeeping of such information.

Acceptance: This is a strategy for organisations willing to retain the cost and responsibility of risks. It is a reasonable strategy for the type of risks that the cost of investment against the risks outweighs the total losses sustained in the long run, in the event of the risk occurring.

Managing supply chain information risks requires the collective effort of the supply chain members. Hence, the level of trust among the supply chain trading partners is a determinant and a requirement of how the organisations within a supply chain network can mitigate uncertainties and reduce information risks (Li *et al.*, 2015; Nishat Faisal *et al.*, 2007). This is so because, when there is trust among the supply chain trading partners, information and information systems' distortions, disruptions and risks are easily and quickly shared within the supply chain, and hence, are promptly managed before they cause substantial damage to the supply chain's structure, processes and operations. The top management's willingness and commitment to take up risks also determines how successful an organisation will be able to manage information and information system risks (Nishat Faisal *et al.*, 2007; Seth *et al.*, 2015).

4.4 Information Security within Supply Chains

Security in supply chain entails the reduction of the risk of losses caused by information and information systems' misuse or intrusion (Roy & Kundu, 2012; Sindhuja & Kunnathur, 2015). Hence, security is essential to supply chains. The attributes of security are confidentiality, integrity, authentication, availability and non-repudiation, and its objective is to reduce the risks associated with the confidentiality, integrity and availability of information and information systems (Fuchs *et al.*, 2011). According to Hamill *et al.* (2005) and Ouedraogo, Khadraoui, Mouratidis, & Dubois (2012), the thought of producing information systems that are secure and that will remain 100% secure over time, so as to protect information, is the desire of information system developers, however, the implementation of this thought is often considered impracticable due to the continuously changing system environment and the difficulty in determining or predicting, during the developmental process, the possible future threats to information and information systems.

Information security is a major concern to organisations because it is a determinant of how coordinated the processes and functions within the organisations' structure will be (Xiao-yan, Yu-qing, & Li-lei, 2011). According to Kolkowska & Dhillon (2013), information security is the application of technical (e.g. firewalls and anti-virus) and non-technical (e.g. policies and standards) measures to the protection of information. It has also been described by Fuchs *et al.* (2011, p.748) as the way of "protecting information and information systems from unauthorised access, use, disclosure, disruption, modification, or destruction". Furthermore, it has been described by Cherdantseva & Hilton (2014) as a professional activity and a multidisciplinary area of study that involves the development and implementation of different types of security countermeasures (technical, legal, human-oriented and organisational) that can help with the preservation of information and the protection of information systems.

Organisations are often concerned about information security breaches because of their far-reaching effect on the organisations' interaction with their consumers and partners, and also, because of their effect on the supply chains' operations (Blos, Hoeflich, Dias, & Wee, 2016; Windelberg, 2016). According to Nishat Faisal *et al.* (2007), organisations are also concerned about security breach to information and the information systems used for acquiring, storing, processing and sharing information, because they understand that any security breach to information or information systems could be detrimental to the supply chain network's ability to be competitive. According to Wolden *et al.* (2015), supply chain information and information systems are no stranger to cyber crimes, threats and security breaches, and thus requires security framework in fighting and preventing them from attacks.

Security framework in supply chains can help balance between the design and structure of security enhancing measures (Wolden *et al.*, 2015). In the study of Speier *et al.* (2011), a security framework (Figure 4.2), security was developed. The explanation of the framework shows that security breaches "occur when there is a highly motivated offender, a suitable target at an available location, and/or an absent or insufficient guardian" (p.724). The explanation further shows that organisations need to identify and understand the vulnerabilities within their information systems that could attract an attacker. They should also identify and understand the part of information and the component of information system that could be targeted by attackers. Furthermore, they should identify and establish appropriate measures for the protection of information and information systems from security breaches and threats.

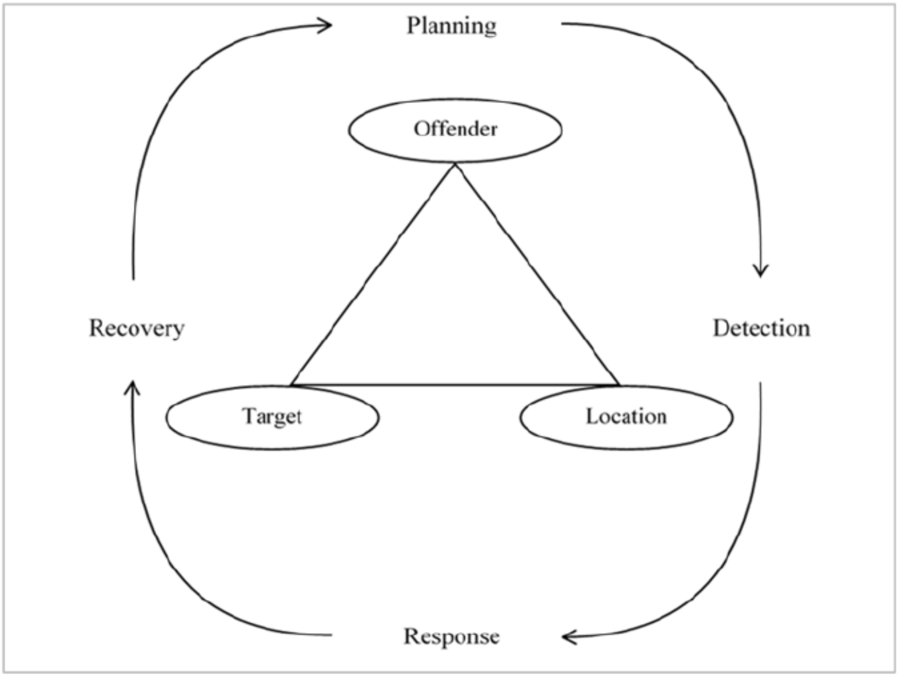


Figure 4.2: Supply Chain Security Framework (Speier *et al.*, 2011)

Ensuring the security of information and information systems does not only protect information but also protects information users. However, nearly half of security violations happen from within the organisation (Crossler *et al.*, 2013). Hence, according to Bunker (2012), people and processes should be considered as critical components in ensuring the security of information. Similarly, according to Da Veiga & Eloff (2010), organisations' approach to ensuring the security of information should involve dealing with employees' and their behaviour. This is because employees' behaviour is an important factor that determines the success of security measures.

Bunker (2012, p.20) in his work stated that organisations should cultivate the culture of asking their employees the important question of "if this information was about you, what additional steps would you take to protect it?" This question often helps re-direct the mind of employees, especially those with a nonchalant attitude towards the security of information.

One of the problems with security is that organisations under-report security crimes (Hunton, 2012), or are even sometimes reluctant to report the crimes due to reasons such as the fear of negative publicity and the fear of becoming less competitive (Choo, 2011; Sindhuja, 2014). The reliance of organisations on audit or risk management committees that have individuals with few or no IT specialist, knowledge or background, attending to issues such as information security is also a problem to information and information system security. This is because making security decisions on the basis of lack or incomplete knowledge has been identified by Cherdantseva & Hilton (2013) as one of the major causes of most security issues. The cost associated with the protection and security of supply chains is also another problem to information and information system's security (Speier *et al.*, 2011; Yang & Wei, 2013).

The role of top management in the management and security of information and information systems has been emphasised extensively in the literature. Speier *et al.* (2011, p.728), in their study, stated that "top management must be visible in their commitment and dedication to implementing security initiatives". They also stated that the commitment of executives to security and the fostering of security culture is a required condition for the establishment of an effective security environment. This is also indicated in the study of Montesdioca & Maçada (2015), where it was explained that for the implementation and adoption of information security practices to be successful, there must buy-in and support from top management. This is because they are in a better position to formulate mechanisms and strategies that can be used in the protection of information and information systems from existing and new security threats. They are also in a better position to approve decisions relating to information security.

4.5 Security Measures

Empirical evidence shows that the number of threats and risks incidents affecting and relating to the security of information and information system will continue to increase and proliferate. Hence, the implementation of security measures has become paramount to the effective and efficient use of information and information systems. The implementation of security measures helps manage the threats associated with the increasing adoption of information systems. It also helps organisations reduce internal information threats, and more importantly, threats from outside of the organisation. Although, according to Wolden *et al.* (2015), even with security measures in place, the chances of an attack taking place still exists, because malicious end-users are always finding security loopholes in information systems so as to commit a crime.

Attackers of information and information systems are getting sophisticated by the day, and are consequently, continuously developing innovative and evolving attacking techniques that are being used to circumvent security measures and controls. These techniques are causing the business environment to continuously experience an evolving and dynamic threat landscape (Borum, Felker, Kern, Dennesen, & Feyes, 2015; Choo, 2011). Hence, according to Ouedraogo *et al.* (2012), information security experts and practitioners fear that today's state of the art security measures, protocols and protection mechanisms might be easily bypassed in the nearest future. To reduce this fear, Ouedraogo *et al.* (2012) suggested that organisations should have confidence in their security measures, and the confidence should be based on the fact that:

- ➢ The security measures that were/have been identified as important in the risk assessment process are being/has been adopted and put into operation.
- ➢ The security measures are correctly configured and are functioning optimally at any given time
- ➢ No known vulnerability of information or information systems and their components, which can affect the security measures have been left unattended or unmitigated.

It is important for organisations to have practices or mechanisms that can ensure the proper implementation of information security measures. Such practices or mechanisms should, however, not be complex because complex security practices or mechanisms are often perceived as a barrier to the acceptance and usage of security measures (Ifinedo, 2014). Similarly, according to Hariga *et al.* (2014), such practices or mechanisms should be related to industry and security standards. They should also entail a properly developed information security program that would be able to facilitate the identification of potential threats to the organisational environment and to the supply chain network. According to Ouedraogo *et al.*, (2012), two important checks can be performed in order to determine the effectiveness and efficiency of security programs, practices or mechanisms on information and information systems. The checks are:

Availability Check: This is a check that determines, monitors and confirms the presence and availability of security mechanisms and protective measures. It should be the first activity to be performed before going on to determine the effectiveness and efficiency of any protective or security mechanism(s). Non-availability of protective measures or security mechanisms simply makes it impossible to check for the effectiveness of any security measure(s).

Conformity Check: This is a check that determines, monitors and measures the compliance of security mechanisms and protective measures against predefined policies or industrial standards. The policies could be internal policies of the organisation or policies that govern the industrial practices of the organisation.

A common source of security risk to information and information system that is sometimes overlooked is the improper implementation of security measures, and in cases where security measures are properly deployed, unidentified threats within the organisations' environment could render the measures less effective (Ouedraogo *et al.*, 2012). Security measures should be based on visibility, such that information that is accurate and can help in mitigating vulnerabilities can be generated (Wolden *et al.*, 2015). To achieve this though, users should be made to understand the importance of security measures and the practices and controls used for securing information and information systems. This was also echoed in the study of Da Veiga & Eloff (2010) where it was emphasised that the organisational culture and the employees' understanding and behaviour towards information security measures and practices are determinants of the effective use of the security measures put in place within the organisation.

According to Zailani *et al.* (2015), there are two categories of security measures. They are the preventive and corrective measures. The preventive measures focuses on minimising vulnerabilities and threats, and also on preventing the occurrence of risks. While the corrective measures focuses on limiting the impact or adverse effects caused by the occurrence of risks. Another two categories of information security measures that were identified in the study of Kolkowska & Dhillon (2013) and Sindhuja & Kunnathur (2015) are the technical and non-technical security measures. According to these authors, information security measures should include the application of both technical (e.g. firewalls, Intrusion Detection System (IDS) and anti-virus software) and non-technical (e.g. policies and standards) measures. Bulgurcu, Cavusoglu, & Benbasat (2010) also shared this opinion by stating that the success of security measures can be achieved only when organisations invest in both technical and non-technical resources.

4.5.1 Technical Measures

To ensure information security and reduce risks, organisations often rely on technical measures or technology based solutions (Bulgurcu *et al.*, 2010). Technical measures protect an organisation's hardware, software and information from being intercepted, interrupted, modified, disclosed, destroyed or fabricated. They also help "set up network security controls and cryptographic techniques for the smooth, uninterrupted and secured flow of information along the supply chain" Sindhuja & Kunnathur (2015, p.485). However, as important as technical measures are, they are rarely sufficient in providing a complete protection to organisational information and information system resources (Ifinedo, 2014). According to Da Veiga & Eloff (2010) and Sindhuja & Kunnathur (2015), technical measures can include prophylactic mechanisms such as firewall, Intrusion Detection System (IDS) and anti-virus that are used to protect hardware, software and information. They can also include access control mechanisms such as password and biometric controls that are used to ensure authorised access to information and information systems. These technical measures are further explained below.

4.5.1.1 Antivirus

Organisations and their supply chain trading partners are continuously and increasingly facing several new breeds of malicious programs such as viruses and worms, which are getting more sophisticated and dangerous. These programs are no longer simply damaging files but are also attacking trading organisations networks by exploiting vulnerabilities such as known default passwords, HTTP input validation flaws and buffer overflows (Gordineer, 2003). One of the information security management practice that has been identified by different individuals, organisations and standards in the management of malicious programs is the use of anti-virus software (Singh, Gupta, & Ojha, 2014). Anti-virus software are computer software programs that are used to respond to disruptive actions, and to prevent or recover from virus infections and attacks (Speier *et al.*, 2011; Sung, Ku, & Su, 2014).

Malicious programs have the tendency to spread rapidly within organisations, without any human interventions (Gordineer, 2003). After spreading and affecting an organisation, they subsequently often spread and affect the organisation's supply chain members and their respective workstations, servers and network. With anti-virus software, organisations can protect their workstations and servers, and also invariably, protect the workstations and servers of the organisations within their supply chain network. To achieve this though, the continuous and timely update of anti-virus software is very important. This is because the update of anti-virus software and their respective signatures determines the effectiveness of the operations of the anti-virus software. It also determines the immune level of the software to viruses (Sung *et al.*, 2014), and the ability of the software to be able to prevent emerging malware attacks.

Hackers often utilise techniques such as code obfuscation, packer and emulator detection to evade their malware from being detected by anti-virus software. To reduce the effect of these techniques, anti-virus software uses detection methods such as Static analysis, permission-based analysis and behaviour checking in malware detection (Hsieh *et al.*, 2015). Also, to minimise the effects of malware, most organisations use multiple layers of anti-virus protection such as a gateway, server and even desktop (Gordineer, 2003). In addition to this, most organisations also configure their anti-virus software for automatic virus scanning on their networks and servers. However, the challenge with the automatic virus scanning of the anti-virus software is that it slows down the operation and processing capability of the servers and the systems on the network, hence, some organisations have had to cancel this functionality of their anti-virus software (Workman *et al.*, 2008).

4.5.1.2 Access Control

Access controls are a very important component of information security. According to Fuchs *et al.* (2011), one of the most important ways of ensuring information security, and that is also considered as one of the most pervasive and fundamental mechanism in information assurance is "Access Control". Access controls are important in the protection of information and information system assets from unauthorised access, retrieval, modification, disclosure or use, and consequently, from disruption and destruction. They are also important in ensuring that the level of accessibility to the different types of information and information systems used within an organisation and across the organisation's supply chain network is properly controlled (Sindhuja & Kunnathur, 2015). However, according to Morris, Tanner, & Alessandro (2010), access controls are not entirely sufficient in ensuring the safety of information or information system.

Supply chain organisations are adopting the use of proper and effective logical access controls in their quest to ensure the security of information. This is because access controls help in "the management of admission to system and network resources" (Fuchs *et al.*, 2011, p.748). These organisations are also adopting the use of proper authentication for the external connections to their network, so as to ensure that access is being granted to the appropriate individuals or organisations. One of the authentication and access control measure being used is "password". Passwords are used to prevent unauthorised access into organisation's systems and network, and also to restrict access to organisational information (Mujeye, Levy, & Mattord, 2016). As explained in the study of Ahlmeyer & Chircu (2016), other authentication methods being used by organisations are the Kerberos (used for verifying users) and X.509 (an encryption authenticator).

Access controls limit the type of information that can be requested and the type of person that can request such information, however, they do not control or determine how the information being accessed is subsequently or eventually propagated or used (Morris *et al.*, 2010). Hence, according to Workman *et al.* (2008), it is the responsibility of users and organisations to ensure that their sensitive information is guided and protected from unauthorised access. To ensure this, users and organisations are encouraged to have strong passwords that will include numeric values, case alterations and designated range of characters such as special ASCII characters (e.g. asterisks, ampersands etc.). They are also encouraged to ensure that the passwords are not shared, are well protected and are frequently updated. The frequent updating and protection of passwords are a practice that should apply to all types of access control and authentication measures.

4.5.1.3 Firewall

Organisations are encouraged to install firewalls so as to prevent their network and information system resources from being breached by attackers. According to Tseng, Lo, Liu, Chang, Merabti *et al.* (2016, p.2), “a firewall is a network security gateway separating an internal private network from other external public networks.” In the study of Ifinedo (2014), it is encouraged that organisations deploy firewalls because they help with perimeter defence, by monitoring and providing access control to organisations’ inbound and outbound network connections and traffic. Similarly, in the study of Ahlmeyer & Chircu (2016), it is explained that firewalls should be deployed because they help organisations limit their communication to only known and trusted hosts. According to Borum et al. (2015) however, investing in firewall only, is by itself not sufficient in protecting informational assets from threats. Hence, Ahlmeyer & Chircu (2016) suggested that firewalls should be deployed with other intrusion detection mechanisms.

In order to ensure that access to information, information systems and network resources are granted to only the IP addresses that exist on trading organisations network, and to also ensure that access is granted to the list of IP addresses that have been assigned to the partners/associates of the organisations within the trading network, organisations are deploying firewalls as a security mechanism within their trading network (James, Grosvenor, & Prickett, 2004). Within the trading networks and their other different supply chain associates, firewalls are sometimes being implemented on either side of the servers of the trading organisations. This practice help to prevent unauthorised access from a remote location into the trading organisations network. According to Workman *et al.* (2008) however, the use of firewall is still a challenge to organisations and their trading partners because attackers of information systems are always finding means of circumventing firewalls.

Firewalls follow a set of pre-defined rules and security policies that are used to ensure the protection of organisations internal network. These policies are defined in such a way that a firewall can either reject, accept or drop any connection that is passing through it. As explained in the study of Tseng *et al.* (2016), the earlier firewall technology used packet-filtering technology, which uses packet header information to determine what packets to allow or drop from flowing through the firewall. The limitations (e.g. only checks packet header information and keeps no record of connection) of this technology led to the emergence of proxy firewall, which requires that all information being communicated must flow through a proxy server that has firewall deployed on it. With the advances in firewall design and development though, firewalls can now be used to “protect the outside from packets flooding attacks that originates from within a network”, a concept known as reverse firewall (Zargar *et al.*, 2013, p.2053).

4.5.1.4 Intrusion Detection System (IDS)

To protect organisations from security breaches and attacks, there is a need for a full-fledged system and network analyser, which can scan and monitor organisations' IP addresses and their network activities (Chauhan *et al.*, 2013). Monitoring is an example of a measure that can be used to bridge the gap between security threat and security measures (Ifinedo, 2014). To carry out monitoring activities, one of the systems being deployed by organisations is the intrusion detection system (IDS). IDS is used to detect and monitor organisations' perimeters for any potential external penetration. According to Zargar *et al.* (2013), IDS learns the normal behaviour and pattern of either the application-level or network/transport level traffic. To achieve this, some IDS use artificial intelligence and data mining techniques. IDS also monitor the features of the traffic flows at various intervals and location within the organisation. Based on what they have learnt and the information they have gathered during the monitoring process, they can detect any changes in the usage and traffic patterns of organisations' resources.

The assumption that most threats come from outside of organisations' boundaries has made organisations increasingly deploy IDS to monitor their inbound traffic. With this assumption, the deployment of IDS is often deemed as a valid preventive security breach measure within supply chains, but not a complete security measure (Bottazzi & Italiano, 2015). The idea of IDS not being a complete security measure is also echoed in the study of Borum et al. (2015), where it was stated that investing in IDS is an appropriate information security measure but it is not sufficient in protecting information from threats and cyber crimes. Even though IDS is not considered a complete security measure against information threats, organisations are still, however, encouraged to deploy it, as it will help prevent their network and systems from being compromised by external malicious individuals or organisations (Zargar *et al.*, 2013). It will also help in the defence against attacks such as DoS and some forms of malware (Yuvaraj, 2015).

4.5.1.5 Updates/Patches

To address vulnerability issues in information system and technology related product, vendors often release security updates and patched. One of the reasons for the release of these updates and patches often includes the provision of new codes that improves performance, that fixes bugs, that adds new functionality to software and hardware, and that provides new protection mechanisms that help manage security threats or attacks (Lysne *et al.*, 2016). Hence, according to Issac *et al.* (2014), security updates and patches hardens users' information systems against security breaches and attacks. They (i.e. security updates and patches) help protect organisations and their respective supply chain member organisations from being exposed to potential malware and cyber threats (Martin & Rice, 2011). They, therefore, have become important to today's organisations and their respective supply chains.

Unpatched or not up-to-date systems are a danger to any individual or organisation because they can be easily exploited by malware (Choo, 2011). Hence, according to Issac *et al.* (2014), updating the signature of security software on a regular basis is important. This is also echoed in the study of Singh *et al.* (2014), where it was stated that organisations information security management practices should include the regular update and patching of security software such as anti-virus, so as to ensure that they (i.e. security software) are kept up-to-date with the latest preventive or reactive codes. Being up-to-date also ensures that these security software are capable of safeguarding against emerging threats. Device drivers, system and application software such as operating systems and Adobe Flash should also be updated on a regular basis (Lysne *et al.*, 2016). Browsers should also be kept updated at all times with critical and recent security updates, as this help in the fight against online threats and attacks (Issac *et al.*, 2014).

Martin & Rice (2011) reported a study conducted by Symantec that shows that 37% of home users and SMEs do not security update or patch their operating systems or application software. According to Bojanc & Jerman-Blažič (2008), a reasonable number of security breaches and attacks could be avoided or prevented if information systems and their hardware, software or applications are kept up-to-date with appropriate security updates and patches. An example of this can be seen in the case of the Nimda worm, which appeared in 2001 and infected several computers within a short period of time after its appearance (Rajesh, Reddy, & Reddy, 2015). This worm or its negative effects could have been prevented or avoided if the patches (which were available) for fixing the worm's vulnerability was downloaded and installed by organisations on their network or systems before becoming infected.

4.5.2 Non-Technical Measures

In the protection of information and information systems, it is important to consider a variety of countermeasures that are not limited to technical measures only. This is because, technology is not enough in addressing the security issues of information and information systems (Bunker, 2012). According to Bang, Lee, Bae, & Ahn (2012), behavioural issues that involve users should be considered in the security of information and information systems. While, according to Da Veiga & Eloff (2010), a reliable internal process and a good corporate governance practice that is built on well-structured policies and standards should be considered as an important requirement in the protection of information and information systems. In the study of Sindhuja & Kunnathur (2015), non-technical measures were identified as formal controls that are often rule-based, and that serves as the basis for the adoption, implementation and enforcement of the technical measures. Some of the non-technical measures that can help with information security are explained below.

4.5.2.1 Policies

Information access is made safe, and the confidentiality and reliability of information are also ensured when suitable information security controls such as policies, procedures and regulations are put in place (Xiao-yan *et al.*, 2011). Policies are an important component of any supply chain network because they can help in reducing the impact of distortion, disruptions and threats to the members of the supply chain network. The findings in the study of Wolden *et al.* (2015) shows that with the proper implementation of policies and regulations, organisations can effectively prevent or mitigate against the threats and risks of attacks on the supply chain information and information systems. Hence, the policies and regulations in place within organisations and within supply chain should be properly designed and implemented, and should also have guidelines that ensure the enforcement and management of security programs and practices.

Policies are sometimes the causes of information security failure because errors in them causes vulnerabilities in security measures (Sindhuja & Kunnathur, 2015). According to Yang & Wei (2013), well-structured security policies and regulations are critical to the successful management of security threats in supply chains. They are also important because they ensure that all actions and processes pertaining to products or services' development, and also, all activities involving information and information systems have authorised access and are performed by the right individuals (Windelberg, 2016). Hence, part of the objective of supply chain management practices should be to ensure that the supply chain is free of security policy violations. It should also include ensuring that the internal and external environment in which the supply chain operates, conforms to government regulations and policies (Li *et al.*, 2009).

Information security is a statement of the responsibilities and roles of the employees in safeguarding the information and information system resources of the organisation (Bulgurcu *et al.*, 2010). It is also the set of rules which are used to protect information assets from both external and internal threats (Sung *et al.*, 2014). It often consists of rules that ensure the protection of information and information systems within organisations. It also usually comprises of the set of values and instructions that users must adhere to, hence, they are used to control and guide the behaviour of users in the protection of the confidentiality and integrity of information, and in ensuring the availability of information systems and their components. Sindhuja & Kunnathur (2015) presented a study which revealed that so many organisations have information security policies in place, however, the dissemination, uptake and compliance of these policies are not often given so much priority.

Compliance with information security policies and regulations ensures information security and the effective use and management of information systems. However, compliance is still an issue to security policies and regulations. This for example, is because most organisations normally amend and ensure compliance with their control measures such as policies and regulations in a reactive manner, that is, after the network or information security breach has occurred, when in actual sense, the policies and regulations should be developed and implemented, and their compliance be enforced proactively, so as to take care of the possible network or information security breaches that could occur (Olivier *et al.*, 2006). In the study of Kolkowska & Dhillon (2013), it was explained that the use of an integrated system in facilitating the exchange of information can help ensure compliance with security policies and regulations.

As explained in the work of Kolkowska & Dhillon (2013), the resistance to security regulations and the inability of policies to illustrate current security practices are some of the reasons for the failure of security regulations and policies. According to Olivier *et al.* (2006), another cause of information security policy failure is that most organisations do not define extensively, their information security procedures, and in organisations where these procedures are well defined, compliance with the procedures is sometimes an issue. According to Kolkowska & Dhillon (2013), coercion, rewards and sanctions are important measures to consider in order to ensure that trading partners comply with information security policies. The cultivation of security culture and the correspondence of information among trading partners can also ensure compliance with information security policies and the protection of supply chain resources (Zailani *et al.*, 2015).

4.5.2.2 Standards & Frameworks

In order to ensure compliance with the security policies and regulations used among all the organisations in a supply chain network, there is a need for the standardisation of such security policies and regulations (Sindhuja & Kunnathur, 2015). Similarly, according to Windelberg (2016), in order to ensure the security of supply chains' information and information systems, there is a need for compliance with organisational and security standards. Standards guide organisations in the development and enforcement of information security practices (Blos *et al.*, 2016). They help organisations in the reduction of information loss, information distortion or possible risks that can disrupt supply chains. Furthermore, they help organisations in developing general policies and procedures. Hence, conformance to good practices and standards, and exercising due diligence and due care are important in ensuring that security measures and practices are effective.

Information security within supply chain requires the establishment or adoption of security standards, frameworks or practices, that can be used in preventing information and information system attacks (Wolden *et al.*, 2015). Although, as identified by Angeles (2009), the lack of a standard framework for supply chain information structure is still an issue of concern to supply chains. There should be an agreement among supply chain partners on information security and technology standards. This is because the level at which information system and technology risks are minimised increases when standards are established or adopted. Also, as these standards (established or adopted) become more stable and mature, the information shared within the supply chain, becomes more regular and adequate (Xue *et al.*, 2013).

Standards and practices are influencing today's global supply chain. Hence, any type of standard used within supply chains should not create barriers to collaboration and co-evolution (Eamonn & Kelly, 2015). Information security management standards are used to describe the various architecture and documents, from different sources, that provides recommendations on issues relating to information and information system security, especially in the areas of planning, auditing and managing the overall information security practices applicable to an organisation (Sindhuja & Kunnathur, 2015). According to Olivier *et al.* (2006), Xiao-yan *et al.* (2011) and Ahlmeyer & Chircu (2016), information security management standards and frameworks include (but not limited to) the Control Objectives for Information and Related Technologies (COBIT), International Organisation for Standardisation (ISO) and International Electrotechnical Commission (IEC). These are explained below.

> *COBIT*: "is a risk management based framework that is classified as an IT governance framework", which organisations use to maximise security controls (Wolden *et al.*, 2015, p.1848). One of the benefits of adopting COBIT as an organisational standard is that it ties back to the broader organisational objectives. Another benefit of adopting it as a standard by organisations and within supply chains is that it is not limited or confined either to technology or any single unit within the organisation or supply chain (Stroud, 2014), but covers the overall organisational or supply chain's activities.
>
> COBIT has gone through different modifications, and it now incorporates not only IT governance elements, but also, controls and management activities. At the moment, it is in its 5th iteration, hence it is now referred to as COBIT 5 (Ahlmeyer & Chircu, 2016). COBIT 5 ensures that there are enforcement and management of security within the organisation. To do so, it adds a new dimension to information security, via set rules and policies that further strengthens the application of enterprise security (Wolden *et al.*, 2015), and that also ensures that security is adequately managed between organisations and their consumers.
>
> *ISO/IEC*: Across the globe, the ISO is the most widely known and recognised standard-setting body (Koppell, 2011). Similarly, the IEC is also a recognised body that publishes international standards for all electronic, electrical and related technologies (often referred to as electrotechnology). These standards are adopted by a wide variety of organisations and are often incorporated into international agreements and domestic laws (Koppell, 2011). They have also been widely adopted for supply chains, as shown in the study of Stroud (2014), Blos

et al. (2016), de Oliveira, Marins, Rocha, & Salomon (2017). Some of the ISO/IEC standards that are applicable and have been adopted for supply chains are:

ISO 31000 (Risk Management): is a standard that provides the general guidelines and principles on risks management (Blos *et al.*, 2016). It serves as a foundation for supply chain managers to understand and ensure enterprise risk and supply chain risk management.

ISO/IEC 27002 (Information Technology Security techniques): is formerly known as ISO 17799. It is a standard that can be used for establishing an information security program or improve the existing information security practices. It is aimed mainly at the senior management of organisations, as it helps them take essential actions and make necessary decisions (Xiao-yan *et al.*, 2011) regarding the security of information and information systems.

ISO/IEC 27036-3 (Information Security for Supplier Relationship): is a standard that "specifies the fundamental information security requirements pertaining to the supplier-buyer business relationships" (Blos *et al.*, 2016, p.1568). This is important to supply chains as most supply chain organisations depend on the existing or formed relationship within the supply chain.

ISO 27001:2005 (Information Security Management Practices): deals with security practices that covers areas such as physical and environment security, personnel security, organisational security, security policy, assess control and compliance (Sindhuja & Kunnathur, 2015). It is an important standard to supply chains because it ensures the establishment and compliance of the trading partners to security practices and measures.

ISO 28000 (Specification for Security Management Systems for the Supply Chain): is an available "specification on security management system requirement that deals with security assurance in the supply chain" (Blos *et al.*, 2016, p.1568). It allows a supplier to ensure and enforce the necessary processes required for the reduction of risks and promotion of resilience. It also assists in the management of risks in supply chain relationships (Stroud, 2014).

IEC 61508: is an international standard designed for creating the partitioning, diversification or independence of information systems and their components, such that containment and redundancy can be guaranteed when security breaches, faults or failure occurs (Windelberg, 2016). It is a standard that can also help in ensuring the security of supply chains' information and information systems.

4.5.2.3 Training & Awareness Programs

In the study of Bulgurcu *et al.* (2010), it is suggested that organisations can use three security countermeasures to address security threats. The measures are the security education, training and awareness (SETA) of users; the implementation of security policies; and the monitoring of information systems. The security education, training and awareness of users are important because they make it possible for users to maintain the current knowledge of security threats and the best means of managing them (Choo, 2011). Educational programs provide the knowledge required in taking positive action against security threats or attacks, while awareness campaigns keep users continuously thinking about security threats. Through training and awareness programs, and with the help of other culture building activities, organisations can easily integrate technical security control measures (e.g. firewalls and anti-virus) with non-technical control measures (e.g. policies and standards) (Sindhuja & Kunnathur, 2015)

Users exposed to security training often show greater enthusiasm and performance with regards to information security. A study conducted by Bulgurcu *et al.* (2010), to understand the impact of information security training on employees' attitude to comply with information security policies shows that employees with security training have significantly positive beliefs, performance and attitude towards security measures. In the study of Wolden *et al.* (2015), it was also shown that the level of security training and awareness of the supply chain members influences the way they behave and react to security programs, frameworks and procedures. Hence, the security training done by organisations or within supply chains should involve all the organisations' employees or the supply chain members, and should also be on a continuous basis. In agreement, CESG (2010) also explained that training and awareness programs should be designed for all employees, especially the employees with information security responsibilities.

The level of knowledge, training or education of users influences the users' compliance behaviour with information security practices and programs. That is, users with a higher level of training or education will be more exposed and conversant with information security practices, programs and policies. Likewise, users with inadequate experience, training or education in security can also be a source of vulnerability and weakness to information systems and consequently to the information acquired, processed, shared and stored by the systems. Hence, according to Bunker (2012), one of the ways of solving information and information systems' security vulnerability and threat issues is by changing the perception and attitude of employees through training or education. This is so because, "ignorant users can get themselves into troubles even with the best and most sophisticated defences available" (Issac *et al.*, 2014, p.1).

The awareness of supply chain members to information security is important in the interpretation and use of supply chain information security policies and regulations (Wolden *et al.*, 2015). Similarly, information security awareness of employees is important in the successful utilisation of information security measures. This also means that the higher the awareness, the more likely it is to reduce the risks of information system failure and to also reduce the possibility of attacks on the supply chain and its information (Windelberg, 2016). Awareness of how vulnerabilities are created and how they can be exploited is also important in defining security requirements. According to Martin & Rice (2011) and (Sindhuja, 2014), to create or increase security awareness, organisations must develop a knowledge base for information security challenges, practices and issues, which should be shared with employees. They can also do so through the development and use of seminars, flyers, talks etc. from within and across organisations.

4.5.2.4 Audit

One of the non-technical security measures that can be used to ensure the security of information within any organisation or supply chain network, is the continuous monitoring and auditing of the activities surrounding information and the information systems used within the organisation or the organisation's supply chain network. According to Perez-Castillo & Piattini (2013), audit is necessary for all organisational sector, irrespective of their size, capacity or net-worth. This is because, it involves prioritising the impact of loss, appraising value and evaluating the organisational assets' (e.g. informational, information system infrastructure, intellectual property etc.) vulnerabilities and exposure to threats (Borum *et al.*, 2015). It also involves the use of a comprehensive framework and pathway to assist organisations in achieving their objective of IT governance and management (Perez-Castillo & Piattini, 2013).

Auditing, sometimes referred to as assessment, helps ensure that the adequate and right security measures are adopted, implemented and effectively utilised in a manner that can help prevent or minimise distortions and disruptions to information and information systems (Wolden *et al.*, 2015). It also helps understand how shifts in threat environments can impact on organisational information security and management behaviour. For these reasons (and much more), conducting an audit of each of the processes at each stage of a supply chain structure is important, especially, in order to provide some level of assurance for the supply chain members (Axelrod, 2011). It is also important because it enables the supply chain members to determine whether the security measures put in place are adequate or being effectively used for the protection of the information and information systems used within the supply chain (Wolden *et al.*, 2015).

Conducting an audit is mostly considered a preventive measure, but it is also a practice that can be performed after something has happened (Wolden *et al.*, 2015). According to Axelrod (2011), a more thorough audit can still be initiated after threats or rogue components are discovered in an attack or security breach. An example of this practice (i.e. auditing after an attack or security breach has happened) can be found in the use of audit log to facilitate a post-analysis or on-going analysis of complaints, compliance issues or security breach or attack. The importance of auditing practices (pre- or post- security breach) has made most regulatory organisations enforce auditing standards for compliance purposes. These organisations are also suggesting the engagement of the services of auditing firms to determine the effective use of controls in ensuring that standards and policies are being adhered to within organisations (Dowling, 2014).

Providing real-time audit of information and information systems for compliance, for all the parties involved in the sharing of information, information security policies and regulations is important in ensuring the security of information (Morris *et al.*, 2010). Hence, the auditing of information and information system should be an on-going practice and not just a snapshot. According to Morris *et al.* (2010) however, the cost involved in performing most types of audit is a challenge to most organisations, hence most audits are not always performed on an ongoing basis or in real-time. Another challenge to auditing, especially financial and information auditing, is the amount of experience, skills and in-depth knowledge (which unfortunately is not always readily available) required in performing such type of audit (Perez-Castillo & Piattini, 2013).

4.6 Information Assurance within Supply Chains

Information is important and valuable to organisations, however, most organisations do not give it the same protection, or request for similar assurance, as they do with their organisational finances. In the study of Roy & Kundu (2012), it is stated that efforts are being put in place by organisations, to define techniques that can be used to control information security-related risks in supply chains. However, not much has been done to give assurance that these techniques will be effective in the management of information security related threats and risks across supply chains. This could be because there is an assumption by most organisations that when security is addressed, assurance is also covered, when in reality, security protocols may be implemented but not working properly (Ouedraogo *et al.*, 2012). According to Axelrod (2011), it could also be because of the insufficient availability of expertise and information needed in making decisions regarding assurance, especially information assurance.

The need for information assurance is, and will continue to be important to organisations. This is because information assurance is a dynamic domain that is continuously changing in response to the continuous evolution of technology, business needs and the society. Information assurance has been described by Bunker (2012, p.21) as the "ability of an organisation to manage the risk to the governance, compliance, confidentiality, integrity and availability of its information at all times." It has also been described by Cherdantseva & Hilton (2014) as a professional activity and a multidisciplinary area of study that aims at protecting organisations, by reducing the different types of risks associated with information and information system, through the provision of comprehensive security countermeasures that are systematically managed and driven by cost-effectiveness and risk analysis. As explained in the study of Hamill *et al.*, (2005), information assurance objectives are, but not limited to:

- the protection of information and information systems and their environment
- the detection of potential attacks to information and information systems
- the response (reaction) to any possible type of attack on information and information system
- the restoration of information and information systems' after any form of attack

Information assurance is increasingly attracting the interest of information security professionals and researchers. This is because of the increase in the lack of compliance with information security policies and regulations among today's global trading partners. It is also because information assurance is perceived as a practice that can help in protecting information and information systems by ensuring their confidentiality, integrity, availability, authentication and non-repudiation (Hamill *et al.*, 2005). It also helps in protecting information and information systems by incorporating detection and reaction capabilities that ensures and facilitates information systems' restoration (CESG, 2010). As explained in the study of Jouini *et al.* (2014), the detection and reaction capabilities also ensures and facilitates the provision of a response mechanism that is properly focused, and a restore capability that re-establishes the confidentiality, integrity and availability of information and information system to their original state or even to an improved state.

According to Denolf *et al.* (2015), every supply chain trading partner wants some level of assurance that the information that will be shared using the supply chain information system will not be exploited, and will be kept confidential. To provide such assurance, the audit of each of the activities and information at each stage of the supply chain should be frequently performed. Monitoring of critical processes and the validation that standards are followed should also be performed frequently throughout the supply chain (Axelrod, 2011). Also, to provide such assurance, Wolden *et al.* (2015) suggested that contemporary methods that are technically enhanced should be used. According to Hamill *et al.* (2005), these methods should involve the use of processes and techniques such as access controls, intrusion detection software, multi-level security and secure network server. Furthermore, according to Windelberg (2016), these methods should also involve verification testing and independent validation.

However, according to Cherdantseva & Hilton (2013), information assurance is not limited to only the implementation or application of technical security countermeasures or the protection of electronic information. It also encourages and advances a holistic approach to the security of all kinds of information (electronic or not) and information systems, by exploiting and combining different types of available countermeasures (technical, legal, human-oriented and organisational e.g. policies) for the adequate protection of information and information systems. Hence, according to Ifinedo (2014), to gain assurance on the ability of deployed security measures, that they will adequately protect information system assets, activities such as monitoring, continuous assessment etc. must also be carried out on the deployed security mechanisms or measures. As explained in the study of Maconachy, Schou, Ragsdale, & Welch (2001), information assurance and security issues can be addressed using two approaches, and the approaches are:

The threat-based approach: This approach focuses on analysing threats to information in technical details.

The goal-based approach: This approach focuses on communicating with stakeholders by security experts, in a manner that does not require technical knowledge.

Communication is vital to the provision and implementation of information assurance, hence, communication plans has to be developed in order to achieve information assurance objectives (CESG, 2010). Authors and organisations are also emphasising on how vital policies and controls are, in providing assurance on organisational information and information systems. According to Morris *et al.* (2010), organisations will be more willing to share information if they have the assurance that the agreed upon policies, controls or rules for sharing and using information are being enforced. This is so because the level of controls and the type of policies in place within an organisation helps the organisation with the timely detection and prevention of attacks on the organisation's information and information systems. According to CESG (2010) however, information assurance controls and policies cannot be enforced when there is poor cultural attitude by the employees, to security.

Bunker (2012) classified controls in information assurance into three groups. He further stated that these controls are interrelated as their objectives are to secure information. The controls are:

Strategic Controls: These are controls that are put in place to ensure that information assurance strategies align with organisational needs. They involve activities around compliance, risk, governance and business alignment.

Operational Controls: These are controls that cover the day-to-day activities of the business. They include incident handling and response, backup, physical security, configuration and patch management, continuity and disaster recovery.

Tactical Controls: These controls depend on technology and the people and processes that surround the use of technology. They are used to ensure the protection of users and information from security vulnerabilities, threats and risks. They involve activities around the installation of anti-virus and intrusion prevention applications, secure information exchange and remote security controls.

The strategic benefits that information assurance can enable include the reduction of information risk, the reduction in the total cost of implementing reactive measures for information security breaches or attacks, and the establishment of an effective business process (CESG, 2010). To achieve these benefits, Roy *et al.* (2012) suggested that a process framework that facilitates a consistent business practice and assures information security management across the supply chain should be developed. Morris *et al.* (2010) also suggested that a Continuous Compliance Assurance (CCA) mechanism that is embedded in a trusted enclave, be adopted by organisations. According to them, these mechanism fosters trusted information sharing among organisations, by assuring the compliance with the policies and regulations regarding the information to be shared.

One of the most common challenges in establishing information assurance practices is the inadequate availability of resources, particularly money. This is so, especially when financial benefits are not obvious or readily available (Hamill *et al.*, 2005). Another challenge being faced by organisations with regards to information assurance is the insufficient support obtained from top management and stakeholders. According to Bunker (2012, p. 20), information assurance "needs to start from the top". Hence, according to CESG (2010), it is important to drive information assurance through an organisational level programme and process rather than driving it through programmes and processes that are only at the system level. This is because the board and stakeholders tend to pay more attention to the design, deployment and operation of controls, programmes and processes that affect the overall activities of the business.

4.7 Conclusion

Information and information systems are important supply chain assets that need to be protected so as to maintain their availability, confidentiality and integrity. Hence, the design of most modern supply chains is extending to include security dimensions that can help to mitigate potential malicious actions and to reduce the exploits of vulnerabilities on supply chains' information and information systems. These security dimensions are not based on technical measures (e.g. anti-virus and firewall) only, but also includes non-technical measures (e.g. policies and standards). This is because, technical measures alone are insufficient in the protection of information and information systems (Montesdioca & Maçada, 2015). Most supply chains consist of multiple organisations. Hence, any distortion to information severely affects the operations of the multiple organisations within the supply chain. Organisations are therefore increasingly seeking assurance that the information being used within the supply chain is adequately protected. As a result of this, information assurance has become an important requirement among today's trading partners.

CHAPTER 5: RESEARCH METHODOLOGY

5.1 Introduction

Methodology in research is a way of conceptualising and thinking about data. It is the principles and assumptions that underpin a research study and the approach used in the study. It guides a researcher's decision on what methods and processes to use in a study, and how the research questions to be used in the study should be framed (Giddings & Grant, 2006). Giving the details of the methodology used in achieving the objective of a research is important because it makes the data collection and analysis process transparent (Bowen, 2005). The details of a study's methodology that should be provided should include the study's research design and approach, the data collection method and instrument, the population and sample of interest, the recruitment and selection of the study's participants and the data analysis technique employed in the study. In this chapter, as seen in Figure 5.1, all these are presented and described, in relation to this study.

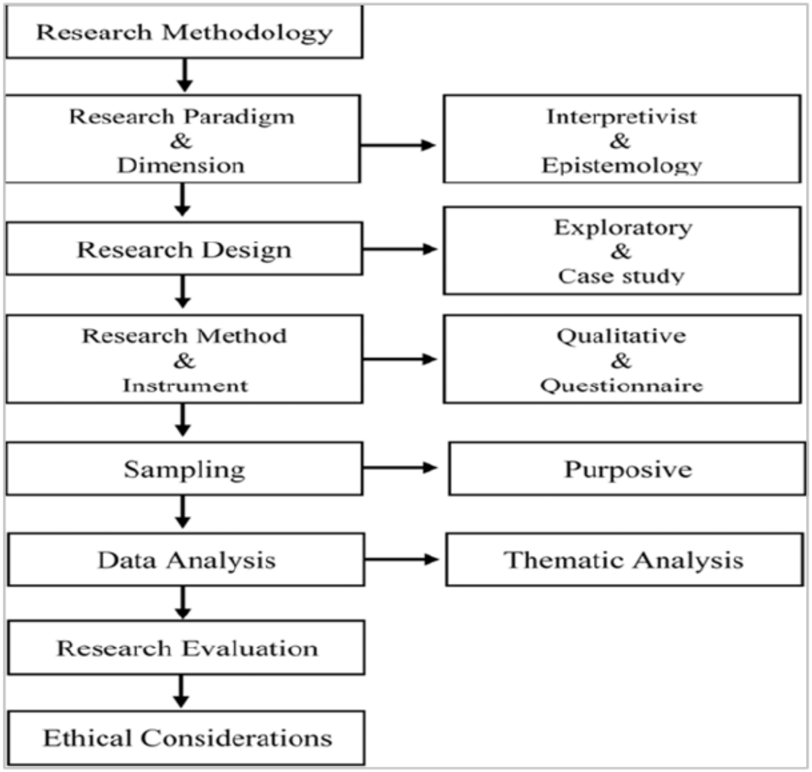


Figure 5.1: The Complete Layout of the Chapter

5.2 Research Paradigm & Dimensions

Paradigm may be described as the set of beliefs or assumptions held by people, which illustrates their understanding of the world (Humphrey, 2013). It may also be described as an integrated concept, structure and pattern with scientific and academic ideas, which includes the methodological approaches and tools used for solving a research problem (Thomas, 2010). According to Trifonas (2009), paradigms and their respective philosophical assumptions and dimensions are important to researchers because they help with the proliferation of existing and emerging patterns of knowledge. They also help with the proliferation of the different disciplinary agendas that serve to convene a particular research practice, custom or skill in the scientific and social world. In this section, the common research paradigms and dimensions, as identified in the literature, are discussed. The paradigm adopted in this study is also presented in this section.

5.2.1 Research Paradigm

Research paradigm may be described as a framework or a research culture with a set of ideas, values and philosophical assumptions that are shared by the members of a certain research group or community, regarding the nature and conduct of research (Kuhn, cited in Thomas, 2010). Its philosophical assumptions and inherent ideas, when adopted in a research provide the researcher with a convenient structure, methodology, model or framework for examining problems and finding solutions to the problems. According to Burnett (2012), adopting the appropriate paradigm helps position a research on its course, by guiding the researcher in decisions concerning methodology, research approach and data analysis. It is therefore important for researchers when conducting a research, to identify and understand the ideas and assumptions that best suits their study, so as to be able to adopt the most appropriate paradigm for their study. The next section presents some of the common paradigms found in the literature.

5.2.1.1 Positivist/Scientific Paradigm

The positivist research is a research that seeks to know (Burnett, 2012). According to Humphrey (2013), it is a research process that ensures the securing of objective knowledge. It was stated in the study of Giddings & Grant (2006) that the positivist paradigm is considered and often viewed as synonymous with quantitative research. This is because, within this research paradigm, only quantifiable data are considered as evidence. This also mean that researchers conducting a positivist research are expected to gather data on large representative samples so as to uncover statistically significant correlations. However, one of the major challenges with this approach is the understanding and utilising of statistical data, especially in the social world. There is a shift from within the positivist, to the post-positivism. According to Ryan (2006), in a post-positivist research, significantly large amount of qualitative data can also be generated. This is because texts or peoples' words are also considered as evidence in the post-positivist research approach. However, the difference between this approach and the interpretivist approach (which also generates qualitative data) is that, with this approach, "the same questions must be presented in the same order to all respondents, often with fixed categories to answers" (Humphrey, 2013, p.8). This is so as to ensure and safeguard objectivity.

5.2.1.2 Interpretivist/Constructivist Paradigm

According to Burnett (2012), an interpretivist research is a research that seeks to understand. It is a research paradigm that is popularly used when undertaking studies with the core objective of understanding social phenomena. This means that, with this paradigm, researchers tend to "derive their constructs from the field by an in-depth examination of the phenomenon of interest" (Thomas, 2010, p.295). Interpretivist believe that an account grounded in multiplicity of views and voices will generate a more holistic truth about any social reality. It was stated in the study of Giddings & Grant (2006) that the interpretivist paradigm is considered and often viewed as synonymous with qualitative research. This is because, it allows researchers to draw upon their own intuition, experience and imagination in order to develop and form an understanding of the story being told by others. It is also because it allows for the generation of themes, concepts or topics that help researchers achieve their research objectives. One of the major challenges of this paradigm, however, is that there can be unusual or exaggerated responses or reactions from the participants of a study being conducted using this approach. These unusual or exaggerated responses or reactions, if not properly managed, may distract the study being conducted from achieving scientific credibility (Humphrey, 2013), and subsequently, their main objectives.

5.2.1.3 Critical/Radical Paradigm

A critical research is a research that seeks to change or confront the injustices existing in the society (Burnett, 2012). It seeks to understand the relationship between societal structures (e.g. political, economic and cultural) and the ideological way of thinking that constrains human imagination of changing or confronting unjust social systems. It recognises the existence of multiple truth and also seeks to investigate the differential power relationships that exists between truth and the structures and social actors that lay claim to them (i.e. truth). Hence, it is considered an approach that can be adopted when interrogating the uneven distribution of privilege and advocating for equity and greater access. According to Clark (2014), critical researchers, just like interpretivist researchers, often rely on qualitative means of acquiring information, except that, they often require a greater level of autonomy from the individuals or people participating in the study or being studied. Some authors, however, explained that critical researcher, in some situations, also adopt the quantitative method. This means that they (critical researchers) can sometimes adopt the mixed method approach, in order to acquire information. One of the challenges of this approach is that there is a possibility of the researcher unknowingly listening to the experiences of those that are least affected by the social issues of injustice.

5.2.2 Research Paradigm Dimensions/Characteristics

According to Guba (1990), the research paradigm (discussed above) a researcher adopts can be characterised through their *ontology*, *epistemology* and *methodology*. In the study of Thomas (2010), these characteristics were referred to as dimensions. In most of the studies that dealt with research paradigm, these same dimensions/characteristics were identified. However, in some other studies such as that of Giddings & Grant (2006) and Humphrey (2013), a fourth characteristic called *axiology* was identified. These characteristics (i.e. the four characteristics) were explained to reflect a researcher's belief of the way of seeing the world with regards to reality and knowledge. The next section discusses the ontological, epistemological, methodological and axiological stance and position in research. It also presents the researcher's position, which subsequently influenced the research paradigm adopted in this study.

5.2.2.1 Ontology

Ontology deals with a researcher's belief of what is reality, what exist in the world and what the structure and nature of reality is (Giddings & Grant, 2006; Lehner & Kansikas, 2013). It is also perceived as the realm of being. According to Humphrey (2013), at the ontology level, positivists assume that things exist independently of the perceiver and that they are as they appear to be. They also believe that there is a single reality or truth which can be best determined through observation and measurement. Hence, they are considered to have an objective viewpoint that knowledge is quantifiable. According to Patel (2015), the interpretivist, on the other hand, assumes that there is no single reality or truth. They believe that reality is often created by people, either as an individual or as a group, and they also believe that reality can be determined from the actors' perspective, through interactions with the actor or the actors' environment. Furthermore, they believe that reality has to be observed and interpreted, hence they are often considered to have a subjective ontology. Also having a subjective ontology, are the critical researchers who believe that realities or truth are constructed entities that are often under constant influence, and that can only be determined through interacting (directly or indirectly) with reality. Both the interpretivists and critical researchers try to understand why and how things happen.

5.2.2.2 Epistemology

Epistemology deals with how we come to know about reality. It deals with a researcher's belief about what counts as knowledge, the nature of human understanding and the knowledge that can be obtained through human understanding and experiences (Giddings & Grant, 2006; Lehner & Kansikas, 2013). At the epistemology level, the interpretivist believe that reality can be derived through peoples' subjective experiences (Thomas, 2010). According to Humphrey (2013), they also assume that the knowledge of a phenomenon can best be acquired by directly interacting with, or experiencing the phenomenon. Hence, they typically adopt a qualitative methodology in their quest for knowledge and are also considered to have subjective interaction with the phenomenon being studied. Furthermore, at the epistemology level, the positivist assumes that knowledge can be rendered transparent to all and can also be expressed in the universal language of statistics. Hence, they typically adopt a quantitative methodology in their quest for knowledge and are also considered to have an objective interaction with the phenomenon being studied. For the critical researchers, they adopt a similar approach as the interpretivist, hence they are also considered to have a subjective interaction with their subjects.

5.2.2.3 Methodology

Methodology deals with a researcher's belief of how knowledge can be gained (Giddings & Grant, 2006). It helps establish the process of finding out about knowledge or a phenomenon. It includes the strategies, plan and designs linking the choice of methods (i.e. the data collection and analysis techniques or procedures adopted in a study) to the required outcomes. According to Patel (2015), the positivist often use an experimental or survey research methodology. Hence they employ a quantitative method of data collection and analysis, which includes the use of questionnaire, sampling measurement, statistical analysis or scaling. The interpretivist, on the other hand, use meaning as against measurement methodology (Thomas, 2010). They often use grounded theory, discourse analysis, action research, heuristic inquiry or phenomenological research methodology. Hence they employ a qualitative method of data collection and analysis, which includes the use of interview, observation or narratives. Critical researchers, similar to the interpretivist, use discourse analysis, action research, ethnography or ideology critique methodology. They are known to, therefore, employ interviews, ideological review or focus groups for acquiring knowledge. However, in some cases, they employ questionnaire in order to acquire information. Hence, they in some instances adopt a positivist research approach.

5.2.2.4 Axiology

Axiology deals with a researcher's belief that is concerned with the acquisition of knowledge (Freedman, 1999). The axiological positioning of a researcher is an important factor in the choice of the methodology to be used to acquire knowledge in a study. According to Giddings & Grant (2006), it is also an important determinant in a research decision-making process. Giddings and Grant further explained that, for instance, a study being conducted to understand social injustice or a person with a strong belief, values or affinity towards issues of equity and social justice, will likely be drawn to the radical/critical paradigm, and hence, will adopt a radical/critical approach and methodology in the acquisition of knowledge. This is because this paradigm (i.e. the radical/critical) focuses on social change and social action. Similarly, a study being conducted to simply know about a phenomenon will be drawn towards adopting the positivist paradigm and hence will adopt a positivist approach and methodology in the acquisition of knowledge. While a study that seeks to understand the how and what of a phenomenon will be drawn to the interpretivist paradigm, and hence will adopt an interpretivist approach and methodology in the acquisition of knowledge

5.2.3 The Research Paradigm and Dimension of this Study

It is important for researchers to base their study on certain philosophical assumptions and perspectives (Thomas, 2010). Hence, it is important for a researcher to decide on the research paradigm to be adopted in their study, and work within the framework of the paradigm. In this study, the philosophical assumptions and perspectives that was adopted are that of the interpretivist paradigm. This is because the study seeks to understand 'why' and 'how' things happen. The paradigm was also adopted because it facilitates and accommodates researchers' reflexivity, which was useful in preventing bias in the study. The adoption of this paradigm, its philosophical assumptions and methodology also served as a guide to the researcher in obtaining explanations and experiences, with detailed examples, from the study's participants. Since this study was about acquiring knowledge (axiology) through human understanding and experiences, and also about understanding the how and why of the phenomenon being studied, the epistemology dimension/characteristic was also adopted in the study.

5.3 Research Design

Research design can be described as the master plan or logic of a research study, which shed light and also guide researchers on how their study is to be conducted (Thomas, 2010). It may also be described as the overall strategy adopted by a researcher, to integrate the different major components of research (e.g. samples, research methods etc.) in a logical and coherent manner that ensures that the set-out research objectives are achieved, and the set-out research problems and questions are also effectively addressed. With the research design in mind, researchers are able to make rational choices and decisions, and also address issues relating to the purpose of their study, the settings (e.g. location, investigation type etc.) of their study and method of data collection and analysis (Sekaran, 2006). In the review of literature done by the researcher, it was discovered that research design was sometimes referred to as research approach or research strategy. Some of the common research design/approach identified in the literature, to be particularly suitable for studies adopting the interpretivist paradigm, are described below:

Exploratory Design: This design approach is suited for studies in which not much is known about the phenomenon being studied, or when no information is available on how similar research issues or problems to the one being studied, have been solved in the past. It requires that an extensive preliminary work is done, so as to understand the phenomenon being studied or to gain more familiarity with the phenomenon, within the context in which it is being studied. According to Sekaran (2006), it is a design approach that might also be useful in a situation where some facts are known, but more information is still required in the development of a viable conceptual or theoretical framework.

Explanatory Design: This is a design approach that is adopted when a study is looking to explain a phenomenon, or when a study is trying to answer questions that sought to explain a presumed relationship in a social or real-life context (Baxter & Jack, 2008). It is also suitable for studies investigating causes and outcomes.

Descriptive Design: This design approach is undertaken when a research aims to ascertain and also describe the characteristics of a phenomenon. It is also useful when a researcher wants to acquire information about the status of a phenomenon, so as to be able to describe what exists (and the issues) about the phenomenon. Its goal, according to Sekaran (2006), is to aid the researcher in profiling or describing the relevant aspects of the phenomenon being studied, from an organisational, individual or other perspectives.

Grounded Theory Approach: This is an approach that focuses on the systematic gathering, coding and analysis of data, so as to derive a theory or theories. Hence, in its approach to studying or understanding a phenomenon, it is designed towards the building of theory directly from gathered data. It is often applied when the phenomenon being studied is in a relatively early stage of development or when trying to address a complex issue that has significant variation (Speier *et al.*, 2011).

Phenomenological Approach: In this approach, the researcher is often interested in the lived experiences of the individuals participating in the research study. This approach helps to explore some of the philosophical underpinnings of a phenomenon (Lichtman, 2013).

Case Study Approach: This approach is useful when investigating or trying to understand a phenomenon within its social or real-life context, especially when the boundaries of the phenomenon and the context in which it is being studied are not clearly defined (Yin, 2003). It involves an in-depth study that explores a phenomenon with a view of advancing the understanding of the phenomenon (Thomas, 2010). With this approach, a researcher's interest could either be to simply understand the case in hand (*intrinsic case study*), or to explore a case, so as to shed light on the issues concerning the case (*instrumental case study)* (Cousin, 2005). As explained in the study of Baxter & Jack (2008), a case study approach can also take an exploratory, explanatory or descriptive form.

Hypothesis Testing: This approach is often adopted when the study being conducted is aiming at discovering and establishing a relationship between variables, or two or more factors in a situation (Sekaran, 2006). Hence, it is an approach that is relevant to researchers looking to explain the variance in variables, or trying to predict what may occur.

In order to understand the phenomenon being studied (in this study) with greater depth, and from the social and real-life perspective and experience of the study's participants, the case study approach was adopted in this study. Both the intrinsic and instrumental procedure of the case study approach was adopted in this study. Also, because not so much is known about information assurance within the supply chain context, an exploratory design was also adopted in this study. This, therefore, means that the exploratory design and the case study approach were considered befitting for achieving the objectives of this study.

5.4 Research Methods

In the study of Thomas (2010), Myers was cited to have described research method as a strategy of enquiry, which progresses from the underlying assumptions adopted in a study, to the research design and data collection and analysis methods adopted in the same study. The most popular classification of research methods has been into quantitative, qualitative and mixed methods. The distinction between these methods is in the form of data collection and analysis, and also in the manner in which data are collected and analysed. These methods are also used to create distinction in the nature of knowledge to be acquired. Neither of these methods is better than the other (Thomas, 2010). In fact, according to Guba & Lincoln (1994), these methods can be adopted in any research paradigm, if used appropriately. The suitability of any of them to a research study should be decided, based on the context, objective and nature of the study.

The quantitative research method is generally associated with numbers and statistics. It is often considered a deductive approach that generates numbers that in most cases need to be analysed, summarised and described. According to Lacey & Luff (2009), quantitative data may be explored by calculating mean and standard deviation and by doing cross tabulations. After analysis, it may also be described through the use of tables, charts and graphs. Patterns and relationships can also be explored and determined in quantitative data by performing an analysis of variance or multiple regression. In a quantitative study, research questions can be addressed using quantitative techniques such as questionnaires, measurement of standard outcomes (e.g. morbidity, staff absence rate or mortality), attitude scaling etc. They can also be answered using qualitative techniques such as interviews, focus groups etc. (Lacey & Luff, 2009). According to Trifonas (2009), quantitative research which enforces the suppression of researchers intervention in the process of data collection may also still have some form of bias through the measurement instrument and the population being surveyed.

Qualitative research method, on the other hand, is generally associated with words and narratives. It is mostly considered an inductive approach that is well suited for answering the ‘what’, ‘why’ or ‘how’ questions (Ritchie, Lewis, Nicholls, & Ormston, 2003). According to Lacey & Luff (2009), it has been described as a subjective and interpretative exercise in which the researcher is fully and intimately involved. Its purpose is to examine a phenomenon in a natural setting, by acquiring the ideas and perception of the participants of a study (Lichtman, 2013). With this type of research method, there is the likelihood that the views, assumptions and preconceptions of the researcher influences data collection and the data collection process, and consequently, the emerging concepts or theory. Hence, Lacey & Luff (2009) suggested that the researcher be more visible or reflexive in this research approach, so as to prevent any bias. Qualitative methods use narratives or storytelling to make sense out of data. Hence, the researcher using a qualitative research method is often required to draw upon their own intuition, experience and imagination to develop an understanding that can help in generating themes, concepts or topics that are useful in achieving the study’s objectives. With the mixed method, however, both the quantitative and qualitative methods are adopted (Ritchie *et al.*, 2003).

As stated in section 5.2.3, the interpretivist paradigm was adopted in this study. This paradigm has been explained (in section 5.2.2.2) to be considered and often viewed as synonymous with qualitative research. The epistemology dimension that deals with understanding a phenomenon through peoples’ experiences and perspective (i.e. interpretivist epistemology) was also adopted in this study. Therefore, in this study, the research method adopted is the qualitative research method. This method was employed in this study because the researcher needed to have a contextual information, with rich insight and meaning into the study’s participants activities and experiences, while at the same time, uncovering their personal views and perspectives (Guba & Lincoln, 1994). Since this study adopted a qualitative research method, a data collection instrument that can aid in the collection of qualitative data was also adopted in the study. The research instrument adopted in this study is discussed in the next section.

5.4.1 Research Instrument

In a qualitative study, the data collection instrument is usually the researcher herself/himself (Brink, 1993; Merriam, 1995). Although, the instrument or method that a qualitative researcher often use include interviews, focus groups, making observations and handwritten field notes. It may also include video recordings, visual images or other types of media (Lacey & Luff, 2009). In this study, the data collection instrument was open-ended, in-depth interviews. Interview was selected because it allows direct contact with the study’s participant, which subsequently led to focused, rich, constructive and detailed suggestions and responses (data) being gathered from the study’s participants. Interviews can be *structured*, *unstructured* and *semi-structured* (Thomas, 2010). In a structured interview, the interviewer uses a set predetermined questions to extract information. These questions are usually short and clearly worded, and they often require precise responses in the form of a set of given options that are read out or presented on paper to the interviewee. In an unstructured interview, the interviewer poses open-ended questions that allow the interviewee to freely express their opinion. With this type of interview, the direction of the interview is not predetermined but determined by both the interviewer and the interviewee. Hence, each interview mostly takes a different format. In a semi-structured interview, the features of structured and unstructured interviews are combined.

Since interview was adopted as the means of data collection in this study, an interview guide was prepared so as to ensure that there was some structure to the interviews (Bowen, 2005). The interview sessions were, however, conducted as conversation sessions, so as to facilitate some level of flexibility in the data collection process, and also enhance the easy extraction of detailed information from the respondents. This means that a semi-structured interview was used in this study as the primary means of data collection. Additional data collection method used in this study was desk-based, which was done through the review of policies and documents (both electronic, Internet-based, and hard-copy) relating to supply chains, and supply chains' information security and information assurance. Risk profile analysis of organisations was also done, so as to acquire additional data. The alignment of this study's research questions to the framework adopted in this study is presented in Chapter 6.

5.5 Sampling

Irrespective of the research method and approach to a study, it is a general requirement for the researcher to decide on the sample to be selected to participate in the study. If the population and sample of a study are not correctly determined or targeted, the outcome of the study might do more harm than good. Hence, data has to be collected from the right people, objects or events that can provide the correct and appropriate answers that can help address the issue being investigated. According to Sekaran (2006, p.265), population "refers to the entire group of people, events or things of interest that the researcher wishes to investigate", while, population frame is "a listing of all the elements in the population from which the sample is drawn". Samples, on the other hand, are a subset of a population, while sampling is the process of selecting the right and sufficient sample to represent the entire population (Surbhi, 2016).

Sampling strategies are generally divided into two categories which are probability and non-probability (Surbhi, 2016). Probability sampling, also referred to as random sampling, is a sampling strategy in which all the elements in a population have an equal chance or a known probability of being selected. According to Ritchie *et al.* (2003), this sampling strategy is generally considered to be most appropriate for quantitative research and inappropriate for qualitative research. Non-probability sampling also referred to as non-random sampling, is a sampling strategy in which units or group to represent a population are deliberately selected from within the population. In this sampling strategy, samples are selected based on certain criteria that fit the objectives of the study being conducted, and not all the elements in the population have an equal chance or a known probability of being selected. It is generally considered the most appropriate sampling strategy for a qualitative research.

In this study, being an exploratory and a qualitative study, the non-probability sampling strategy was adopted. The non-probability sampling strategies are purposive sampling, convenience sampling, quota sampling and snowball sampling (Surbhi, 2016). Although, in the study of Feild, Pruchno, Bewley, Edward P. Lemay, & Levinsky (2006), non-probability sampling strategy has been broadly categorised into two, which are, convenience and purposive (e.g. quota and judgemental sampling). With purposive sampling (also referred to as criterion-based sampling), the sample selection is based on certain criteria, characteristics or particular features. The judgemental sampling, in which samples are selected based on the elements that are best positioned to provide the required information, the quota sampling, in which certain elements are represented based on the assignment of a quota, and the theoretical sampling, in which the researcher samples units, people or incidents, based on “their potential contribution to the development and testing of theoretical constructs" (Ritchie *et al.*, 2003, p.80), are all classified as types of purposive sampling strategy. With convenience sampling, the sample is chosen based on ease of access to the sample elements that can provide the needed information. While, with snowball sampling, people who are already interviewed are asked to identify other people they know that fit the study or sampling selection criteria. In this study, the purposive sampling method was adopted.

In qualitative research, the selection of sample size should be based on the ability of the subject to provide relevant information that answers the research questions (Brink, 1993). Hence, to avoid insufficient or inaccurate data, researchers are encouraged to use their judgement and specific criteria, based on the best available evidence, to determine the subjects that can provide accurate and well-informed responses to the questions being asked. This study is based on two different fields of study, the first being information security and assurance, and the second being supply chain. To adequately cover the objectives and scope of the study, participants were drawn from two categories of organisations, which are supply chain and logistics organisations, and Information Technology (IT) consulting organisations. Samples were drawn from three different organisations from each of these two categories. The reason for drawing samples from three different organisations from each of these two categories, is so as to have diverse respondents that can present broad views on the subject being investigated.

According to Sindhuja (2014, p.460), "most studies on information security have considered organisations as the unit of analysis". Hence, in this study, six organisations were used as the unit of analysis. The rationale and criteria considered in selecting these organisations are:

Rationale

- Supply chain and logistics organisations were chosen because the context of the study is within supply chains' structures and processes. Logistics is generally considered an integral part of supply chain, hence the choice of logistics organisations.
- IT consulting organisations was chosen because the main focus of the study is on understanding information and information systems' security and how assurance can be provided on these two (i.e. information and information systems). The consideration for this rationale is further presented in the criteria that were considered when choosing the IT consulting organisations.

Criteria

The organisations that were chosen for this study met the following criteria:

Supply Chain Organisations

- Have a functioning supply chain operation, structure and process.
- Have a working technology or information system for driving their supply chain operations, structures and processes.
- Have a good number of employees (at least 500) working across the different units of the supply chain.
- Be "willing to allow access to employees at various organisational levels and be willing to disclose any information the researchers considered pertinent to the study."

IT Consulting Organisations

- Must be serving at least one supply chain organisation, especially with regards to their IT infrastructure
- Must have dealt with some form of information security issues/challenges of the organisations they are servicing.
- Be "willing to allow access to employees at various organisational levels and be willing to disclose any information the researchers considered pertinent to the study".

It is also important to provide the criteria for the selection of participants that participated in a study (Bowen, 2005). The criteria for selecting the individuals that participated in the study are:

Supply Chain Organisations

- Must be actively involved in the structures and processes of the organisation.
- Must be involved in the use and sharing of information within the organisation's supply chain network.
- Must be involved in decision making within the organisation, hence, team leaders, managers and directors were mostly selected to participate in the study.
- Employees from within the IT unit of the organisations were also selected to participate in the study. This is because of their engagement with the technologies and information systems used within the organisation to drive their operations, structures and processes.

IT Consulting Organisations

- Must be involved with the client side of the business, especially the clients with supply chain businesses and operations.
- Must have dealt with some form of security issues/challenges of the organisations they are servicing.
- Must be involved in some level of decision making.

The number of participants drawn from each organisation and that represented each category, that is, supply chain and logistics organisations, and Information Technology (IT) consulting organisations are presented in Chapter 7 (the analysis chapter).

5.6 Data Analysis

Regardless of the adopted research approach, methodology or paradigm, data analysis means the same thing - the process of making meaning from acquired data (Simon, 2011). It also entails the interpretation of the meaning made from the acquired data. In a quantitative study, the researcher, in most cases, often wait until the required amount of data sample is collected before data collection is brought to a close and analysis is initiated. In a qualitative study, however, the researcher has the liberty to analyse their data on a continuous and on-going basis, that is, throughout the data collection process or in some cases, throughout the lifespan of a research project (Simon, 2011). The continuous data analysis that can happen in qualitative data analysis has been considered as one of the key benefits of using the data analysis method. This is because such analysis (i.e. the continuous analysis of data) can lead to new areas of the study being identified and investigated as the study progresses (Lichtman, 2013).

According to Ryan (2006), data analysis helps in providing the evidence that is required in showing the existence of a certain phenomenon or a certain type of knowledge. Hence, it is considered an integral part of any research process. However, it is the most complex aspect of conducting a qualitative research study (Lichtman, 2013) because it involves taking a large amount of data that may be without any clear meaning or that may be cumbersome, and interacting with it (i.e. the data) in such a way that meaning and sense can be made from it. According to Lichtman (2013), most researchers of qualitative studies often get engrossed in data collection that they only start any form of data analysis after all data has been collected. This makes qualitative data analysis seem like a linear progression or process that occurs immediately after data collection and before writing the results when in actual sense, it should be treated as a spiralling or circular process involving the gathering and analysis of data.

There is no one right way to data analysis in a qualitative study (Lacey & Luff, 2009). This is because data analysis in a qualitative study "is a process that moves between questions, data and meaning" (Lichtman, 2013, p.255). It is also mostly considered an inductive and iterative process, which is geared towards identifying key concepts, patterns or categories from the collected and analysed data (Bazeley & Jackson, 2013). As explained in the study of Bowen (2005), it is considered an inductive process because the key concepts, patterns or categories that are identified during the process (i.e. data analysis process) emerge out of the transcribed data rather than being imposed or suggested before data collection, transcription and analysis. Bazeley (2009), however, further explained that data analysis in a qualitative study goes beyond the emergence or simple identification of concepts, patterns and categories, it also involves the analysis and interpretation of the identified concepts, patterns or categories. According to Lacey & Luff (2009), the stages in a qualitative data analysis are:

Transcription: Qualitative studies often involve some degree and form of transcription. When conducting a qualitative study, it is not often appropriate to write up summary notes from the tape recordings, because there is a possibility of the researchers' bias, as the researcher may only include the sections that seem interesting or relevant to them in the summary note. Hence, it is often recommended that the recorded data be transcribed verbatim from the tape recordings.

Data Organisation: It is necessary, after transcription, to organise data into section (for easy retrieval). This can be done by either giving each interview a code or number or by breaking the interview into different context. At this stage also, the interview respondents are given a code number or referred to by a pseudonym, for the purpose of ensuring their anonymity and confidentiality. It is also recommended that the unit of analysis is decided at this stage. That is, whether each paragraph, sentence, line or word of the transcribed data be numbered for easy retrieval and analysis purposes.

Familiarisation: Once the transcription and data organisation process begins, the process of familiarisation is also initiated. This is so because, in the transcription and data organisation stages, the researcher would have listened to the recordings or watched the video materials (where applicable), and would also have read and re-read the transcribed data, made memos and summaries. All these activities familiarise the researcher with the data. This stage is more important if the main researcher did not gather the data themselves.

Coding: Certain ideas manifest in the transcript that can be given preliminary code. These ideas could manifest in the form of words, phrases, sentences or concepts. These codes are often identified by the terms used by the respondents or by the researcher in the form of names used to identify the underlying concepts expressed by the respondents. The codes serve to begin the process of data categorisation and analysis. They in some cases might change from time to time. In the study of Lichtman (2013), it was also explained that coding often leads to categorisation, and subsequently, to concepts (sometimes referred to as themes) being developed. In the study, coding, categorisation and concepts were referred to as the three Cs of analysis in a qualitative data analysis.

Concept Identification: At this stage, emerging concepts are being identified, and re-coding is being done so as to develop better defined categories. The identified concepts are often associated with the identified issues with which the research was started. These concepts are often generated from the data itself, although, other theoretical ideas and concepts could also be incorporated in the final report.

Report Writing: It is at this stage that the meaning of the identified themes or issues from the transcribed and analysed data are discussed. The relationship between the themes and their meaning and impact on the research study is also presented at this stage.

In the analysis of a qualitative data, several methods can be adopted. Some of these methods are explained below:

Content Analysis: This is a qualitative data analysis method that according to Lichtman (2013, p.259), "has a structure and is more in keeping with the position of looking for rigour and acceptance". It adheres to the naturalistic paradigm because it is a method that is used to extract and interpret meaning from the content of text data (Hsieh & Shannon, 2005). With this method, the number of times a concept or a particular word occurs in a narrative is categorised quantitatively and then subjected to statistical analysis (Lacey & Luff, 2009). Hsieh & Shannon (2005) in their study identified three approaches to content analysis, and they are; the *Conventional approach* (in this approach, categories and concepts are derived directly from the text), the *Directed approach* (in this approach, data analysis starts with prior research findings or a theory that is used to guide the development of categories and concepts) and the *Summative approach* (this approach involves keywords or content counting and comparisons, after which the interpretation of the underlying context in done).

Thematic Analysis: This is the most commonly used qualitative analysis method because it is considered as a tool that can be used across other qualitative analysis methods. It is also considered an analysis technique that is independent of any epistemology and theory, and hence, can be applied to different types of epistemological and theoretical approaches (Braun & Clarke, 2006). According to Braun & Clarke (2006, p.79), it "is a method for identifying, analysing and reporting patterns (themes) within data". Hence, it is perceived as an analysis method in which all units of data (e.g. paragraphs or sentences) are given a particular code, so as to enable their easy extraction and examination in more details, and thus be able to generate patterns (Lacey & Luff, 2009). The patterns identified using this method are often identified through the process of coding, sifting and sorting. These patterns do not just illustrate themes, but also illustrates the categories of analysis and the analytic points that a researcher should use in making sense of his/her data and in presenting the findings of his/her study. According to Lichtman (2013), however, it is not easy to capture a person's thoughts and feelings, and identify them in patterns or portray them in themes. In this study, thematic analysis was adopted as the method of data analysis.

Discourse Analysis: As explained in the study of Souto-Manning (2014), discourse analysis is a valuable method of analysing social phenomenon, because it identifies and presents the connection between social contexts, situations and discourses. According to Lichtman (2013), this is a technique that was originally perceived as the analysis of the structure of text content in terms of syntax and semantics. But, it is now seen as a way in which text is being analysed based on how and where they are situated in the overall text being analysed. Parker (2013), however, explained that the researchers adopting this method might need to adopt ideas from other methods.

Narrative Analysis: According to Souto-Manning (2014), narrative help in putting meaning into what is experienced, known and felt in the real world. It is one of the most used means of systematising human experiences and interactions. Hence, this analysis method focuses on how people interpret and make sense of their interactions and experiences in society, through language. In this type of analysis, the emphasis is on telling stories or finding the narrative that can be used as a formal or structured way of transmitting information. As explained in the study of Braun & Clarke (2006), this method is an example of a case-study or biographical form of analysis which searches for patterns or themes for narration, within a data item (e.g. individual interview), as against across an entire data set.

Constant-Comparative Analysis Method: This method allows social theories to be systematically generated from data, through a process of structured and rigorous data analysis (Bowen, 2005). It is an analysis procedure that is closely associated with grounded theory (Lichtman, 2013). When using this analysis method, the researcher looks for and tries to establish relationships between emerging categories and concepts, by constantly and continuously comparing them (i.e. the emerging categories and concepts), until a theory or theories emerge. The constant comparative process is often continued by the researcher until what is called theoretical saturation is reached. Theoretical saturation is the point where no new significant concepts or categories are emerging. The emerged theory or theories in the constant-comparative data analysis approach is often perceived as provisional until validated by others (Lacey & Luff, 2009). What distinguishes this method from other qualitative data analysis method is that this approach emphasises a theory (or theories) as the final output of the research, while most other qualitative data analysis methods may legitimately terminate their result at the description or interpretation level.

Framework Analysis method: This method shares many common features with thematic analysis. It is an approach that is adopted in qualitative data analysis when outcomes or recommendations are required within a short period of time. There are five stages involved when using the framework analysis method (Lacey & Luff, 2009), and they are:

Familiarisation: involves the transcription of collected data and the reading of transcribed data.

Identifying a thematic framework: involves the initial coding, which is often based on the emerging issues that were identified in the familiarisation stage.

Indexing: involves the process of using textual or numerical codes to identify specific information which corresponds to the identified themes from the transcribed data. This stage is commonly known as the *coding* stage

Charting: involves using headings that have been derived from the themes to create charts that allow the dataset to be easily read. The charts can be based on each theme across the respondents or each respondent across the themes.

Mapping and Interpretation: at this stage, associations, concepts, patterns and explanations are derived and developed from the themes and charts. This stage is often aided by visual plots and displays.

Qualitative Comparative Analysis (QCA): This is an analysis method that is employed when the study deals with comparison across cases. As explained in the study of Lichtman (2013, p.260), "its purpose is to preserve the complexity of a single case while making comparisons across cases". According to Jordan, Gross, Javernick-Will, & Garvin (2011), it involves the identification of specific or particular outcome of interest and the conditions or factors that have been deemed to possibly be affecting the outcome. In this method, the data collected are quantified and tabulated for each contributory factor and outcome under analysis. One of its main strength is that is it a technique that allows the investigation of multiple conjectural relationships across cases.

5.6.1 Data Analysis Process in this Study

This section explains how the data analysis process (Figure 5.2) in this study was conducted, starting from data collection to data analysis. As explained earlier in section 5.4.1, interviews were conducted in this study. Prior to the commencement of the interviews, expert analysis of the data collection instrument and process was done as a form of pilot study. This helped with identification and management of potential researcher's biases (Chenail, 2009). For the expert analysis, the research instrument was given to experts in the core fields (i.e. Information Security and Assurance, and Supply Chain) that this study is evaluating. This is so as to get their input on the research instrument and the anticipated data collection and analysis process. The expert analysis also served as a means of ensuring the credibility of the research questions and the data collection and analysis process. After the expert analysis was concluded, where necessary, questions were refined and the data collection and analysis process was modified, as deemed fit.

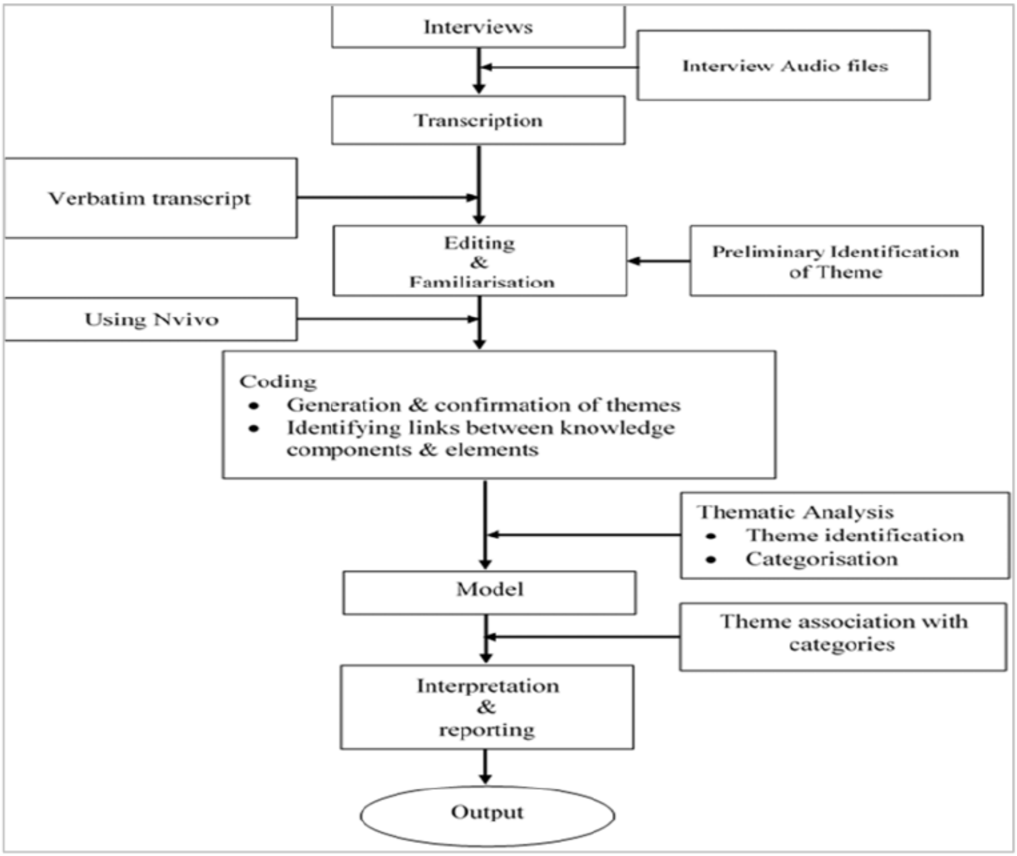

Interviews
Interview Audio files
Transcription
Verbatim transcript
Editing & Familiarisation
Preliminary Identification of Theme
Using Nvivo
Coding
• Generation & confirmation of themes
• Identifying links between knowledge components & elements
Thematic Analysis
• Theme identification
• Categorisation
Model
Theme association with categories
Interpretation & reporting
Output

Figure 5.2: This Study's Data Analysis Process

During the pilot phase, but after the expert analysis was completed, interviewing the interviewer approach as suggested by Chenail (2009), was also used by the researcher to further ascertain the credibility of the research instrument and the research process. This approach as described in the study of Brink (1993), enables the researcher to be conscious of the required manners and courage needed for conducting the interviews. Using this approach, the researcher enlisted a colleague to serve as the interviewer while he assumed the role of a participant. The use of the interviewing the interviewer approach was also useful in decreasing the possible bias that the researcher could have (consciously or unconsciously) while conducting interviews with the study's participants (Brink, 1993). After the pilot phase was completed, the research instrument, where necessary, was further adjusted.

All the interviews conducted with the study's participants were recorded with an audio recorder. The final analysis of data started after all interviews were completed. In this study, the completion of interviews (i.e. the point when data collection was terminated) was determined when saturation point was reached. As explained in the study of Lichtman (2013), that unlike in a quantitative study where data collection can be terminated once the required sample size has been reached, in a qualitative study, the termination of data collection can be determined once saturation point is reached. Saturation point is reached when nothing new is being learnt or no new information is being acquired (Fusch & Ness, 2015). It is an important point to be conscious of by a qualitative researcher because failure to reach it may affect the validity and quality of the research being conducted.

It is important for interviews to be transcribed because a transcribed interview is a more rigorous type of evidence that offers a more accurate representation of what was captured during the interview (Hammersley, 2010). In this study, in order to obtain an accurate representation of what was captured in the interviews, all the conducted interviews, which were recorded, were transcribed verbatim in Microsoft Word. Transcription is not a simple and straightforward task. It is a task that requires judgement about the level of details to be captured. To ensure the level of required details and information is captured, the transcription in this study was done using a listen-and-type method as against using a voice recognition software. This is because the listen-and-type method has been deemed to be more accurate when transcribing (Johnson, 2011). Although, it is a more difficult and time consuming method.

An important aspect of data analysis in a qualitative research is the search for concepts, meaning, patterns, categories or themes through the analysis and interpretation of the transcribed data (Yin, 2003). In this study, the analysis of data was done on an ongoing basis as suggested by Simon (2011) and Lichtman (2013), and not after all interviews and transcription were completed. Hence, the analysis started through the process of data familiarisation and organisation (Lacey &

Luff, 2009). At this stage of analysis, where necessary, notes, memos, mind-maps and summaries were made during the interview sessions and also, after each of the interviews had been completed. These notes, memos, mind-maps and summaries were manually analysed so as to generate preliminary themes that were later used in the final data analysis. These preliminary themes also served as a guide to the subsequent data that were collected (i.e. subsequent interviews).

The familiarisation of data was also done on all transcribed data, but this was after all interviews and transcription have been completed. This was done so as to generate additional themes. After familiarisation was completed, the categorisation and organisation of data were then performed on the transcribed data. This helped with the identification of additional new themes, patterns and concepts that emerged from the data. The categorisation (sometimes referred to as coding) done in this study also helped the researcher in making comparisons and contrast between the themes, patterns and concepts that emerged from the final analysis of data (Thomas, 2010). Thus, making it possible for the researcher to deeply reflect on the complex threads of the data, so as to make sense out of them. After this process was completed, the identified themes, patterns and concepts that emerged were then associated with the identified issues with which this research was started.

In order to effectively perform the analysis of the data collected in the study, a qualitative data analysis software (QDAS) called NVivo was used to aid data management and the process of data analysis. NVivo is a tool designed to facilitate the process of qualitative data analysis. According to Lacey & Luff (2009), it makes the process of coding and re-coding much simpler, and enables the relationships between coded data to be developed and displayed, sometimes, in the form of models. These models graphically depict the interviewees' responses. In this study, NVivo was used to enhance the easy search and retrieval of data e.g. particular words or phrases. With its use, themes and concepts were coded and some (i.e. themes) were generated. These themes and concepts, in addition to the notes, memos and summaries that were made during the interview sessions, were used to show the relationship between the findings from this study's analysed data and its objectives.

This study adopted an inductive approach in the analysis of data. After themes were generated and coded into the NVivo software, thematic analysis, which is adopted in this study as the analysis method, was then used to identify (i.e. from the generated themes) the themes that were relevant and appropriate for answering this study's research questions. By using thematic analysis, the researcher was able to perform the analysis and interpretation of the identified themes. This was done by moving the identified themes from a broad categorisation towards a more focused but detailed categorisation. This movement (i.e. from a broad to focused categorisation) further led to the discovery of themes that were eventually used in the final interpretation and reporting of the study’s findings, in relation to the study’s objectives. These discovered themes and their interpretation and reporting are presented and discussed in the data analysis and discussion chapters.

5.7 Research Evaluation

The traditional and two most common criteria for evaluating the credibility of a research study are validity and reliability. These two criteria are, however, mostly used in experimental and scientific studies, and they are also often based on standardised instruments for measurement (Thomas, 2010). Hence, they are popularly considered to be rooted in the positivist paradigm. Qualitative studies are not usually based upon standardised instruments, hence, validity and reliability as evaluation criteria are not often strictly or easily directly applied to them (Morse, Barrett, Mayan, Olson, & Spiers, 2002). In this study, the researcher takes cognisance of the fact that several authors, in their qualitative studies, have used the term trustworthiness in place of validity and reliability, when referring to the criteria used for evaluating the credibility of their research. The researcher, therefore, in this study, also prefers to use the term trustworthiness as the criteria that was used to evaluate the credibility and scientific merit of this study.

5.7.1 Trustworthiness

Evaluating the quality of a research is important if the findings from the research are to be considered viable or usable (Noble & Smith, 2015). Similarly, according to Merriam (1995), rigour is needed in all types of research in order to ensure that findings are to be believed and trusted. Trustworthiness is the corresponding term that is used as a measure of quality in a qualitative research. It has been described by Thomas (2010) as the extent to which the data collection and analysis of a qualitative study are believable and trustworthy. According to Thomas (2010), trustworthiness can be established by using four strategies. These strategies were developed in parallel to the internal and external validity, reliability and objectivity that are used as evaluating criteria in a quantitative research. The strategies are described below.

5.7.1.1 Credibility

This is the extent to which the collected and analysed data are believable and trustworthy. It is equivalent to internal validity, which is a criterion to evaluate how research findings match reality (Merriam, 1995). Although, in a qualitative study reality is subjective and relative to the meaning that people construct or interpret it to be, within their social context. To ensure the credibility of this study, expert evaluation was done (Brink, 1993). In this case, the interview schedule was given to experts in the core fields of this study for their input on the questions and possible outcomes of the study. To further ensure credibility, member check was also done with the findings of the study (Merriam, 1995). This means that feedback was sought from the participants of this study, on the data (transcribed), interpretations, findings and conclusions made in the study.

5.7.1.2 Transferability

This is often considered a challenge in qualitative research, because of the subjective nature of qualitative research. It is similar to external validity (Thomas, 2010), which is a criterion used to determine how the findings of a study can be generalised. The generalisability of a study means the extent to which the account of a particular population or situation can be extended to other populations or situations (under the same setting) other than those that were directly studied (Noble & Smith, 2015). Ryan (2006), although, believes that the emphasis of any research should be on quality and key insights rather than being on quantity and easy generalisation. Generalisability in qualitative research is therefore sometimes ignored in favour of giving preference to enriching the local understanding of the phenomenon or context being studied. However, as stated in the study of Thomas (2010), in a qualitative research, generalizability is something that has to be resolved by the reader of the research report. Their resolution should be based on how close the report is, to the context of the phenomenon they are studying.

According to Thomas (2010), transferability can be achieved or enhanced by providing a rich description and detailing the assumptions underlying a study, the research method adopted in a study and the context and overall settings in which the study was conducted. When this is done, it provides other researchers with sufficient information that can enable them to determine the applicability of the findings from such study to other studies. In this study, therefore, to enhance transferability, a detailed description of the process in which data was collected and analysed was provided (Bowen, 2005). These details also include the philosophical assumption that guided this study and the procedure that has been adopted by the researcher in constructing and connecting the findings from the analysed data to the identified issues with which this research was started. These details, the researcher believes can enable readers and other researchers appraise the importance of the meanings derived from the findings of this study, which subsequently can enable them to make their own judgement and draw their own inferences, regarding the transferability of this research outcome to their study.

5.7.1.3 Dependability

This is likened to reliability (Golafshani, 2003), which is a criterion to evaluate how consistent and reproducible the methods employed in conducting a research can be, under similar circumstances. It is also often described as the extent to which research findings can be replicated under similar circumstances and in a similar context. In a qualitative study, reliability is practically impossible because human behaviour and activities are not static, they are highly contextual and continuously changing based on different (influencing) factors. Thus, the different experiences of the participants of a study and their multiple interpretations of the reality of the same phenomenon but in a different context may not necessarily yield the same results. In this study, however, to provide some sort of reliability, the researcher tried to show that the results of this study are consistent with the data collected (Merriam, 1995). Furthermore, in order to provide reliability, "auditing which consists of the researcher's documentation of data, methods and decision made during the thesis as well as its end products" was done (Seale, cited in Thomas, 2010, p.322).

5.7.1.4 Confirmability

This is the degree to which the findings of a research study can be corroborated of confirmed by others. It is related to objectivity, which is a criterion for evaluating the extent to which accounts for or is aware of individual bias or subjectivity (Thomas, 2010). In order to ensure the confirmability of this study, the researcher will archive all the data that was collected, and also, the findings from this study, in an organised and retrievable form, so that they can be easily accessible to whoever is interested.

5.8 Ethical Considerations

This being a qualitative study, in-depth and open ended interviews were conducted. These interviews require that the researcher interacts directly and deeply with the participants of the study, so as to be able to obtain their perspectives, explanations and experiences, with detailed examples, of the phenomenon being studied. Since the study requires deep interaction with participants for the interviews that were conducted, the researcher was conscious of the fact that he was entering into the private space of the study's participants. This, therefore necessitates that ethical issues be taken into consideration, during and after the data collection process and also after the research study was concluded. According to Bowen (2005), researchers have an obligation to respect and protect the anonymity, confidentiality, privacy, dignity and rights of their study's participants. To ensure all these in this study, some issues, as suggested in the study of Thomas (2010), were addressed, because they have been identified as significant for ethical considerations. These issues are presented below:

> *Informed Consent*: In any research involving the human subject, informed consent is an important feature to be considered for ethical considerations (Bowen, 2005). Prior to commencement, participants in this study were informed by the researcher of the nature, purpose, data collection method and the extent of this research study. In addition to this, the researcher also explained the role of participants to them before the commencement of each interview. After all these had been done, the researcher then obtained informed consent from

each participant. Most of the obtained consents were verbally given by the participants, even though they were provided with printed informed consent document (Appendix C). These verbal consents were recorded on the same audio recorder used to record the conducted interviews of each respective participants.

Privacy, Anonymity & Confidentiality: The participants in this study were informed by the researcher, prior to the commencement of each interview that their privacy and that of their respective organisations will be protected. To ensure the protection of privacy and confidentiality, and also maintain anonymity, the researcher ensured that any identifying characteristics of each participant were removed before the widespread dissemination of the study's findings.

Voluntary Participation: Despite being told that their privacy, confidentiality and anonymity will be protected and ensured, participants were still made to know that their participation in the study was absolutely voluntary. They were also made to know that they could withdraw from participating in the study at any in the course of the data collection. Participants were made to know all this, before the commencement of their respective interviews.

Harm & Risk: Participants in this research study were guaranteed by the researcher that they will not be put in a situation where they might be harmed in any way, because of their participation in the study

Honesty & Trust: The researcher ensured that all ethical guidelines, as provided by the University of KwaZulu-Natal were strictly adhered to, in all relationships with the study participants and their respective organisations.

5.9 Conclusion

This chapter presented the research paradigm, the research method, approach and instrument that was adopted in this study. It also presented the population, sample and sampling criteria used in this study. Furthermore, the data analysis method and ethical considerations of this study were also presented. A qualitative research approach and method was adopted in this study. This approach often produces multiple realities of a phenomenon within the context in which the phenomenon is being studied. To adequately capture these realities, interviews were conducted. The analysis of the conducted interviews (i.e. after transcription), using thematic analysis, allowed for concepts and themes to develop. These concepts and themes are presented and discussed in the data analysis and discussion chapters, respectively. The next chapter, however, presents the framework that was adopted in this study. The chapter also presents the key research questions, and how these questions are aligned to the framework adopted in this study.

CHAPTER 6: RESEARCH FRAMEWORK

6.1 Introduction

A framework is a logical structure that guides the development of a study. According to Nalzaro (2012), it can be derived from existing theories, in which case it is referred to as a theoretical framework, and it can also be derived from related concepts, in which case it is referred to as a conceptual framework. Models, similar to frameworks, are symbolic representations used to express relationship among constructs and concepts, using minimal words. Theories, also similar to frameworks, are constructed so as to be able to explain, predict and understand phenomena.

In this study, a framework has been adopted to help in identifying the starting point of the research problem and to also help in establishing a direction for addressing the problem. In chapter 5, the research instrument of this study was presented. The research questions (presented in this chapter) entailed in the research instrument was derived and aligned to this study's research framework (also presented in this chapter). In this chapter, therefore, the alignment of this study's research questions to the framework adopted in this study, is presented. This chapter also presents how the framework applies to the overall study, so as to achieve the study's objectives. The layout of this chapter is presented in Figure 6.1.

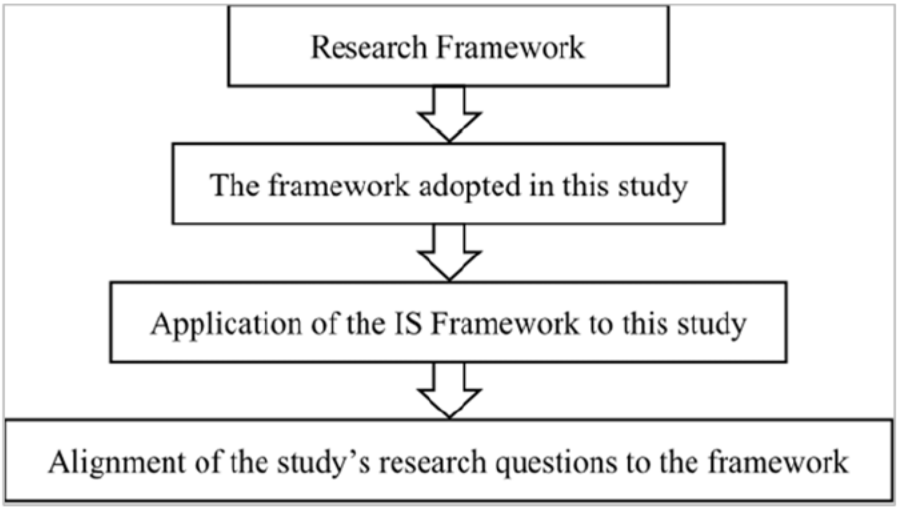

Research Framework
The framework adopted in this study
Application of the IS Framework to this study
Alignment of the study's research questions to the framework

Figure 6.1: The Layout of the chapter

6.2 The Framework Adopted in this Study

According to March & Smith (1995), research studies relating to information technology should not just be about information systems and their inherent technologies, but also about organisations. Hence, in this study, the "Information Systems (IS) Research Framework" (Figure 6.2) presented in the study of Hevner, March, Park, & Ram (2004) was adopted. This framework is composed of people, organisations and their existing or planned information systems. This framework has been explained in the study of Carlsson (2006), Peffers, Tuunanen, Rothenberger, & Chatterjee (2007) and Cronholm & Göbel (2016) as being useful and practical in solving identified research or organisational problems relating to IT or IS. The framework provides a structure that helps in connecting different concepts or methods. It also helps in understanding, evaluating and executing information system research, by combining the behavioural science and design science approach to identify problems in research or organisations, and to also develop, test and evaluate artefacts when and where necessary. These artefacts are often in the form of models, constructs, instantiations and methods that can be applied in providing possible solutions to identified research or organisational problems relating to IT or IS (Peffers *et al.*, 2007).

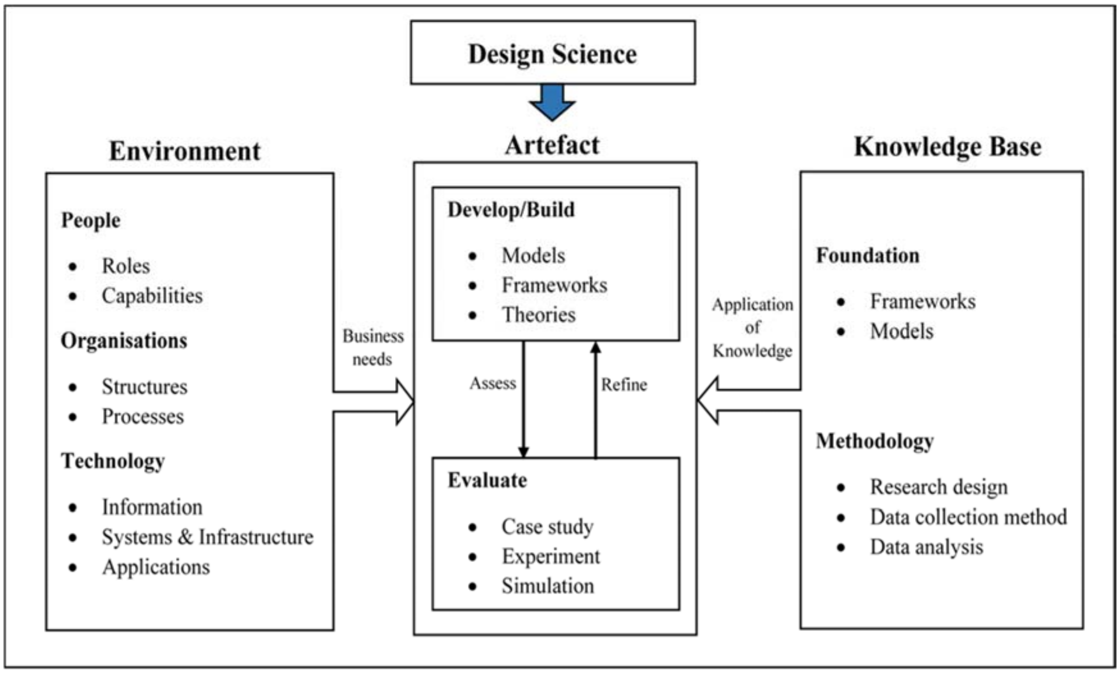


Figure 6.2: Adaptation of the Information Systems (IS) Research Framework to this Study (Hevner *et al.*, 2004)

Behavioural science and design science paradigms are fundamental to the discipline of information systems because they contribute to the convergence of people, organisation and technology (Peffers *et al.*, 2007). Technology and human behaviour are inseparable. Hence, the relevance of behavioural science, which helps in the identification of appropriate theories, frameworks or models that predict or explains organisational or human behaviour, in an IS research. According to March & Smith (1995), behavioural science, also be referred to as natural science, is a research domain that is aimed at understanding natural conditions and behaviour. It is often viewed as consisting of two main activities which are *discovery* (the process of identifying, generating or proposing frameworks, theories, models etc.) and *justification* (activities involving the validation of such frameworks, theories, models etc. for appropriateness of use). In this study, behavioural science was relevant to the identification of the framework that helped in understanding organisational and human behaviour with regards to technology, information, information systems, supply chain processes and their structures.

In recent years, IS researchers have developed and are increasingly adopting design science as an IS research approach and paradigm. Design Science is a problem-solving process with the objective of developing technology-based solutions to identified organisational or research problems (Hevner *et al.*, 2004). It may also be referred to as an approach that allows for phenomena to emerge from the interaction of people, organizations and technology in a way that the phenomena may be qualitatively or quantitatively assessed to yield an understanding that is adequate for problem-solving. According to March & Smith (1995), it attempts to create artefacts that serve human purposes of solving identified problems, especially technology oriented problems. With regards to the contribution to knowledge, design science research can contribute based on significance, generality and novelty of the designed artefact.

Design science involves two main processes which are to build an artefact and to evaluate the artefact for performance and fit to solving the identified problem (Cronholm & Göbel, 2016). The artefacts created through the design science approach are innovations that define the practices, ideas and technical capabilities through which the analysis, design, implementation and use of information systems can be efficiently and effectively accomplished. The creation of these artefacts often relies on existing theories, models or frameworks that have been developed, tested or modified through the intuition, creativity, experience and problem-solving capabilities of researchers. The evaluation of the artefacts helps in the generation of knowledge that can be used for further improving the built artefacts. For the evaluation of the effectiveness and quality of an artefact, empirical techniques, mathematical and computational methods are often used.

According to Hevner *et al.* (2004), the use of behavioural science and design science approach in an IS research should be done in two complementary phases. In the first phase, the behavioural science approach should be used to address the research through the identification (or development) and justification of theories, frameworks, models, constructs etc. that predict, explain or present human or organisational behaviour, ideas or phenomena that are related to the identified research problems, and that can guide in addressing the identified research problems. In the second phase, the design science approach, which extends beyond the boundaries of human or organisational capabilities, should be used for the development and evaluation of artefacts that are designed to provide a possible solution to the identified research problems.

The main objective of this study is to develop an information assurance model that can enable organisations to protect and sustain their respective information within the supply chain structures, and that can also enable them to minimise or prevent the risks that information within the supply chain processes could be exposed to. Thus, applying the IS research framework, this study develops and proposes an artefact in the form of a model for supply chain information assurance. According to Hevner *et al.* (2004), models are used to represent a real world situation and they help in the understanding of identified problems or challenges and in providing guidance on how to find a solution to the identified problems or challenges. Similarly, according to Nalzaro (2012), they are used to express concepts and relationships which help in the better understanding of a phenomenon being studied.

6.3 Application of the IS Framework to this Study

The *Environment* in the IS research framework represents the space in which the IS phenomena or problem of interest is being investigated. As stated in the study of March & Smith (1995), IT research should be adapted to the environment in which they are being conducted. In this study, the environments where the supply chain and logistics organisations, and the IT consulting organisations, which were the two categories of organisations from which the study's participants were drawn. As stated in section 5.5, three different organisations from each of these two categories were selected as this study's unit of analysis, and hence, they (i.e. the six organisations) constituted the environments in which the study was conducted. As shown in the IS research framework (Figure 6.2), the environment in which a study is conducted should be made up of people, the organisations and the information systems and technologies used for facilitating or enhancing the organisations' processes and functions.

In this study, selected *people* (selection criteria was stated in section 5.5), based on their roles and capabilities within the six organisations were interviewed. The *organisations* were also evaluated, through the study's participants. However, being the context in which this study was conducted, emphasis on the organisations' structures and processes was placed on the supply chain and logistics organisations used as case study in this study, The *information systems and technologies* used by the organisations (i.e. the six organisations) for acquiring, processing, storing and sharing information was also evaluated, through the study's participants, so as to determine how security and assurance can be adequately provided on information. Although for security and assurance, the emphasis was placed on the IT consulting organisations, this is because they are required (as part of the selection criteria in this study) to have dealt with some form of information security issues/challenges of the organisations they are servicing.

The *Knowledge Base* in the IS research framework represents the raw materials that help in the accomplishment of an IS research. It constitutes the foundation and methodology upon which an IS research study is based. Its effective use ensures rigour in an IS research. As shown in the framework (Figure 6.2), the models, frameworks, theories etc. adopted in a study, serves as the foundation upon which the knowledge base of the study is built, while the data collection method, validation criteria, data analysis techniques etc. adopted in a study informs the methodology adopted to drive the generation of knowledge in the study. The methodology used to achieve the objectives of this study was presented in Chapter 5. However, the frameworks (within the framework component of the knowledge base section) within the IS research framework adopted in this study are presented in this chapter.

In the first phase of the application of the IS research framework to this study, the frameworks that help in understanding supply chain information security were identified and adopted. These frameworks were also relevant in understanding human and organisational behaviour and activities that affect the security of information and information systems within supply chains. As explained by Hevner *et al.* (2004), rigour is achieved in a study when existing models, frameworks or theories are appropriately applied to the study. Hence, the supply chain security framework (Figure 4.2) developed by Speier *et al.* (2011), was adopted in this study. Based on the literature review, changes were, however, made to the framework (as shown in Figure 6.3) for its adaptation to this study. Also adopted, as a framework in this study, was the Supply Chain Information Risk Management (SCIRM) framework (Table 6.4) developed by Maharaj & Ajayi (2011). The SCIRM framework was developed by the researchers to understand the severity of the threats that could exploit information vulnerability within supply chains.

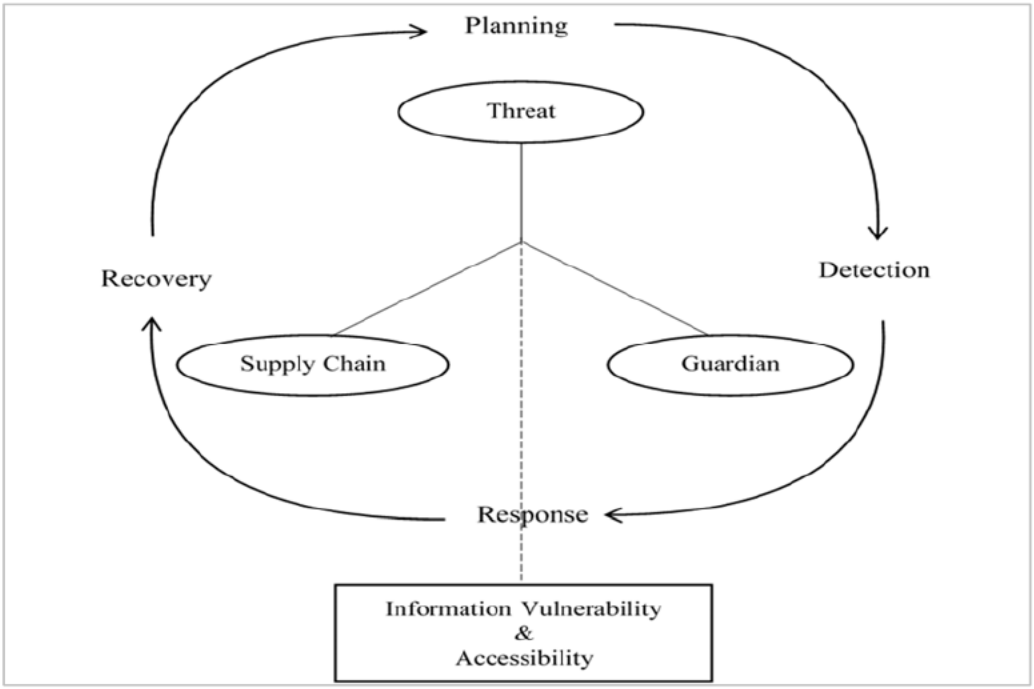


Figure 6.3: Adaptation of the Supply Chain Security Framework to this Study (Speier *et al.*, 2011)

Nodes	risk severity (0 – no risk, 1 – mild, 2- moderate, 3- high)						
	Malware	System Hackers	Organizational Scam	Information Inconsistency	System Breakdown	Environmental Disaster	Total
H-H	0	0	2	3	0	1	R_{HH} = 6
H-S	1	2	2	3	1	1	R_{HS} = 10
S-S	2	1	0	0	2	1	R_{SS} = 6
S-H	0	0	0	1	1	1	R_{SH} = 3

Table 6.4: The SCIRM Framework (Maharaj & Ajayi, 2011)

The meanings of the notations used in the SCIRM framework (Table 6.4) are presented below:

H: Represents Human. This means using an employee as a means of capturing, processing, reporting and sharing information within the supply chain.

S: Represents System. This means using systems (e.g. ERP, EDI) as a means of capturing, processing, reporting and sharing information within the supply chain.

Hence:

H-H: refers to a situation where information is shared by a human to human. This could also be referred to as "Manual" information sharing.

H-S: refers to a situation where information is shared by a human to the system. This could also be referred to as "Semi-Automated" information sharing.

S-S: refers to a situation where information is shared from system to system. This could also be referred to as "Automated" information sharing.

S-H: refers to a situation where information is shared from system to human. This is also another type of "Semi-Automated" information sharing.

The adoption of the SCIRM framework (Table 6.4) in this study was relevant because one of the primary objective of the study is to understand the challenges surrounding the security of information and information systems, and this entails, understanding the vulnerabilities and threats (and their severity) to information and information systems. It was also relevant in understanding how to determine the right reaction (response) strategy and the best restoration (recovery) action (based on the severity of the identified threat or security breach to information) to be adopted in the protection of supply chain information. With the SCIRM framework, human and organisational activities and behaviour with regards to the sharing of information and the exposure of information to vulnerabilities was also examined. The adaptation of the supply chain security framework (Figure 6.3) to this study was important and relevant as well, because it covers, in a process form, the core objectives of information assurance, which as identified in the literature are protection (which involves detection and reaction (response)) and restoration (recovery).

The explanation of the supply chain security framework provided by Speier *et al.* (2011), in relation to its adaptation to this study is that the identification of security and protection approaches (i.e. planning, detection, response and restoration) to supply chain information, builds upon the Routine Activity Theory (RAT) (Cohen & Felson, 1979). The adaptation of the RAT to this study is such that or means that a security breach to supply chain information is triggered or influenced when there is an intersection between the threats to information, the vulnerabilities within the supply chain and the absence or insufficient effective guardians/protective measures. When this situation occurs (i.e. the intersection), information and information systems become vulnerable and accessible to intruders. To manage the vulnerability and accessibility of information to intruders, Speier *et al.* (2011), suggested four processes that should be done successively. The processes are planning, detection, response and recovery. These processes are important in the actions to be taken within a supply chain before, during and after an information security breach or incident.

The *Artefact* component of the IS research framework represents the output of the adaptation and the application of the knowledge base components and the environment component of the framework to the identified research or organisational IT related problems. According to Cronholm & Göbel (2016), the artefact component of the IS research framework is the part of the framework that represents the design science research (which is involved in the development and evaluation of artefacts). In this study, the artefact/output is a model developed for supply chain information assurance. The model was built and evaluated to determine its performance and fit to solving the identified research problems of this study. The evaluation of the model was done so as to also ensure that it is befitting for the environment (i.e. supply chain organisations) in which it is going to be adopted.

6.4 Alignment of the Study's Research Questions to the Framework

In the early stages of data collection in this study, the study's participants that deals mainly with the security of information within the supply chain were asked questions that were aimed at validating the SCIRM framework. After this was done, it was necessary to make adjustments to the framework. The adjusted framework is presented in chapter 8. The adjustments to the SCIRM framework, coupled with the supply chain security framework was then used to form the knowledge base of the IS research framework. According to Cronholm & Göbel (2016), the IS research framework is most effective when primary data are used to develop the artefact that is intended to solve the identified research or organisational IT related problem. In this study, data was collected in an original context. Some of the main questions used to gather data from the study's participants, and how the questions are aligned to the adopted framework is presented below (the complete research questions can be found at Appendix B):

The Environment

People (Role and Capabilities)

- *The study's participants were asked to explain their role within the organisation.*

  The purpose of this question was to determine the role of the interviewee within the supply chain network (in the case of the supply chain and logistics organisations) and for the supply chain organisations they are servicing (in the case of the IT consulting organisations).

Organisation (Structure & Processes)

- *The study's participants were asked to explain the structures in place within the supply chain.*
- *They were also asked to explain the processes involved in the supply chain.*

  The purpose of the two questions above is to understand the function of the different organisations within the supply chain. This applies to both the supply chain and logistics organisations and the IT consulting organisations. These questions also helped identify processes within the supply chain and the organisations that constitute the source, intermediary and destination of the supply chain

Technology (Information and Information Systems)

- *The study's participants were asked to explain the types of Information gathered, stored, used and shared within the supply chain.*
- *They were also asked to explain how the information is gathered, stored, used and shared within the supply chain.*
- *Furthermore, participants were asked to explain the types of information systems used to support the processes and structures of the supply chain.*

The purpose of these questions was to understand the role, impact and influence of information and information systems on the supply chain processes and structures.

The Knowledge Base

Foundation (Framework)

The Supply Chain Information Risk Management (SCIRM) framework

- *The study's participants were asked to identify and explain the types of threats that information is exposed to within the supply chain.*
- *They were also asked to explain the effects and severity of the identified threats to information within the supply chain*.

  Before responding to this question, respondents were provided with the nodes in the SCIRM framework and asked to identify which of the nodes poses the highest or lowest vulnerability point to the supply chain.

The Supply Chain Security Framework

The identified threats in this study (from using the SCIRM framework), coupled with those identified in the literature, were used in the supply chain security framework, to determine the appropriate *guardian*, *protection* and *restoration* approaches and options that are considered viable in ensuring security and in providing the assurance that supply chain information and information systems will deliver and perform as expected.

- *Respondents were asked to explain how the protection (includes the detection and response) of the information used within the Supply Chain is ensured.*
- *Respondents were asked to also explain the effects and severity of the identified threats to information within the supply chain*.
- *They were also asked to explain the measures in place within the supply chain to ensure:*
  - That information access is prevented from an unauthorized access
  - That information system is prevented from unauthorized access
  - The accuracy of information as it flows through the supply chain
  - The consistency of information as it flows through the supply chain
  - That information and information system are available at all times
  - The authenticity of information (also looked at authenticity of information senders and receivers)

- *Respondents were asked to explain the restoration measures within the supply chain, in the case of any information breach*.
- *They were also asked to identify and explain the policies, standards or frameworks used to ensure information security and to provide the assurance that supply chain information will deliver optimally with little or no form of breach*

6.5 Conclusion

Frameworks, just like models and theories that are adopted in a study are deemed to be the foundation upon which the core components of the study is based. Hence, understanding how a study can build on any or all of them (whichever is adopted in the study) is important in achieving the study's objectives and in developing the study's research questions. The IS research framework was adopted in this study because the main aim of this study is to develop and propose an artefact in the form of a model for supply chain information assurance. To complement this framework, two other frameworks, namely, the supply chain security framework and the Supply Chain Information Risk Management (SCIRM) framework were also adapted and adopted respectively in this study. These frameworks guided the development of the research questions used to achieve the study's objectives. The analysis of the participant's responses to the research questions is presented in the next chapter.

CHAPTER 7: DATA ANALYSIS

7.1 Introduction

Data, if left in the form they are collected, does not produce any meaning. Hence, the mass of data gathered through any data collection instrument needs to be analysed so as to generate meaning that helps in identifying key concepts, patterns and ideas, which are relevant to the purpose of collecting the analysed data. Data analysis is a requirement and the foundation upon which a researcher draws conclusion and recommendations. It is therefore important that it is detailed enough to support the researcher's point of view. It is also, however, important that during the data analysis process, the researcher avoid preconceptions and biases, as this might influence the outcome of the analysis of the collected data.

Qualitative data were collected in this study, hence a qualitative data analysis approach was adopted. This approach, often referred to as an inductive approach (Bazeley & Jackson, 2013), allow critical themes, patterns and ideas to emerge out of the transcribed data rather than being imposed or suggested during the data transcription and analysis process. To effectively perform the analysis of the data collected in this study, NVivo was used to aid data management and the process of data analysis.

In this chapter, the themes generated from the analysis of interviews, are presented. The chapter also presents the relationship between the generated themes and the study's research questions. The layout of the chapter is presented in Figure 7.1.

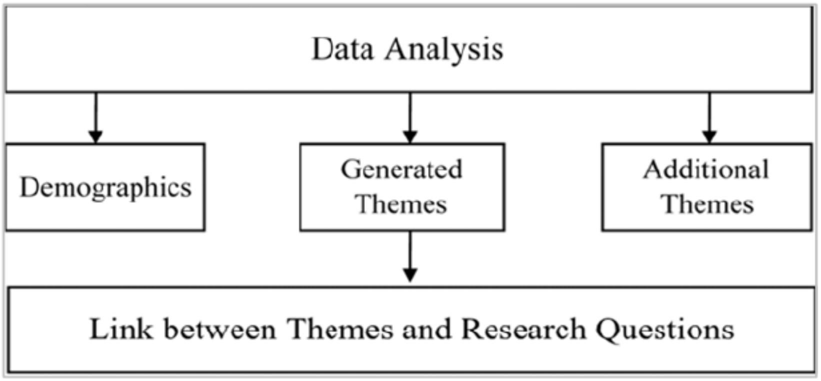


Figure 7.1: Layout of the Chapter

7.2 Demographics

In this study, as explained in section 5.5, participants were drawn from two categories of organisations, which are supply chain and logistics organisation (SCLO), and Information Technology (IT) consulting organisations (ITCO). From each of these categories, three different organisations were selected as the unit of analysis (Sindhuja, 2014). Hence, participants were drawn from six different organisations. The rationale and criteria considered in selecting these organisations were stated in section 5.5. Also, in the same section, the criteria considered in the selection of the participants that participated in this study was stated.

The participants in this study were in total, 19 employees from within the SCLOs and ITCOs. The participants drawn from the SCLOs were 9, and from the ITCOs, were 10. This is because these were the employees that met the criteria stated in section 5.5 and that were also available for interview. The demographic description of each participant is presented in Tables 7.1 – A (SCLO) and 7.1 – B (ITCO).

Participant's Code	Participant's Designation	Organisation's Category	Focus within the Organisation	Years of Experience	Gender
PS – 1	Manager	SCLO - 1	Logistics	Over 10 years	Male
PS – 2	Internal Auditor	SCLO - 1	IT Internal Auditor (Supply Chain & Logistics)	Over 5 years	Male
PS – 3	Executive Director	SCLO - 2	Supply Chain	Over 20 years	Male
PS – 4	Manager	SCLO - 2	Information Technology	Over 13 years	Female
PS – 5	Manager	SCLO - 2	Procurement	Over 15 years	Male
PS – 6	Manager	SCLO - 2	Business Planning	Over 11 years	Male
PS – 7	Manager	SCLO - 3	Supply Planning	Over 12 years	Male
PS – 8	Manager	SCLO - 3	Logistics & Customer Services	Over 9 years	Male
PS – 9	Manager	SCLO - 3	Personal Product Factory	Over 10 years	Male

Table 7.1 – A: Demographic Details of the Study's Participants (SCLO)

Participant's Code	Participant's Designation	Organisation's Category	Focus within the Organisation	Years of Experience	Gender
PI – 1	Partner	ITCO - 1	Strategy & Operations	Over 20 years	Male
PI – 2	Director	ITCO - 1	IT Governance & Security	Over 12 years	Male
PI – 3	Senior Consultant	ITCO - 1	Information Security	Over 9 years	Male
PI – 4	Senior Consultant	ITCO - 1	Information & Systems Assurance	Over 10 years	Male
PI – 5	Director	ITCO - 2	Operations	Over 15 years	Male
PI – 6	Head of IT	ITCO - 2	Data Security & Management	Over 15 years	Male
PI – 7	Manager	ITCO - 2	Solution Architect	Over 10 years	Male
PI – 8	Security Analyst	ITCO - 2	Network Infrastructure Security	Over 5 years	Male
PI – 9	Security Analyst	ITCO - 3	Network Security	Over 10 years	Male
PI – 10	Engineer	ITCO - 3	Infrastructure & Data Centre Systems' Security	Over 5 years	Male

Table 7.1 – B: Demographic Details of the Study's Participants (ITCO)

The notations used in the tables are described below:

Participant's Code

The names of the participants in this study have been omitted for confidentiality reasons. Hence, participants are represented by '*Participant's Code*' (i.e. the first column in the Tables 7.1 – A and 7.1 – B). The participant's code is used as an identifier for each of the participant in the study. This is considered necessary so as to be able to associate responses and quotes (used in the discussion chapter – chapter 8) to their respective respondents. The interpretation of the participant's code, as used in the tables, is explained below:

- P represents Participant
- S represents the SCLO category

- I represents the ITCO category

Therefore, PS – 1 represents a participant from the SCLO category, while PI – 1 represents a participant from the ITCO category. The exact organisation from within each category that each participant represents is shown in the respective tables.

Organisation's Category

The names of the organisations, from which participants were drawn for this study, has also been omitted for confidentiality reasons. Hence, organisations are represented by '*Organisation's Category*' (i.e. the third column in the tables). This representation is also considered important, especially in the discussion chapter. The representation of the categories, as shown in the organisation's category column, is described below:

Table 7.1 – A (SCLO)

As stated earlier, three organisations were drawn from the SCLO category. The representation of the three organisations are:

- SCLO – 1 represents '*the first supply chain and logistics organisation'*
- SCLO – 2 represents '*the second supply chain and logistics organisation'*
- SCLO – 3 represents '*the third supply chain and logistics organisation'*

Table 7.1 – B (ITCO)

Similarly, three organisations were also drawn from the ITCO category. The representation of the three organisations are:

- ITCO – 1 represents '*the first Information Technology (IT) consulting organisations'*
- ITCO – 2 represents '*the second Information Technology (IT) consulting organisations'*
- ITCO – 3 represents '*the third Information Technology (IT) consulting organisations*'

It was stated in section 5.5 that the reason for drawing samples from three different organisations from each of the two categories, is so as to have diverse respondents that can present broad views on the subject being investigated. Another reason was that, each organisation, after agreeing to their employees being interviewed for the study, indicated that only between 2 to 4 of their employees can be made available to participate in the study. This was mainly because of the tight schedule and limited availability of their employees. They all (i.e. the organisations), however, allowed the participants to be determined by the researcher. Hence, giving the researcher some level of control over who to participate in the study.

The limitation, on the number of employees that can be made available to participate in the study, necessitated the need to consider more than one organisation to be used as the study's site of data collection. Hence, three different organisations from each category were used as the study's site of data collection. This, as stated earlier, made it possible to have diverse respondents that could present different views on the subject being investigated.

Participants were determined by the researcher, not only based on their role within the organisational structure, but also, based on the criteria stated in section 5.5. This (i.e. the participant that met the criteria) was determined by the researcher (with the help of a representative from each of the organisations) through a short (about 5 minute) interview with possible participants. Through this interviews, the researcher was able to determine the 2 to 4 employees (as allowed by each organisation) from each organisation that was ideal to participate in the study.

In the selection of participants, the researcher tried to ensure that each of the participants interviewed has different roles, and more importantly, different focus within their organisation. Particular attention was also paid to ensuring that no two respondent from the same organisation have the same role and focus within their organisations. Around 74% of the respondents have more than 10 years of experience, while the remaining, around 26%, has more than 5 years of experience. From their experience, respondents were able to provide relevant and related responses (i.e. to the study's research questions), from which themes related to the study's objectives were generated.

7.3 Generated Themes from Interview Analysis

Most qualitative data analysis falls under the general heading of thematic analysis (Lacey & Luff, 2009). In which case, themes are generated from the analysed data. According to Braun & Clarke (2006), a theme captures the important aspects of the data in relation to the research questions and objectives and represents some of the important meaning and patterned responses within the data set. In the generation of themes in this study (using an inductive approach), the following steps were followed:

- Significant information was identified from the transcribed data
- Identified information was then labelled
- Labelled information was then grouped/categorised, based on similarities, into themes and sub-themes
- The grouped/categorised information (themes) were then loaded into the NVivo software as Nodes and Sub-nodes. The supernodes were considered as the main themes while the sub-nodes were considered as the sub-themes
- The NVivo software was then used to analyse interviews' responses by themes
- Using the NVivo software, models were then generated

These models represent (i.e. graphically) the participants' responses with regards to each identified themes. They also show the relationship between the nodes and sub-nodes that were developed, based on the identified themes from the participants' responses. As explained in the study of Ryan (2006), it is better to present a limited number of themes, so as to capture the essence of the analysed data. After the collected data in this study was analysed, a total of 6 main themes (Figure 7.2), which represented the supernodes in NVivo, emerged.

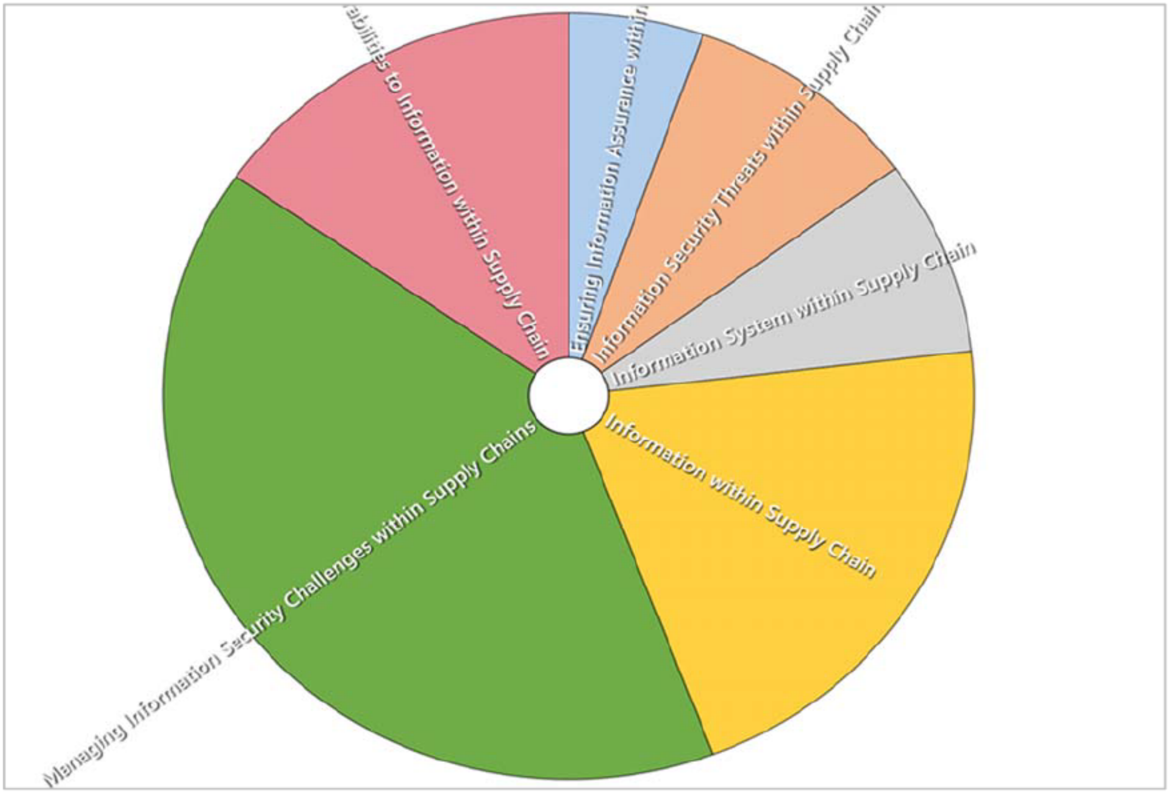


Figure 7.2: Emerged Themes by Number of Coding References

The Figure (7.2) shows the size of the segment that each main theme represents. This size is determined by the number of coding references, from the transcribed interviews responses, that relates to the generated themes. The main themes that emerged (as shown in Figure 7.2) and their sub-themes are presented in the next sections (i.e. 7.3.1 – 7.3.6). The detailed child themes for some of the themes are, however, not presented in this chapter. This is because those themes are considered more relevant in the discussion chapter. Hence, they are presented in chapter 8.

7.3.1 Information within Supply Chain

The study's participants were asked to discuss the relevance and use of information within their respective organisation and between them and the organisations they are partnering or collaborating with. The discussion was also focused on understanding the relevance and requirements of information in dealing with the processes and structures within organisations and their trading networks. As shown in Figure 7.3, four main sub-themes, which are related to the discussion, emerged from the analysis of participants' responses.

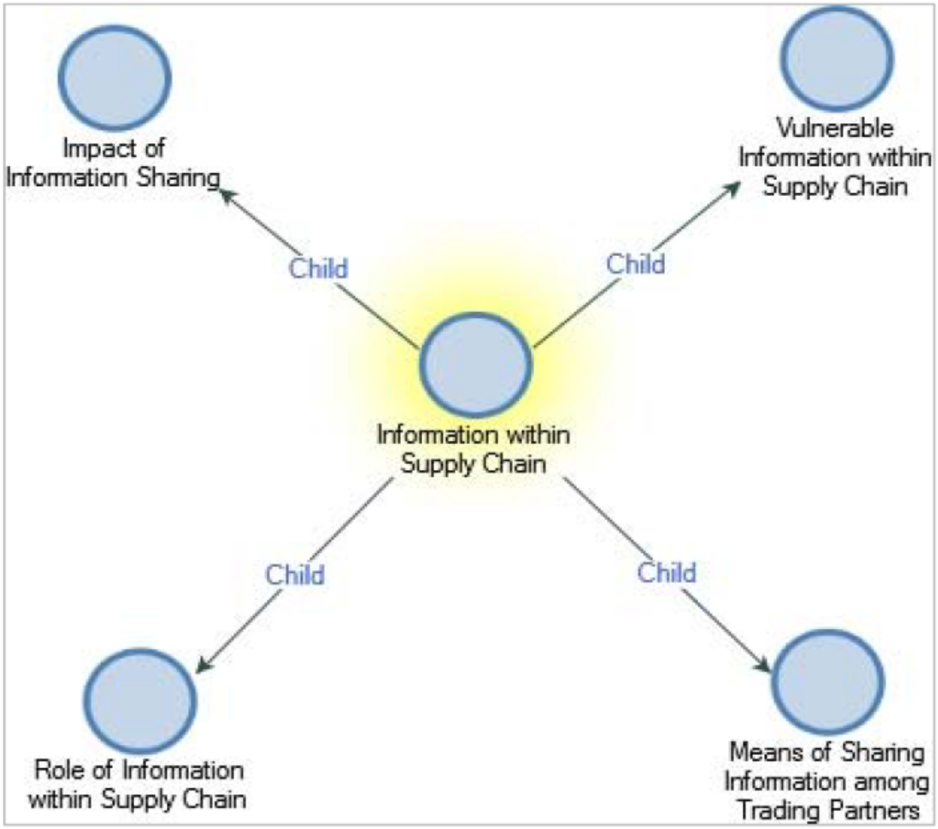

Impact of Information Sharing
Vulnerable Information within Supply Chain
Child
Child
Information within Supply Chain
Child
Child
Role of Information within Supply Chain
Means of Sharing Information among Trading Partners

Figure 7.3: Emerged Themes on Information within Supply Chain

The participants' indicated that information plays an important role within their respective organisations and also within their respective trading networks. Hence, according to most of them, information has to be sufficiently acquired, stored, shared and well protected (either when static or being shared). Some of the roles of information that was emphasised by respondents include its role in being able to enable and enhance forecasting, decision making and trend analysis, which subsequently helps in achieving competitive advantage. The means through which information is acquired and shared, as stated by the participants, was also discovered from the analysed data. It was discovered that information is often acquired and shared among trading partners through two main means, shown in Figure 7.4. The electronic means of information sharing were identified to majorly be through fax, email, and the Electronic Data Interchange (EDI) system, which some respondents likened to using a Web portal for sharing information.

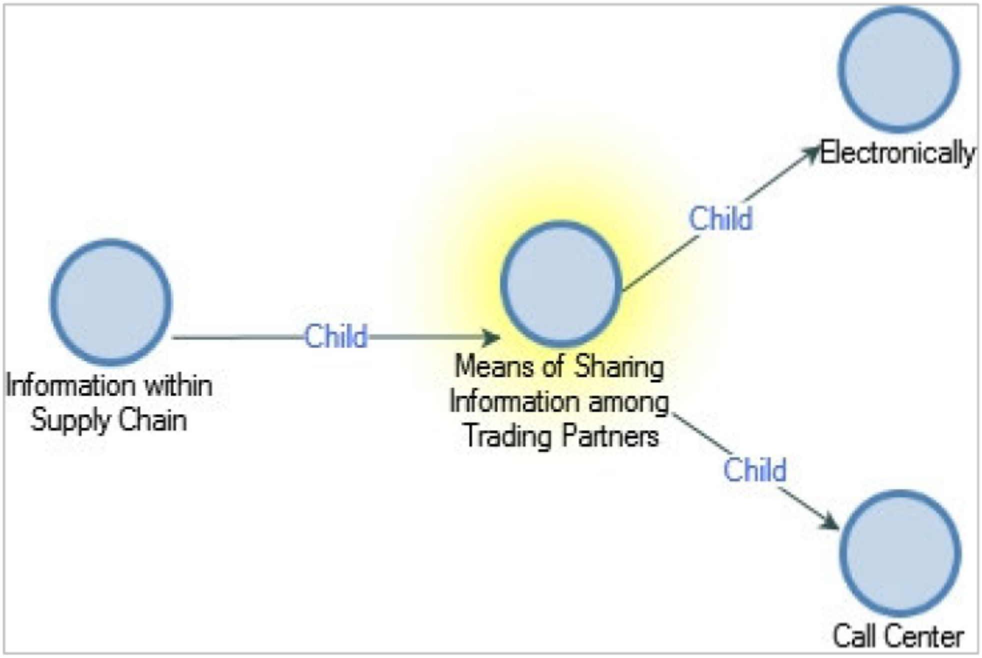

Information within Supply Chain
Child
Means of Sharing Information among Trading Partners
Child
Electronically
Child
Call Center

Figure 7.3.1: Emerged Themes on Means of Sharing Information

The other sub-themes that emerged under this theme, as shown in Figure 7.3, are the impact of information sharing among trading partners, and the vulnerable information within supply chains. The vulnerable information was identified to be critical information that is often acquired, used and shared within a supply chain, so as to optimise the processes and operations within the supply chain. These information are considered critical and vulnerable because they are key to the competitiveness of organisations and their supply chain network. These information include the pricing information, internal process information, client and users' information and the production planning information (e.g. forecast information, demand information, order information etc.). The impact of sharing information, as identified from the analysed data, are enormous, however, three broad categories emerged under this sub-theme. These categories are that the sharing of information helps in optimising the supply chain processes, in enhancing relationships and collaboration between trading partners, and also, in enabling the determination of pricing and production planning decisions.

7.3.2 Information Systems within Supply Chains

In understanding how information can be effectively and efficiently acquired, processed, stored and shared within the supply chain, respondents were interviewed about the role of information system within their organisation and also, in enhancing the processes between their respective organisations and their trading network. As shown in Figure 7.5, two main categories emerged from respondents' responses.

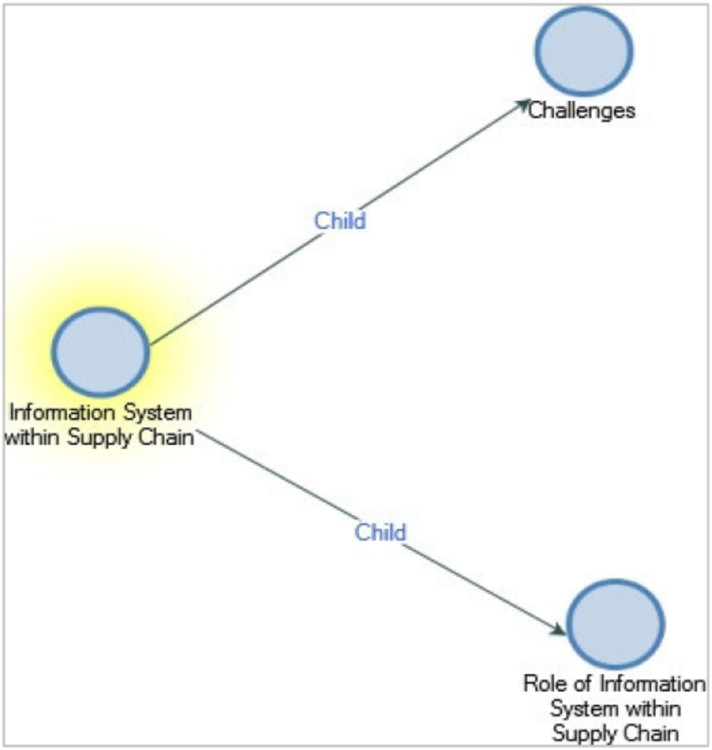

Challenges
Child
Information System within Supply Chain
Child
Role of Information System within Supply Chain

Figure 7.4: Emerged Themes on Information System within Supply Chain

The role of information system was identified to be important in the integration of the information that is shared among organisations. Other key and functional role that information system was identified to be helping organisations achieve include, process integration, decision making, information acquisition and sharing and data mining, especially for the purpose of forecasting and prediction. Different challenges, which are discussed in the discussion chapter, were identified by respondents, as affecting the role of information systems in enhancing organisational processes. Out of these challenges, two were the most recurring from participants' responses, and they are, the under-utilisation of information system (after being installed within the business) and the lack of adequate skills and expertise to guide in the proper installation and full optimisation of information system (mostly, before installation). The two, were, however, identified by some respondents to be related.

7.3.3 Vulnerabilities to Information within Supply Chains

When participants were asked about the security challenges that information and information systems are exposed to, one of the theme that emerged from their responses (transcribed interviews) was the vulnerability of information and information systems within supply chains to different threats and risks. Two main categories were identified from participants' responses with regards to the vulnerability of information and the information systems within supply chains. These categories are, the causes of information and information systems' vulnerabilities and the effect of these vulnerabilities on the overall supply chain processes and operations. From the causes of vulnerability within supply chains, as shown in Figure 7.5-A, the most prominent (i.e. with the most coded references) from the transcribed data are the lack of education, training and awareness of employees and the lack (or manipulation) of controls (e.g. policies). These were identified to, in some instances, lead to negligence among employees. Also, as shown in Figure 7.5-B, the most challenging and often costly effect of the vulnerabilities to supply chain information and information systems is the exposure and accessibility of trading partners information, information system and network to malicious individuals and programs. The other dominant effects that emerged were denial of service and the exposure to organisations to fraudulent activities, which might not be easily detected.

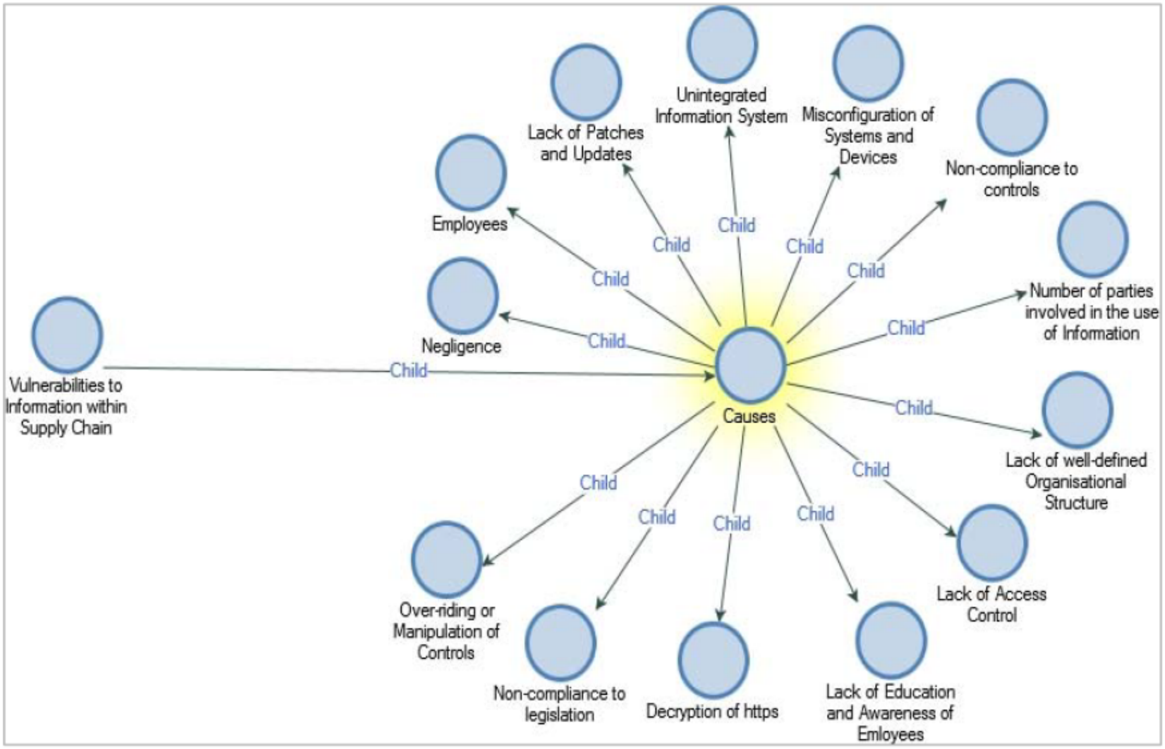

Vulnerabilities to Information within Supply Chain
Child
Causes
Child
Employees
Child
Lack of Patches and Updates
Child
Unintegrated Information System
Child
Misconfiguration of Systems and Devices
Child
Non-compliance to controls
Child
Number of parties involved in the use of Information
Child
Lack of well-defined Organisational Structure
Child
Lack of Access Control
Child
Lack of Education and Awareness of Emloyees
Child
Decryption of https
Child
Non-compliance to legislation
Child
Over-riding or Manipulation of Controls
Child
Negligence

Figure 7.5-A: Emerged Themes on Causes of Vulnerability within Supply Chain

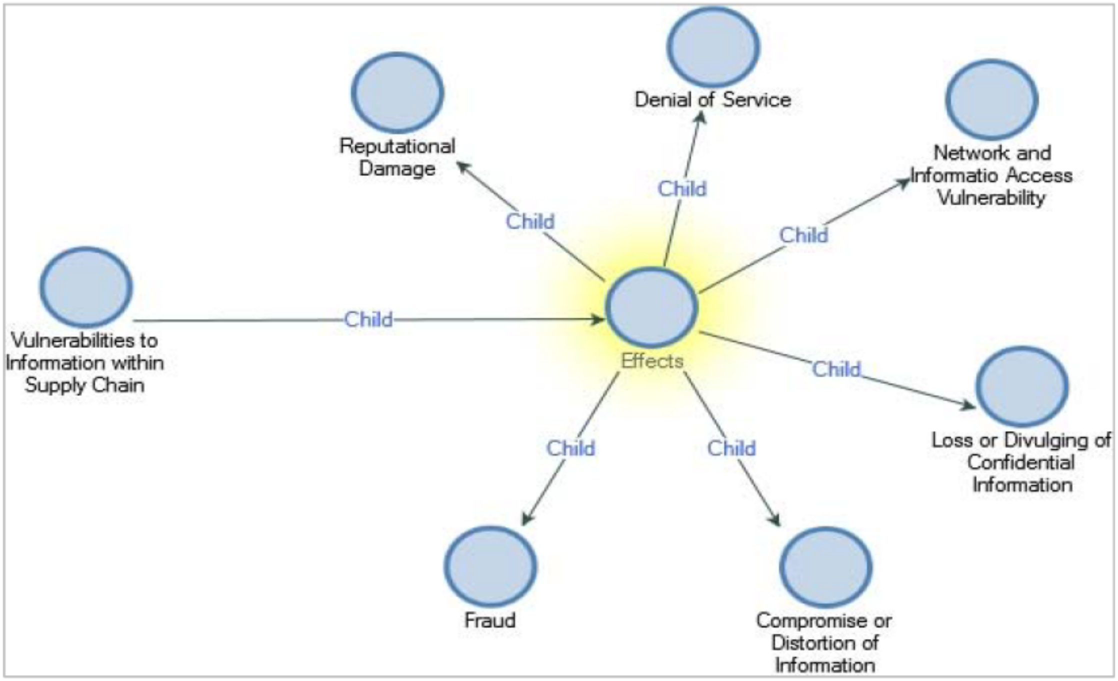

Denial of Service
Reputational Damage
Network and Informatio Access Vulnerability
Child
Child
Child
Vulnerabilities to Information within Supply Chain
Child
Effects
Child
Loss or Divulging of Confidential Information
Child
Child
Fraud
Compromise or Distortion of Information

Figure 7.5-B: Emerged Themes on Effects of Vulnerability within Supply Chain

7.3.4 Information Security Threats within Supply Chain

Participants were asked about the challenges and threats to information within the supply chain. Based on the analysis of the respondents' transcribed interviews, five main categories, shown in Figure 7.6, were identified. Each of these categories represents a significant threat to information and information systems within supply chains, and subsequently, to the overall processes and operation of the supply chain network. Out of the five, employees, sometimes referred to as insider, was the dominant and frequently mentioned by respondents as the most challenging threat to supply chains, just like to any organisation. Social engineering attacks such as phishing, vishing and pharming, were the next dominant threat and challenge to trading partners. It was identified in the analysis that social engineering attacks are being made possible to the perpetrators, by employees within the organisation. Thus, making employees, still the vulnerable link into organisations' network and information.

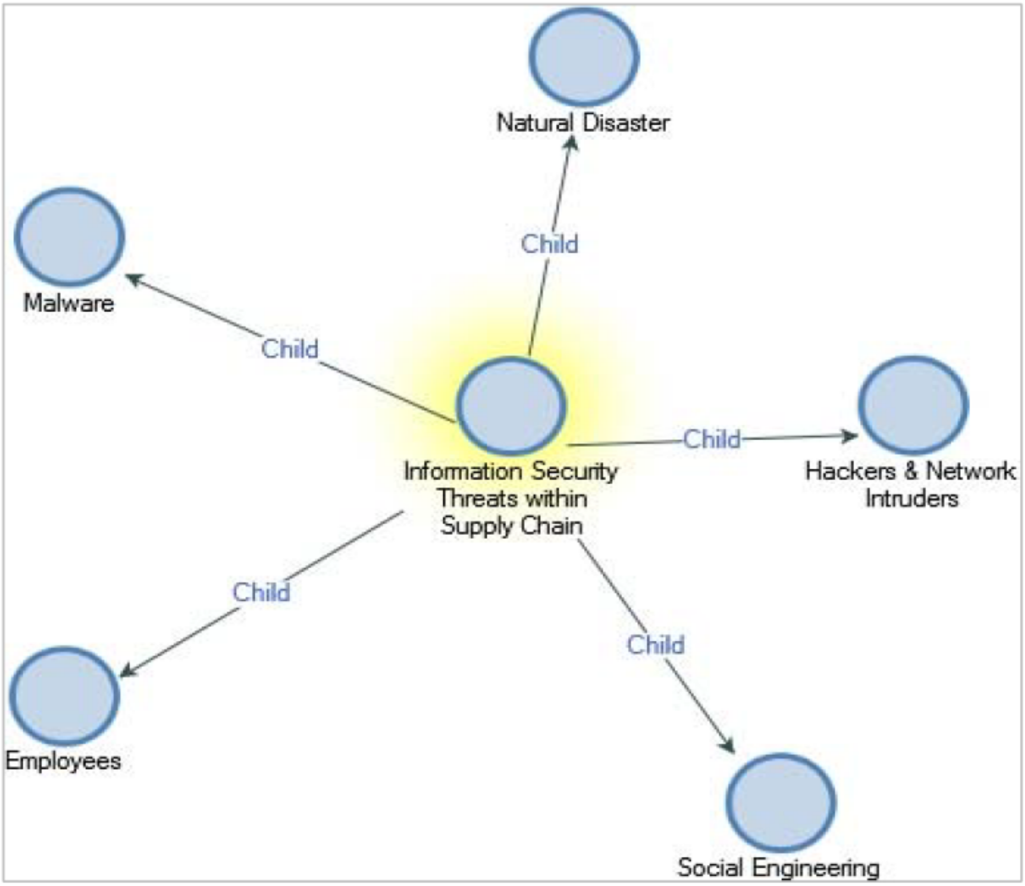

Natural Disaster
Child
Malware
Child
Information Security Threats within Supply Chain
Child
Hackers & Network Intruders
Child
Employees
Child
Social Engineering

Figure 7.6: Emerged Themes on Information Security Threats within Supply Chain

7.3.5 Managing Information Security Challenges within Supply Chain

Among all the themes and their respective sub-themes that emerged in this study, this theme and its sub-themes, had the highest coded references from the sources (transcribed interviews) used to generate nodes and sub-nodes in the NVivo software. Responses to the interview questions with regards to the means of managing the vulnerabilities, threats and risks to supply chain information and information systems yielded three main sub-themes, which are shown in Figure 7.7-A. Out of these three sub-themes, the implementation of controls was the most mentioned by respondents, as the most effective means of managing information security challenges. Over 90% of the responses that were related and coded under this theme fell into the category of the implementation of either technical or non-technical control, as effective means of managing the vulnerabilities, threats and risks to supply chains' information and information systems. The identified technical and non-technical controls, from participants' responses, are presented in Figure 7.7-A and 7.7-B, respectively.

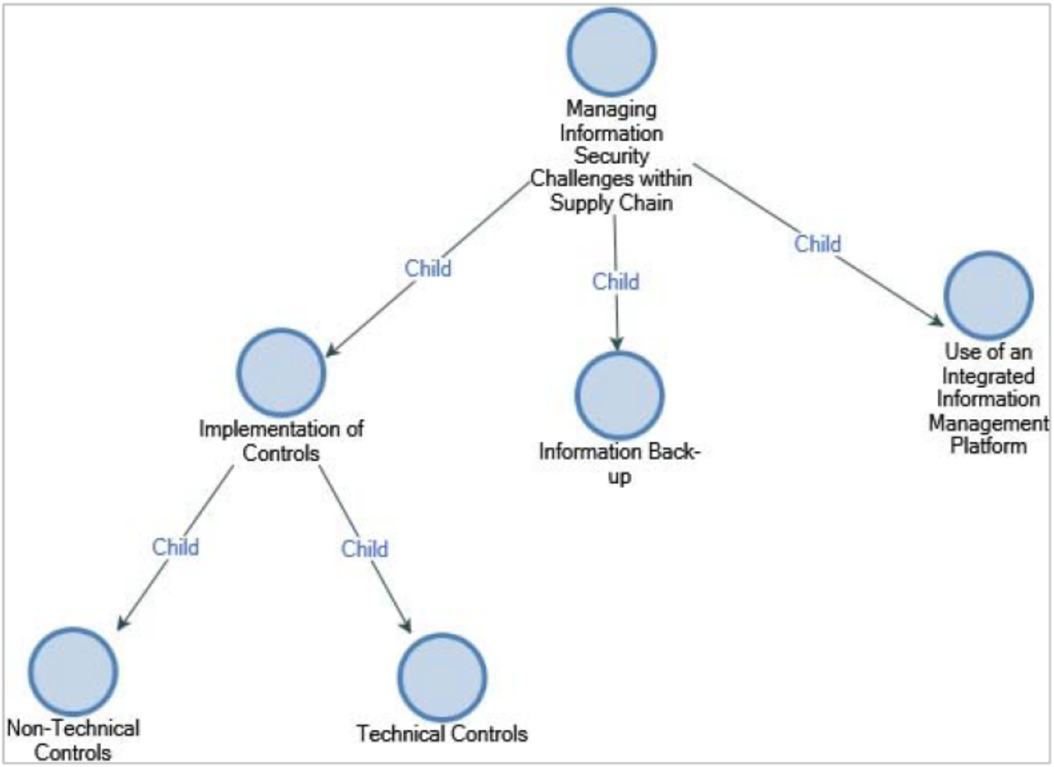

Managing Information Security Challenges within Supply Chain
Child
Child
Child
Implementation of Controls
Information Back-up
Use of an Integrated Information Management Platform
Child
Child
Non-Technical Controls
Technical Controls

Figure 7.7: Emerged Themes on Managing Information Security Challenges within Supply Chain

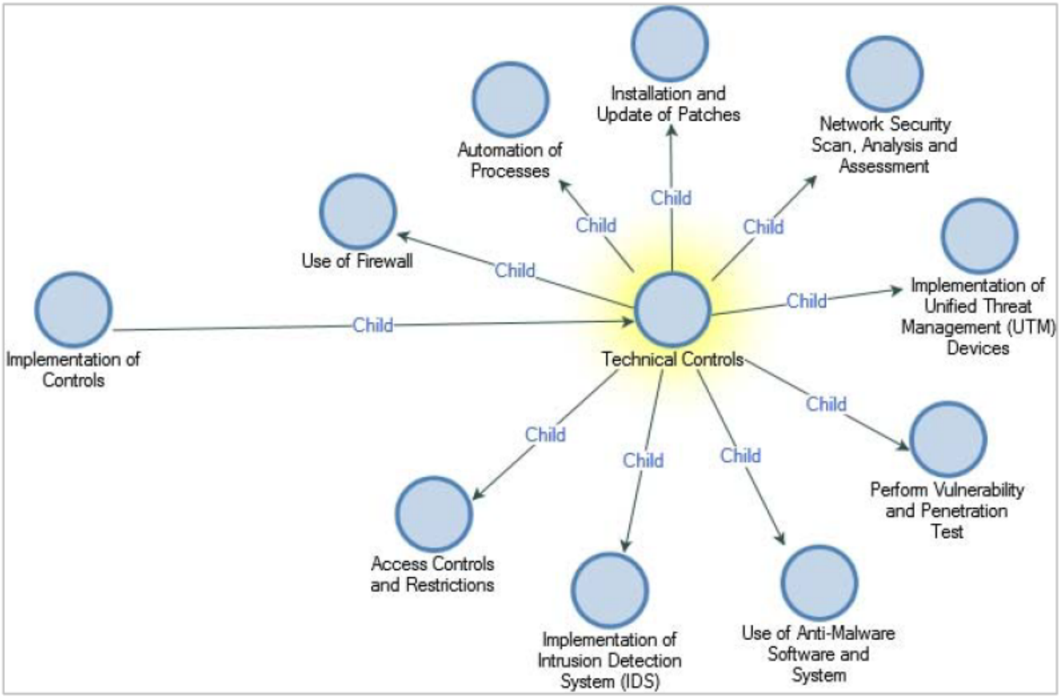

Installation and Update of Patches
Automation of Processes
Network Security Scan, Analysis and Assessment
Use of Firewall
Child
Child
Child
Child
Implementation of Unified Threat Management (UTM) Devices
Implementation of Controls
Child
Child
Technical Controls
Child
Child
Child
Child
Perform Vulnerability and Penetration Test
Access Controls and Restrictions
Implementation of Intrusion Detection System (IDS)
Use of Anti-Malware Software and System

Figure 7.7-A: Emerged Themes on Technical Controls for Managing Information Security Challenges

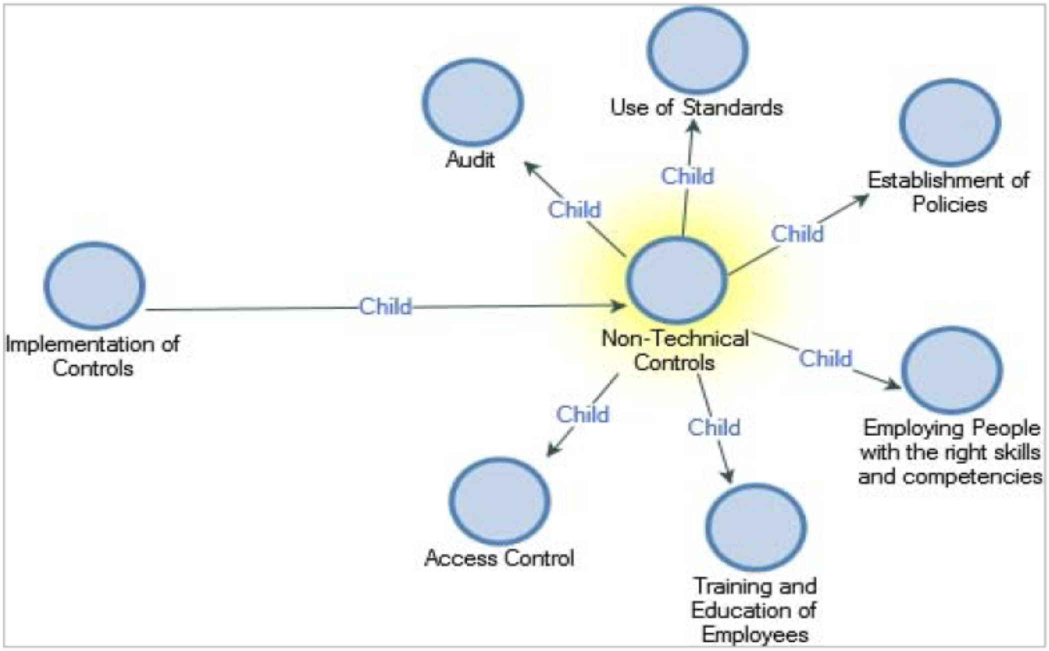

Use of Standards
Audit
Establishment of Policies
Child
Child
Child
Child
Implementation of Controls
Non-Technical Controls
Child
Child
Child
Employing People with the right skills and competencies
Access Control
Training and Education of Employees

Figure 7.7-B: Emerged Themes on Non-Technical Controls for Managing Information Security Challenges

From among the technical controls spoken about by participants, access control was the most talked about. The discussion around it includes the segregation or partitioning of employees' access to organisations' information and infrastructure, the provision of authentication mechanisms before gaining access to information and network, etc. The other prominent technical controls that were also frequently spoken about were the analysis, assessment and scan of organisation network. The discussion around the analysis, assessment and scan of organisation network include performing log analysis that helps in conducting trend analysis. The installation and update of patches, the performance of vulnerability and penetration testing and the use of anti-malware software, were also recurring in the responses of participants, as technical controls that can help in managing information security challenges.

From among the non-technical controls spoken about by participants, policies and the training and education of employees were most prominent. After these two, the other prominent non-technical controls were the establishment of physical access control mechanism and the continuous audit of employees and the organisation's processes. Employing the right people with the right skills, and the use of industry standards was also identified as being useful in managing information security challenges.

7.3.6 Ensuring Information Assurance within Supply Chain

Since the study is based on information security and assurance, participants were asked during the interviews to identify and explain how they think or know that assurance can be provided on the information being shared within trading partners, and also, on the information systems being used to share such information. As seen in Figure 7.8, eight themes (i.e. sub-themes) emerged, during the analysis process, as measures and practices that can help in providing security and assurance on the information within any trading network. All these measures and practices were considered and emphasised, in one way or the other, by respondents, as not only being important to the security and assurance of information, but also to the management of employees and the infrastructure within an organisation and between the organisation and its trading partners.

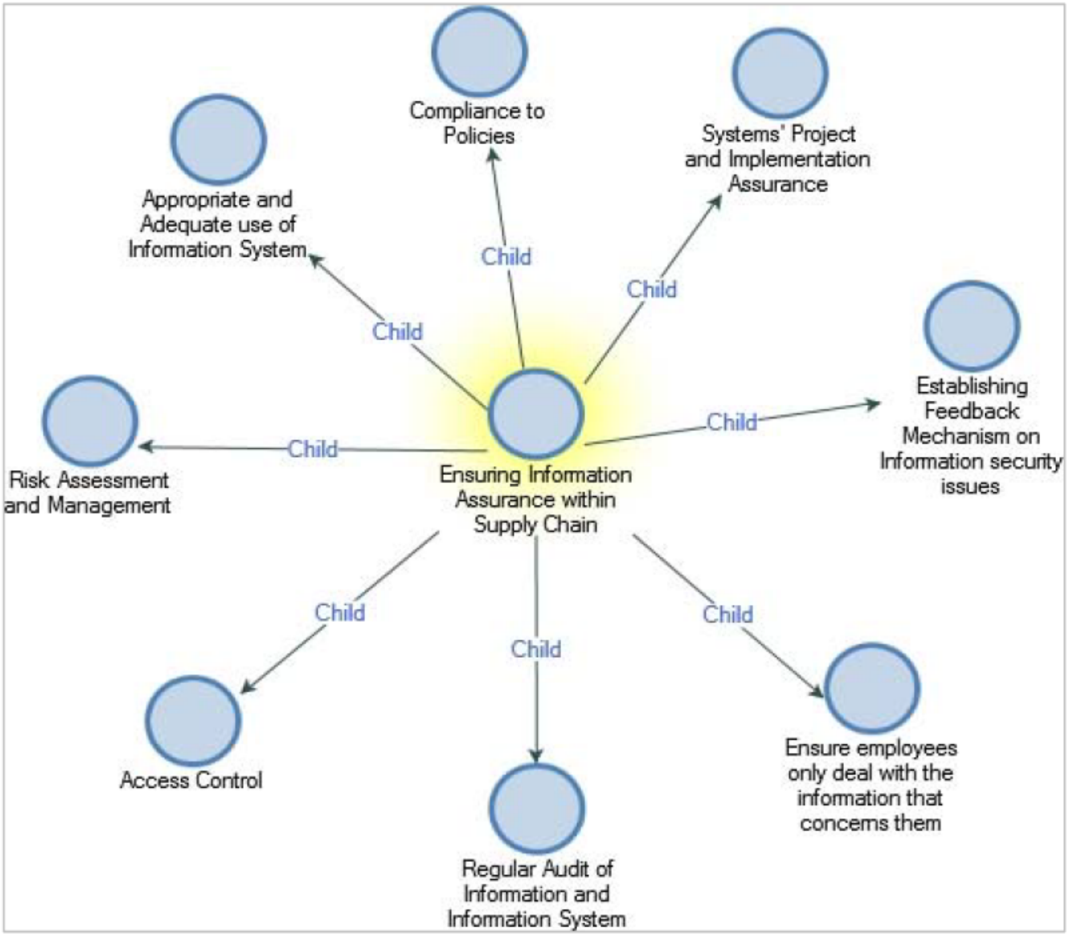

Compliance to Policies
Systems' Project and Implementation Assurance
Appropriate and Adequate use of Information System
Child
Child
Child
Establishing Feedback Mechanism on Information security issues
Child
Child
Risk Assessment and Management
Ensuring Information Assurance within Supply Chain
Child
Child
Child
Access Control
Ensure employees only deal with the information that concerns them
Regular Audit of Information and Information System

Figure 7.8: Emerged Themes on means of Ensuring Information Assurance within Supply Chain

7.4 Additional Themes

Three additional themes emerged during the data analysis process. These themes were also captured as nodes into the NVivo software. They were, however, not represented in the chart generated by the NVivo software, as seen in Figure 7.2. This could be as a result of their low number of coding references. The discussion around the relevance of these themes to this study's objectives is presented in the discussion chapter (chapter 8). These additional themes are presented in Figures 7.9, 7.10 and 7.11 respectively.

7.4.1 Relevance of Supply Chain Structure

The importance of having an efficient structure within an organisation and between the organisation and its trading partners was highlighted by respondents. The analysis of data, as shown in Figure 7.9, shows that the structure within the trading network is a determinant of how agile the functions and strategies within the network can be.

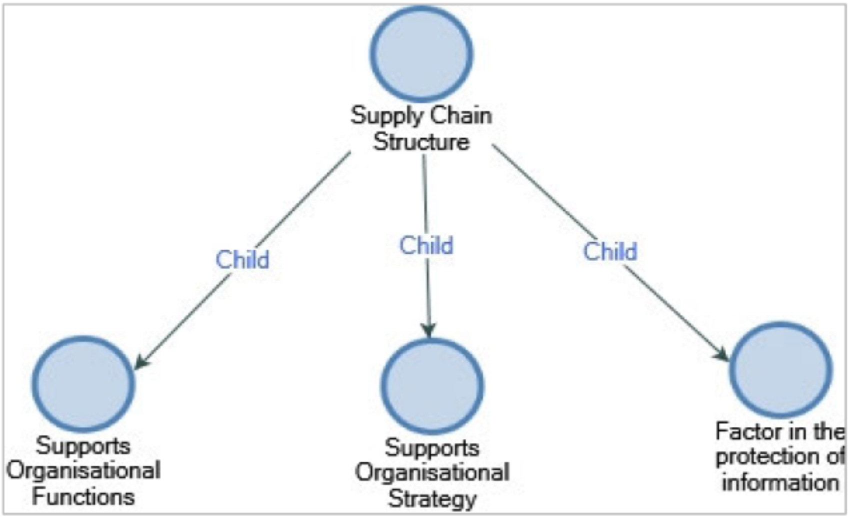

Supply Chain Structure
Child
Child
Child
Supports Organisational Functions
Supports Organisational Strategy
Factor in the protection of information

Figure 7.9: Relevance of Supply Chain Structure

7.4.2 Managing Supply Chain Processes

About 95% of the participants, irrespective of their organisational category (i.e. SCLO and ITCO), identified that one of the most important components of their business operation is the processes involved in the fulfilling of their organisational goals. Hence, it was well stated (i.e. frequency wise) that the processes within the organisation and between the organisation and its trading partners must be continuously and adequately managed. As seen in Figure 7.10, it emerged that the processes within trading network should be audited on a continuous basis.

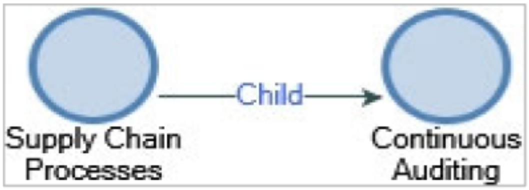


Figure 7.10: Managing Supply Chain Processes

7.4.3 IT Portfolio within Supply Chains

A common perspective of respondents, especially those in the IT units or involved extensively with IT in the SCLO category, and those from the ITCO category, was that the role of IT managers should be elevated to a decision making role. Hence, where and if necessary, a portfolio for the Chief Information Officer (CIO) should be created, and the occupant of such office should be skilled in IT and also be made to sit in board meetings, so as to tender and facilitate decisions regarding information systems and technology. It was also stated, as seen in Figure 7.11, that the role and responsibility of IT managers should be fully integrated into the structures and processes that exist within organisations and their trading network.

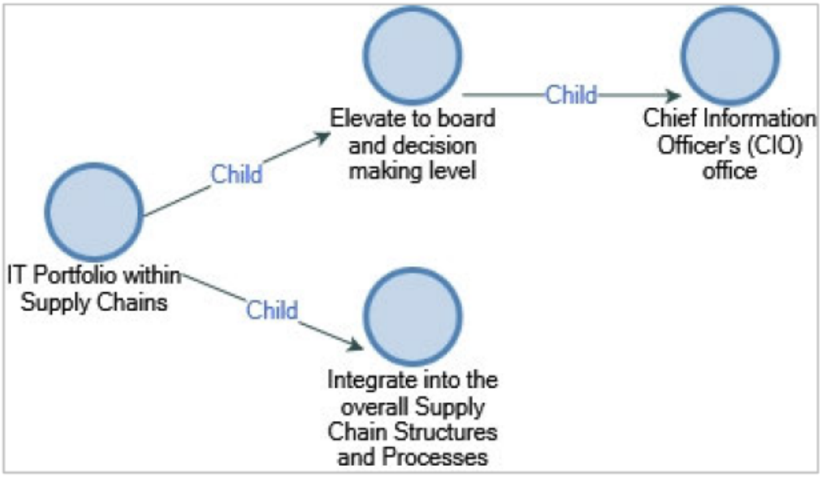

Elevate to board and decision making level
Child
Chief Information Officer's (CIO) office
Child
IT Portfolio within Supply Chains
Child
Integrate into the overall Supply Chain Structures and Processes

Figure 7.11: IT Portfolio within Supply Chains

7.5 Link between Themes and Main Research Questions

According to Ryan (2006), the analysis conducted in any research study should show or establish the relationship between the findings of the analysed data and the research questions of the study in which the data was collected. The Nvivo software was used to classify themes into nodes that are related to the various research questions. The research questions are presented below. However, the below research questions are the main questions. The comprehensive research questions, as outlined in the interview schedule can be found in Appendix B. The research questions are:

- What is the role of information and information systems within supply chains?
- How does sharing information impact on the supply chains' structures and processes?
- How does information systems affect the sharing of information within supply chains?
- What are the security challenges faced by information systems and information, as it moves through the supply chain?

- How are information assurance objectives (availability, integrity, authentication, confidentiality, and non-repudiation) ensured on information and information systems within the supply chain?
- How is information assurance provision for protection, detection, reaction or restoration incorporated into the supply chain structures and processes?
- How is information assurance facilitating a smooth supply chain process and an efficient and effective supply chain structure?

The link between the themes that emerged during the analysis process and the research questions is presented below.

Themes	**Research Questions (RQ)**	**Remark**
Information within Supply Chain	*What is the role of information within supply chains?* *How does sharing information impact on the supply chains' structures and processes?*	As shown in Figure 7.3, the impact of sharing information emerged in this theme
Information System within Supply Chain	*What is the role of information systems within supply chains?* *How do information systems affect the sharing of information within supply chains?*	As shown in Figure 7.4, the role and effect of using information system to share information was identified by the study's respondents
Vulnerabilities to Information within Supply Chain	*What are the security challenges faced by information systems and information, as it moves through the supply chain?*	In response to this RQ, respondent also identified the vulnerabilities that information and information systems are often exposed to

Themes	**Research Questions (RQ)**	**Remark**
Information Security Threats within Supply Chain	*What are the security challenges faced by information systems and information, as it moves through the supply chain?*	The major threats to information, as seen in Figure 7.6, emerged as themes
Managing Information Security Challenges within Supply Chain	*How are information assurance objectives (availability, integrity, authentication, confidentiality, and non-repudiation) ensured on information and information systems within the supply chain?* *How is information assurance provision for protection, detection, reaction or restoration incorporated into the supply chain structures and processes?*	The emerged themes, shown in Figure 7.7, and the respondents' discussion around these themes, helped in understanding these research questions
Ensuring Information Assurance within Supply Chain	*How are information assurance objectives (availability, integrity, authentication, confidentiality, and non-repudiation) ensured within the supply chain?*	The emerged themes, shown in Figure 7.8, and the respondents' discussion around these themes, helped in understanding these research questions

Themes	Research Questions (RQ)	Remark
	How is information assurance provision for protection, detection, reaction or restoration incorporated into the supply chain structures and processes?	
	How is information assurance facilitating a smooth supply chain process and an efficient and effective supply chain structure?	General responses from respondents provided an understanding of this RQ. The responses are presented in the discussion chapter (chapter 8)

Table 7.2: Link between Themes and Main Research Questions

7.6 Conclusion

The experience and exposure of the participants in this study made possible, conversational interview sessions between the researcher and the participants. Interviews were transcribed and the transcribed interview responses were coded into NVivo software as nodes. The nodes represent the different themes that emerged from the transcribed interviews. Six main themes emerged in this study. These themes helped in addressing the research questions of the study. In this chapter, the themes were presented, and the link between the themes and the research questions was also presented. The next chapter presents the discussion of the relevance of these themes to the objectives of this study.

CHAPTER 8: DISCUSSION

8.1 Introduction

The outcome of a research study should establish some form of relationship between the findings of the analysed data and the objectives that led to the study being undertaken. Similarly, according to Trifonas (2009), the outcome and conclusion derived from the analysis of a given set of data should reflect the perspective of the study's participants, and should also represent the actual behaviour of the phenomenon being studied. In this chapter, the result (i.e. outcome) of the study is presented.

In the presentation of the result, supporting evidence in the form of quotations from the raw data (i.e. transcribed data) and also from the literature was used to further explain and justify the findings of this study (Lichtman, 2013). However, in cases where interview respondents have asked for their actual words to be kept confidential, quotations from such transcribed interviews were not used (Ryan, 2006). Also, the names of the participants in this study have been omitted, because they all requested that their names be kept confidential. The layout of this chapter is presented in Figure 8.1.

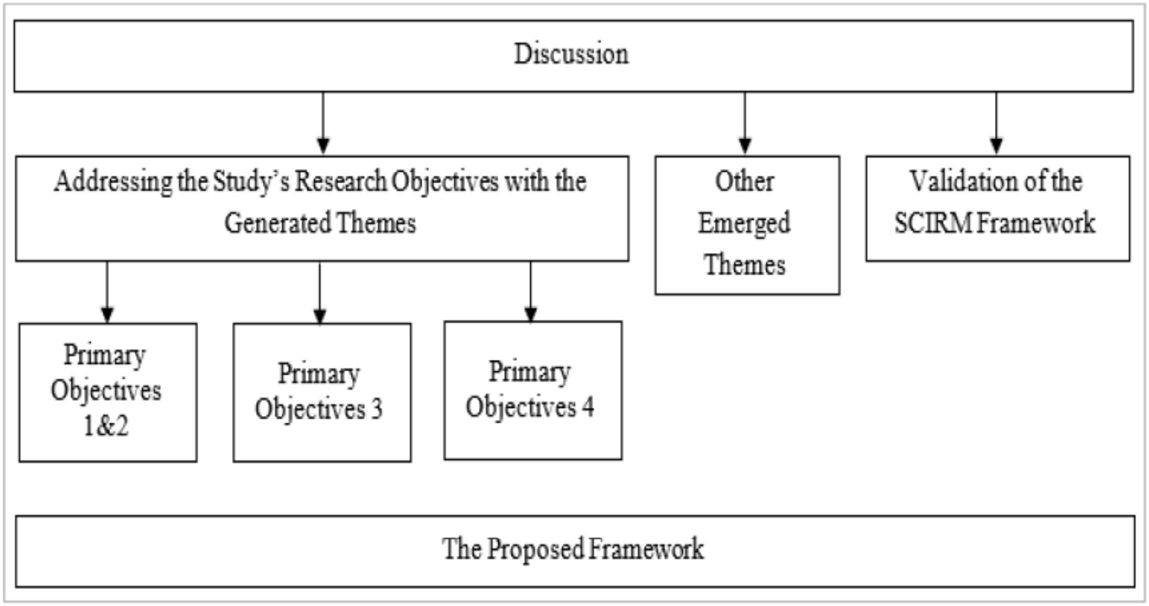


Figure 8.1: Layout of the Chapter

8.2 Addressing the Study's Research Objectives with the Generated Themes

In the presentation and discussion of the result of a study, the researcher is required to show the relationship between the study's objectives and the findings from the analysed data. This section presents the relationship between the study's objectives and the generated themes and their respective sub-themes. The section also presents, where applicable, the relationship between different themes and different sub-themes. This study's main and primary objectives, as outlined in section 1.4, are listed below.

Study's Main Objective

The main objective of the study is:

- To propose an information assurance model that can enable organisations to protect and sustain their respective information within the supply chain structures, and that can also enable them to minimise or prevent the risks that information within the supply chain processes could be exposed to.

To accomplish the main objective, the thesis has four primary objectives which are:

i. To understand the role of information and information systems within supply chains.

ii. To understand how information is shared, and also, the impact of sharing information within the various processes and structures of the different components of supply chains.

iii. To identify and understand the issues and challenges surrounding the security of information systems, and also, information, as it moves through the various supply chain structures and processes.

iv. To understand information assurance as a concept and evaluate its objectives, and also identify how it can facilitate a smooth supply chain process and an efficient and effective supply chain structure.

8.2.1 Primary Objectives 1 & 2

Objective 1: To understand the role of information and information systems within supply chains

Objective 2: To understand how information is shared, and also, the impact of sharing information within the various processes and structures of the different components of supply chains.

Two themes that were generated from the transcribed interviews, and the discussion around these themes, were considered relevant in addressing the first two primary objectives of this study. These themes are:

i. Information within supply chain
ii. Information System within supply chain

These themes, their respective sub-themes, and the discussion around them were centred on the focal points of the first two primary objectives of this study. Hence, both objectives are combined in this section. The discussion of the findings of this study, with regards to these objectives, in relation to the two identified relevant themes and their sub-themes, are presented below.

8.2.1.1 Information within Supply chain

The value and importance of information were emphasised by over 90% of the overall participants in this study. According to one of the participants in this study, "*Information is the most important thing to any organisation and the organisation's trading partners*" (PI-10). This is because it is an important determinant of the effectiveness and efficiency of the processes within an organisation and between the organisation and its trading partners. It is also important in facilitating the transition of resources between trading partners. Hence, according to the same participant (PI-10), losing information is the worst thing that can happen to any organisation. Sharing the same opinion, Miller & Drake (2016) also showed in their study that the loss of information can be a source of any trading network's exposure to threats and risks.

The finding of this study shows that the concern of organisations, with regards to information, includes maintaining the integrity and availability of information. This concern, according to one of the respondents also include, "*ensuring that the information being used within the supply chain network is valid and accessible*" (PS-9). Another participant (i.e. PI-1), in his response, indicated that if information loses its integrity, it becomes invalid and consequently, such information is difficult to work or make decisions with. The analysis of transcribed interviews generated different findings, in the form of themes (i.e. sub-themes), with regards to information within the supply chain. These findings are presented below:

Role of Information within Supply Chain

The findings of this study show that information is an important requirement in the decision making capability of organisations. This is also alluded to in the study of Mitchell & Kovach (2016), where it was stated that information enhances the decision making of the different organisations within a trading network. Similarly, according to one of the study's participant, "*information is important in interpreting and making transactional decisions that can be used for improving the overall processes with the supply chain*" (PS-4). The decision making capability of information was also mentioned in the study of Qrunfleh & Tarafdar (2013), as being important in enhancing collaborative-relationships between organisations. Some of this study's participants, however, stated that the geographical dispersion of some of their trading partners often affects their organisation's decision-making capabilities.

Another finding of this study with regards to the role of information is that information plays an important role in trend analysis. As explained by some of the respondents, with trend analysis, the organisation is able to predict what could happen to their product in the future, based on the historical and current information at their disposal. Respondents also explained that with trend analysis, they are able to determine how their product is faring in the market. Similar to trend analysis, forecasting was also identified by respondents as an important role that information is facilitating within their business and also within their trading network. Similar to this finding, is what was stated in the study of Yu *et al.* (2010), that the availability of information ensures accurate planning, forecasting and production.

According to one of the respondents, "*decision making in the business is dependent on the forecast that is made from the information within the business*" (PS-9). This is because, with forecasts such as demand and sales forecast, organisations are able to make decisions regarding what to produce at a particular time, and at what quantity. To enhance the ability of organisations to forecast, while at the same time encouraging collaboration, an initiative called Collaborative Planning, Forecasting and Replenishment (CPFR) was developed. Under this initiative, trading partners are expected to jointly develop an information sharing mechanism, and also, a forecast process, that is mutually agreeable to all parties. According to Syntetos *et al.* (2016), however, the relationship type among trading partners, is a potential differentiator that enhances or disrupts the forecast accuracy within a trading network.

With regards to the role of information within supply chain, it was also found through the analysis of the transcribed interview responses that one of the most important uses of information is for providing organisations with a competitive advantage. As was explained by one of the respondents that "*information is used for competitive advantage, for example, in terms of pricing. This is because it enables the determination of pricing among trading partners*" (PS-2). The use of information for competitive advantage was also emphasised in the study of Piderit *et al.* (2011), where they explained that for the supply chain to remain competitive, the organisations within the supply chain must be willing to share information.

Means of Sharing Information within Supply Chain

Responses from the study's participants with regards to information show that for information to be relevant and useful within the supply chain, it must be shared among the organisations within the supply chain network. One of the directors interviewed in this study suggested that "*organisations should have a separate information structure that deals with receiving and sharing of information up onto the use of information*" (PI-5). Similarly, in the study of Gunasekaran *et al.* (2015), it was shown that for information to be relevant in making the supply chain resilient and agile, it must be shared in a structured manner among the trading partners.

Respondents in this study identified two means through which information is often shared. The first being through electronic means and the second being through the call centre. In the case of the call centre, as explained by one of the respondents, "*calls are made to the call centre and the call centre representative captures such information to the system*" (PS-1). While in the case of electronic means, information is shared through three major means, which are Fax, Email and the Electronic Data Interchange (EDI) System, which was likened, and in some cases considered by respondents as using a Web portal for sharing information. With regards to call centre being used for information sharing, one of the interviewed managers disapproves of it and believes that the "*call centre should be better used for reception management and not for the capturing or sharing information*" (PS-1).

Out of these three means of sharing information, the EDI system according to one of the respondent "*is the most efficient, effective and reliable compared to the manual/call centre system*" (PS-5). This system was generally considered by respondents as the most secure way of sharing information. Similar to this opinion, Macharia & Ismail (2015) stated in their study that the EDI system, apart from being reliable, also helps trading partners to reduce the time and effort required to share information and perform transactions. Another participant in this study, while discussing the operation of the EDI system, explained that "*in some instance e.g. for pricing, customers are allowed, through an interface, to access an electronic information sharing system, hence a common platform in the form of a Web portal is made available for trading partners to be able to share information*" (PS-5).

Email as a means of information sharing was also frequent in the word count of respondents. In fact, one of the ITCO directors (PI-5) that was interviewed emphasised that information sharing via email should be considered and implemented as a policy, and if there are other existing means of sharing information among the trading partners, then the policy should state that emails should be used to complement and document the information sharing process. His reason was that it is far easier to trace and track email records. Although, according to Nagamalai, Dhinakaran, Ozcan, Okatan, & Lee (2014), email has emerged as one of the preferred means of intruding organisations' network and subsequently, organisations' information.

Impact of Information Sharing within Supply Chain

The prominent finding of this study with regards to the impact of information sharing is that information sharing impacts on the relationship and collaboration level among trading partners. This is as identified by one of the study's participants who stated that, "s*haring of* *information is an important requirement in supply chain relationships and collaboration*" (PS-4). In agreement with this view, Singh & Teng (2016) stated that establishing a collaborative relationship among trading partners is determined by how information is willingly shared among trading partners. They further stated that a collaborative relationship is also determined by the level of trust among trading partners. This (i.e. trust) has been found in the study of Fu *et al.* (2016), to also be influenced by the level at which credible and reliable information is shared among trading partners. Thus, it can be said that information sharing impacts on the relationship, collaboration and the trust level among trading partners.

Respondents also stated that sharing information enables decision making among trading partners. For example, one of the respondents (PS-2) stated that when information is shared, the decision regarding pricing can be adequately made among the trading partners. Although, the same respondent explained that a breach of an organisations information often affects the information shared with organisation's trading partners and subsequently, affects decision making within the overall trading network. Optimisation of processes was also another theme that emerged as an impact of information sharing within the supply chain. It was stated by one of the respondents that "*information, when shared, helps in optimising the purchasing, production and delivery processes within the organisation*" (PS-4). According to Singh & Teng (2016) as well, trading partners should reduce the challenges affecting information sharing and encourage each other towards the adequate sharing of information. This is so as to be able to effectively manage the processes within their supply chain network.

Vulnerable Information within Supply Chain

Organisations information are continuously and increasingly being exposed to different vulnerabilities, especially because, as mentioned by one of the respondents, "*there is a market for information, that is, for information to be sold*" (PI-2). The findings of this study show that organisational information needs to be protected because if they are not, the information becomes vulnerable to malicious individuals and programs. Some of the prominent information that was identified as being vulnerable, if adequate protection measures are not put in place, are:

Users' information: This information is always vulnerable, if not adequately protected. Interest in these type of information is mostly centred on being able to gain access to organisation's network and information, and also for financial purposes.

Internal process information: It was stated by one of the respondents that "*internal process information which includes the business process information, the codes and terminologies used within the business etc., are often of great interest to people who mean harm*" (PI-2).

Pricing information: This was identified by most of the SCLOs' respondents as being one of the most critical information within their business, and especially within any supply chain. It, for example, contains information about how much items are being sourced for, how much they are being supplied for etc. (PS-2). It is therefore considered a determinant of a supply chain's competitiveness. For this reason, it is one of the information that is often of interest and target to an organisation's competitors, making it a vulnerable information, if not sufficiently protected. One of the respondents explained that "*if an organisation is marking up at 10%, and their competitors get hold of such information, they could do a markup of 8% so as to beat the price*" (PI-9).

Production planning information: Different type of information such as order information, demand information, sales information, procurement information etc. where identified by almost all respondent in the SCLO category as being important for planning the organisation's production and overall activities. These type of information, if not well guarded, becomes vulnerable to possible exploitation by the organisation's competitors. The weakness of this type of information also exposes the organisation's trading partners to different risks, especially the risk of inadequate planning.

8.2.1.2 Information System within Supply chain

Information system was identified as being indispensable to the success story of any organisation. It was a common opinion among respondents that information systems are helpful in the processing of daily transactions and the management of daily operations and knowledge. Similarly, Lam *et al.* (2015), in their study pointed to the fact that information systems are increasing the visibility of the operations and processes within supply chains. They further stated that information systems are also facilitating the provision of accurate information to trading partners in real-time. One of the managers interviewed in this study also emphasised the importance and use of information systems in the provision and processing of real-time information. With regards to information system within supply chains, two major themes, which are presented below, emerged from the analysis of interviews.

Role of Information System within Supply Chain

The findings of this study show that information system plays a very crucial role in the capturing, use and management of information. One of the study's participant stated that "*if the information system is used appropriately and adequately, the possibility of information loss will be minimal*" (PS-1). Information loss, usually caused by the vulnerabilities and challenges to the information system, often affect every other aspect of the organisation's business, including the supply chain (PI-2). Some of these challenges are in some instance (e.g. procurement – purchase order), when the trading partners information systems are not integrated to allow for a common platform of information sharing (PS-1).

Information system serves as an integration tool for the transaction and workflow processes involved in a supply chain, and also, for process replication and management (PS-5). It also serves as an enabler (PI-3), as explained by some of the respondents that, "*it enables the provision of portals that facilitate information sharing*" (PI-9), and also "*enables the accessibility of information on a single platform by multiple partners*" (PS-2). Similar to this views, different authors in their work, also stated that the availability and accuracy of information are being significantly improved by leveraging on information systems. Although, authors such as Stefansson (2002); Fu and Zhu (2010) explained that the presence of the overhead cost associated with the acquisition of information system is continuously a challenge to its adoption and implementation. The findings of this study show that information system provides visibility of information and processes and is also a contributor to decision making among trading partners. This is as explained by one of the interviewed personnel that, information system "*helps in interpreting transaction details into meaningful information that can be used for decision making and improving the overall processes within the supply chain*" (PS-4).

Challenges of Information System within Supply Chain

"*When there are challenges to the information system, especially the types that cause weaknesses to the information system, information, by default, becomes vulnerable*" (PI-3). With regards to the challenges faced by organisations in the use of information systems, two major concerns were identified in the interview responses. The first being the under-utilisation of information system within the business. Some of the respondents explained that their organisation often tries to fit the information system into the organisational processes. This they identified, is often a challenge because, in the long run, the information system happens to be under-utilised, as most of its functionalities are not always used. One of the interviewed managers explained that to reduce the challenges to the adoption of information systems, the organisation should adapt their processes to the design of the information system they are adopting and implementing. The other concern raised by respondents with regards to the challenges to information system was the lack of adequate skilled personnel and expertise in the implementation and use of information systems. This is often a challenge, especially when there are issues with the use of such system. Some respondents explained the troubles they have had to go through in order to understand and comprehend the use of their respective information systems. Sufficient training and the gradual integration of information system into the organisational processes and structures was suggested by some respondent as a means of managing these challenge.

8.2.2 Primary Objective 3

To identify and understand the issues and challenges surrounding the security of information systems, and also, information, as it moves through the various supply chain structures and processes

Two themes that were generated from the transcribed interviews, and the discussion around these themes, were considered relevant in addressing this objective. These themes are:

i. Information Security Threats within Supply Chain
ii. Vulnerabilities to Information within Supply Chain

These themes, their respective sub-themes, and the discussion around them were centred on the focal points of this objective. The discussion of the findings of this study, with regards to this objective, in relation to the identified relevant themes and their sub-themes, are presented below.

8.2.2.1 Information Security Threats within Supply chain

The interview responses showed that participants and their respective organisations are constantly being faced with the challenges of threats to their information and information systems. According to one of the participants, these threats and the challenges they pose are on the rise, and this is as a result of organisations drive to establish or join a global market environment. According to Wolden *et al.* (2015), these market environments are causing supply chains and their resources (i.e. information, materials and fund) to become vulnerable to different threats. One of the interviewed participants explained that the fear of threats to information is mostly because "*the threats to information and information systems can be caused by different and multiple unexpected sources*" (PI-6). These threats are also, as identified in the literature, increasingly getting more sophisticated and also complicated to manage.

The analysis of transcribed interviews generated different findings (Figure 8.2) in the form of themes (i.e. sub-themes), with regards to information security threats within supply chains. These findings are presented below:

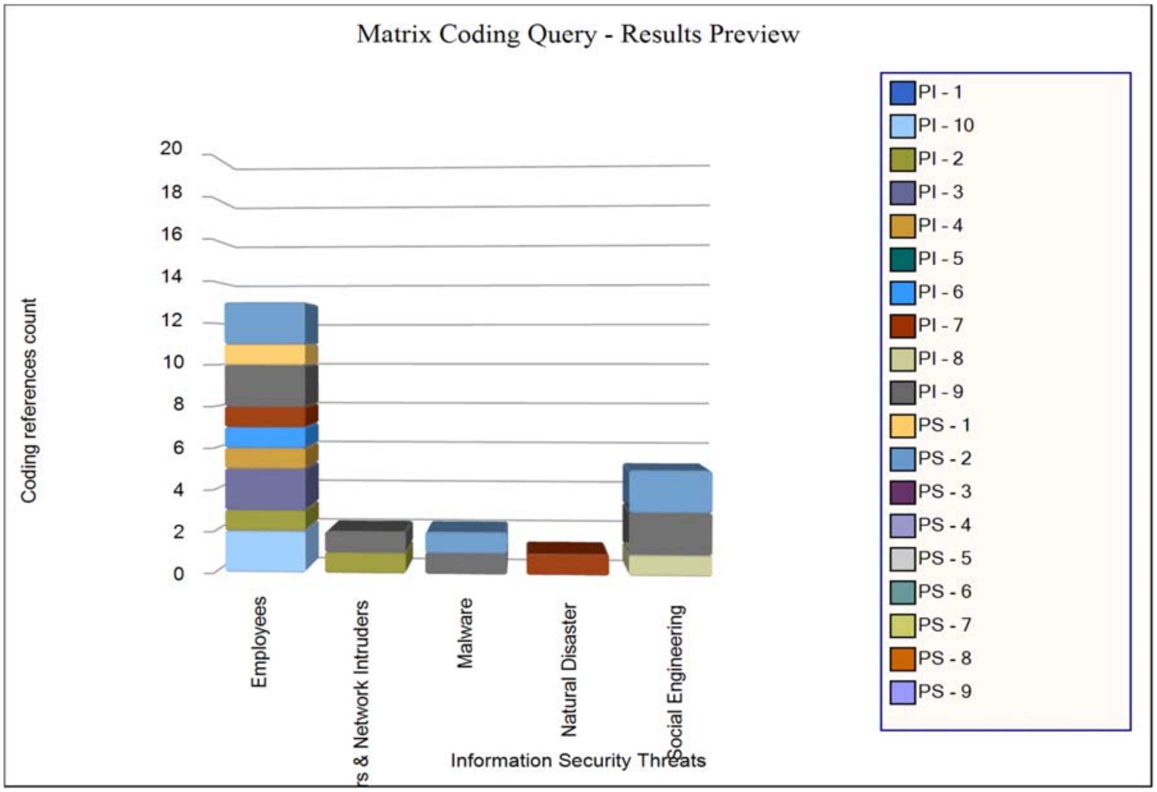


Figure 8.2: Majorly identified Threats (Extract from NVivo)

Employees

Employees, sometimes referred to as insiders, are by far the most mentioned by respondents, as shown in Figure 8.2, as being the most challenging threat to organisations' information and information systems. One of the information security consultants that was interviewed explained that "*organisations still often concentrate on the threats from outside when in reality, the majority and most common and feared threats are internal. This is because, internal employees know the organisational culture, processes and measures in place, and they can circumvent these culture, processes and measures*" (PI-3). He further stated that "*internal employees can take advantage of the relationship and trust level within the business and among employees to exploit the organisational information and processes*". Hence, as explained in the study of Ifinedo (2014), organisations that fail to pay attention to the individuals within their business environment, may fail to achieve success in their effort to combat security threats and attacks.

Crossler *et al.* (2013) and Sindhuja & Kunnathur (2015) explained in their studies that employees are the first line of defence in protecting information and information systems, but unfortunately, they are also the weakest link and consequently, a major threat to information security. Similar to this point of view, is what was pointed out by one of the security analysts, who stated that "*the security of information should start from the people/employees within the* *organisation. This is because the most devastating threats do not come from outside, but from inside*" (PI-9). In further agreement to the view that the security of information should start from the people/employees within the organisation and the organisations' trading network, Wolden *et al.* (2015), stated that organisations and the members of their trading network should implement measures and practices that are effective from within the organisation, and that can help manage the behaviour of employees, especially the behaviours that can cause harm to the organisation's information and information systems.

One of the major class of employees that can be a threat is the employee that no longer works for the organisation. This was also echoed by one of the participants who explained that "*employees that leave the organisation can be a threat to such organisation. This is because of their knowledge of how the organisation's security, culture and processes operate*" (PI-10). Although according to another participant, "*for a current, resigned or dismissed employee to become a threat to information, they must understand and know the vital information that can cause harm to the organisation – this, however, is not always the case*" (PI-9). The findings of this study show that it is a common practice that when an employee leaves the organisation, the privileges of such employee are revoked. The findings of this study, however, also shows that the practice is in some cases not carried out, even long after an employee has left the organisation. Hence, one of the participants explained that "*if a staff privileges are to be revoked, it should be done before informing the staff of such decisions. This is so as to prevent such staff from performing any form of sabotage with their privileges before they are taken away*" (PI-6). The participant further explained that this should also apply to employees leaving the organisation. That is, their privileges should be revoked before such employee leaves. At worst, should be done on the last day of work of such employee, that is, if the employee still has things to do up until their last day at work.

Hackers & Network Intruders

Respondents identified hackers and intruders as threats to their organisation and even to the organisations within their trading network. According to some of the respondents, hackers are in most cases also potential network intruders, hence, they (i.e. hackers) were also referred to as intruders by some of this study's participants. They are referred to as intruders because most of their activities are centred on being able to gain unauthorised access to organisation's network, so as to eventually gain access to the organisation and their trading partners' information and information systems. It was explained by one of the respondents that "*they (i.e. hackers) can use any information to breach an organisational network*" (PI-9). One of the respondents, however, indicated that "*hackers contribute to less than 10% of threats, but the damage they cause to any organisation and their supply chain network can be extremely severe*" (PI-2).

The findings of this study show that hackers are continuously finding ways to evade anti-virus technology. This was also pointed out in the study of Jajoo, Singh, & Nehra (2013). As found in the literature, they often utilise different techniques such as code obfuscation, packer and emulator detection etc. to evade their activities from being detected. Their ability to evade being detected and staying on a system or network within an organisation has made them an important threat to information and information systems. Zhang (2014) in his study also explained that they use the technique of routing packet traffic through a chain of host so as to be able to gain access to organisation's systems, without exposing themselves. They commit crimes such as web hacking, DoS and DDoS attacks, web defacement etc. by exploiting the vulnerabilities within the organisation.

Malware

Another form of threat that was identified in this study was malware. Different types of malware, such as viruses, worms, Trojan, bot, spyware etc. were mentioned by respondents. One of the respondents explained that "*most of the existing type of malware can be used to acquire sensitive information of an organisation*" (PI-6). This was also alluded to in the study of Nishat Faisal *et al.* (2007), where it was stated that most form of malware usually contains instructions that when executed, provides malicious programs that can affect the performance of information and information systems within supply chains, by acquiring sensitive information of the supply chain structures and processes.

One of the security analysts that was interviewed explained that "*malware can be targeted or non-targeted. Most non-targeted malware are often caused by ignorant users within the organisation*" (PI-9). Caballero *et al.* (2011) in their study explained that the targeted type of malware are usually customised for the information stealing of the target organisation or individual. Choo (2011) and Chauhan *et al.* (2013) also explained in their study that some customised information stealing malware often have a phishing-based keylogger component in them. This phishing-based keylogger is a program that is designed to monitor users' activities such as keystrokes, and to harvests login credentials, account numbers, etc. to a collection server.

One of the security analysts also explained that malware often "*comes into the organisation through USBs, emails (which are sometimes targeted) etc.*" (PI-9). In speaking about the means through which malware penetrate organisational network, Roy & Kundu (2012) and Bottazzi & Italiano (2015) stated that the increasing use of the Internet and some of the emerging technology concepts such as cloud computing, for supply chain operations, is also causing an increase in the proliferation of malware into organisations and their trading partners' network. These authors further explained that these technologies have also increased malware's potential as a threat to the operations of supply chains.

Social Engineering

The findings of this study show that social engineering attacks are on the rise. Respondents in this study explained that some of their employees have been victims of social engineering attacks such as phishing, vishing and pharming, and through which their personal and even some business information has been divulged. They also identified that the employees of some of the organisations within their trading network have also been victims, and their activities have affected the integrity of the network. It was explained by one of the respondents that "*organisations are seeing an increase in their help desk personnel receiving phone calls that are luring them into changing people's password and giving out confidential information of the organisation*" (PS-2). The respondent further explained a case they witnessed in their organisation, in which a caller, disguising to be calling from the organisation's Internet Service Provider (ISP) lured the front end personnel into divulging important information that included some organisational password.

Email spoofing and tailgating was also identified by respondents but emphasised mostly by one of the study's participants (PI-8) who believes that these are two forms of social engineering attacks that users seem to not pay so much attention to. The respondents believe that these are common social engineering means of defrauding people. With regards to social engineering increasingly becoming a means of defrauding people, Issac *et al.* (2014) also stated that social engineering attacks are increasingly being used to acquire privileged and private information from victims, so as to cause problems such as identity theft and financial fraud. According to one of the security analyst, "*organisational information on the social network can also be used against them*" (PI-9) in a social engineering attack, hence, he emphasised that organisations should be cautious of the kind of information they make available online.

Natural Events/Disasters

Natural disasters, as explained by some of the respondents, is a threat that nothing much can be done to prevent or stop, except that organisations make futuristic plans for it possible occurrence. One of the respondents explained that organisations should have an IT disaster recovery plan and processes in place, for such occurrences. This is because such plan and processes often help to deal with issues around IT systems during a disaster occurrence. This was also alluded to in the study of Ghannam (2017) where it was stated that IT disaster recovery plans are one of the most required contingency plans in the event of the occurrence of a disaster. It was, however, also noted in the same study that many organisations still do not have such plans in place or are rather hesitant in applying such plans before the occurrence of a disaster.

The findings of this study show that natural disasters do not only directly impact or disrupt supply chain information, their after effects can also have a devastating effect on the information and operations of the overall trading network. This can be seen in earthquake and tsunami which happened in Japan in 2011 and the flooding in Thailand which happened in the same year, in which power outage, road closure, information loss etc. prevented organisations from committing to the full restoration of their supply chain (Ivanov *et al.*, 2014; Park *et al.*, 2013). It was, however, pointed out by one of the directors interviewed in this study that "*natural disasters such as environmental disasters are not a threat to information, they are a means to loss of information. This is because, when they happen, they do not affect the integrity of information, neither do they modify the content of information*" (PI-2).

8.2.2.2 Vulnerabilities to Information within Supply chain

The literature shows that threats often exploit weaknesses and vulnerabilities within organisations. The responses from respondents show that the threats to information can only manifest if and when there are vulnerabilities to the information or information system within an organisation. With regards to the vulnerabilities of information within supply chains, the analysis of respondents' transcribed interview responses generated two main findings in the form of themes. These findings are presented below:

Causes of Vulnerabilities to Information

Respondents identified different causes of vulnerabilities within organisations that often leads to information and information systems becoming exploitable by threats. The most prominent of these causes is the lack of education and awareness of employees. According to one of the respondents, the "*lack of staff education and awareness on security issues is a pathway to information becoming vulnerable*" (PI-8). In the study of Wolden *et al.* (2015), it was also shown that the level of security training and awareness of employees influences the way they behave and react to security programs, frameworks and procedures, and also influences their behaviour toward exposing information towards threats. According to another respondent, the lack of education and awareness of employees includes "*employees not fully understanding the functionality and operation of the system being used in their organisation, and also not fully understanding what their role/profile on the system really means*" (PS-1).

Another cause of information becoming vulnerable that was prominent among respondents' responses was the number of parties involved in the use of information. One of the respondents highlighted that "*the number of people interacting with information and information systems* *determines the level of vulnerability, threat and losses that the information and information system could be exposed to*" (PS-1). Lack of access control (physical or network), manipulation or over-riding of access controls and non-compliance to access control was also identified as being a contributory factor to information becoming vulnerable within any trading network. This is as echoed by one of the respondents who stated that "*security is irrelevant if an organisation has the most secure access controls e.g. biometric but have the doors leading into the organisation constantly open*" (PI-3). This is also similar to the view of some respondents which was that, even if there are physical controls in place, the organisational information and network is still vulnerable if employees use a weak password or share their password with a third party.

The findings from the data analysis with regards to the causes of vulnerabilities to information within supply chains, also show that the lack of software updates and the implementation of patches exposes organisations' information and information systems to different threats and risks. This was also confirmed in the study of Choo (2011), where it was stated that unpatched or not up-to-date systems are a danger to any individual or organisation because they can be easily exploited by malware or malicious individuals. The misconfiguration of information system was also identified by this study's respondents as being the cause of information becoming vulnerable to threats. This, according to respondents is because such misconfigured information system creates a loophole for intruders to gain access to organisation's information. Other causes of vulnerability that emerged from the analysed interviews are negligence of employees, un-integrated information system and the lack of well-defined organisational structures and processes.

Effects of vulnerabilities on Information

The information that flows in a supply chain and the information systems used to share such information, can also be a source of the organisation becoming vulnerable to different threats. Respondents identified fraud as one of the main effects of vulnerabilities (i.e. when exploited by threats) to information and information systems. According to one of the study's participants, "*procurement fraud is made easy when information is vulnerable and breached within the supply chain*" (PI-2). Fraud as an effect of vulnerability to information was also highlighted in the study of Hunton (2012), where it was stated that vulnerabilities are often exploited for financial gains.

Another effect of vulnerability to information that emerged in the data analysis was the denial of services. From the discussions with participants, it was evident that vulnerabilities to information, if exploited, can lead to the denial of organisational services to the legitimate users of such services. Loss of confidential information and compromise of organisational information and information system also emerged as the effect of information vulnerabilities. Similar to these, was also the identification, by respondents, of network and information access, as an effect of vulnerability to information. Reputation damage was also identified as an increasing effect of organisations' information vulnerability. The effects of vulnerability to information that are highlighted in this section were also categorised by some respondents as being the effects of threat on organisations' information.

8.2.3 Primary Objective 4

To understand information assurance as a concept and evaluate its objectives, and also identify how it can facilitate a smooth supply chain process and an efficient and effective supply chain structure

According to one of the directors in one of the IT consulting organisations that were interviewed, "*security and assurance are dependent and related to each other*" (PI-2). A similar point of view was also shared in the studies of Ouedraogo *et al.* (2012) and Cherdantseva & Hilton (2013). Blos *et al.* (2016) in their study, also highlighted an ISO standard (i.e. ISO 28000) that combines security and assurance in the management of security within the supply chain.

Hence, in addressing the fourth primary objective, the themes that were related to information security management and information assurance, from among the generated themes, were considered relevant. Two themes, and the discussion around them, from the transcribed interviews, were considered relevant in addressing this objective. These themes are:

i. Managing Information Security Challenges within Supply Chain
ii. Ensuring Information Assurance within Supply Chain

These themes, their respective sub-themes, and the discussion around them were centred on the focal points of this objective. The discussion of the findings of this study, with regards to this objective, in relation to the identified relevant themes and their sub-themes, are presented below.

8.2.3.1 Managing Information Security Challenges within Supply chain

In the interview sessions, most respondents emphasised the fact that their organisation is always working on establishing new measures or fortifying existing ones, so as to ensure that information and information systems are properly protected and managed. The importance of managing information and information system was also emphasised in the study of Windelberg (2016), in which he explained that the management of the threats and risks to information requires the application of appropriate controls. In this study, findings from the data analysis also show that controls are an important measure in the management of information security challenges.

As shown in Figure 8.3, almost all the participants in this study spoke about one or more forms of control as being important in the management of information security challenges. Although, the findings of this study also shows that most organisations are still lagging in the implementation of these controls. This is as explained by one of the respondents that "*in the implementation of information systems, organisations often focus on getting the system working but not on getting controls in place*" (PS-2).

Another findings, in this study, with regards to controls, is that it is a good practice for the organisations within the same trading network to agree on key controls that can be used in the management of threats within the network. This is so as to enable an easy integration of the security practices of each of the organisations within the network. Based on the findings of this study, controls have been categorised into two, which are, technical and non-technical controls. The analysis of data generated different findings, in the form of themes (i.e. sub-themes), with regards to the technical and non-technical controls that can help in the management of information security challenges within supply chains. These findings are presented below.

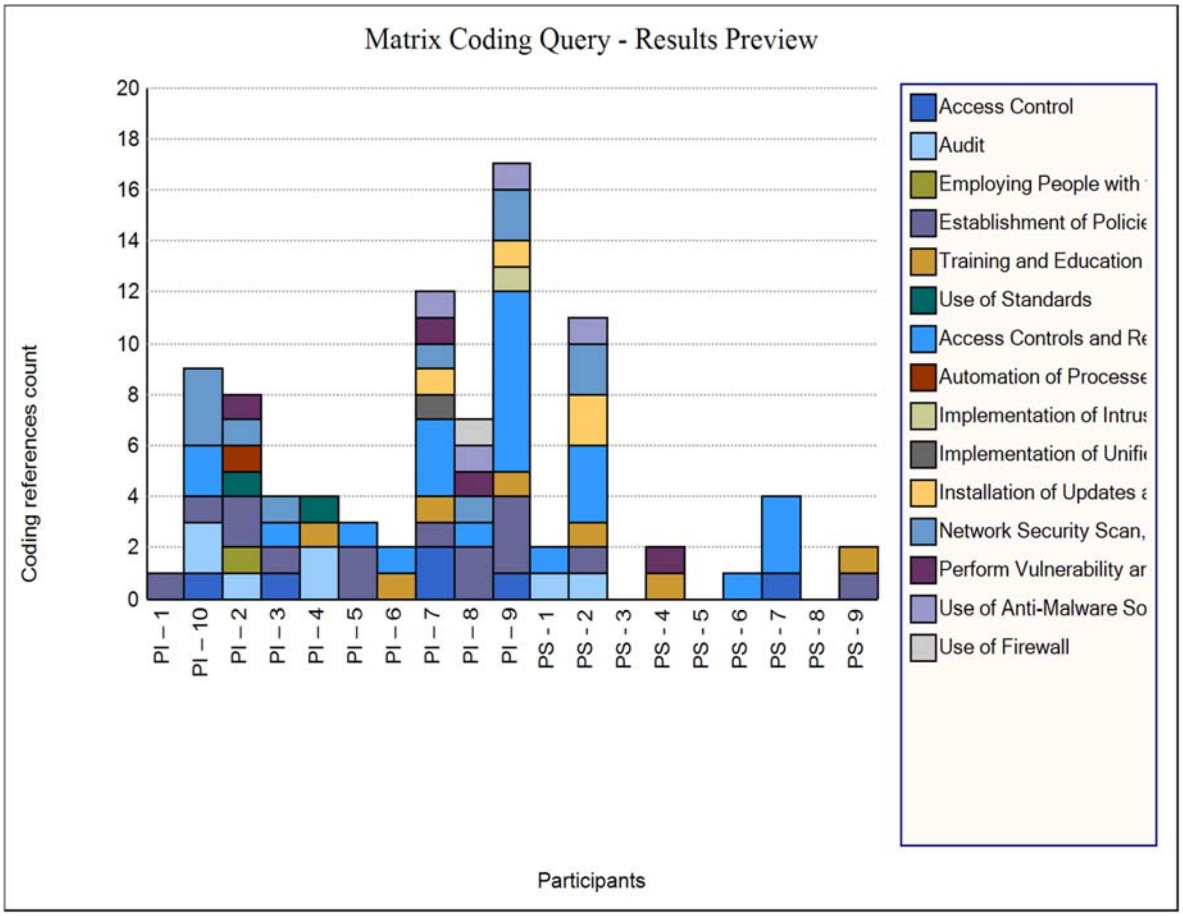


Figure 8.3: Participants' Responses on Controls as a means of Managing Information Security Challenges within Supply Chains (Extract from NVivo)

Technical Controls

Technical controls, as identified by respondents, are very important in the management of information security challenges. The technical controls that were identified by respondents are presented below.

Access Control & Restriction: The findings of this study shows that employees should be allocated only relevant rights to organisational resources, especially information. According to one of the respondents, "*access control and restriction should be implemented so as to restrict users' access to all/any of the type of information within the business*" (PI-5). This was also highlighted in the study of Fuchs *et al.* (2011), in which he stated that one of the most important ways of ensuring information security is through access control. Access control was described by respondents to involve being able to revoke access rights after an employee's departure from the organisation. Also, to include disabling of ports so as to restrict plug-in (e.g. USB) access. The Segregation of Duties (SOD) and partitioning of users were the most prominent means, identified by respondents, as being effective in restricting and controlling employees' access to the organisations' information and network.

Access control was also described to include having measures in place, which ensures authentication before access to the organisation's network is granted. Hence, one of the study's participants stated that "*the network authentication of users must be ensured, even at a server level*" (PI-7). Another respondent also stated that "*employees should have their own individual log-in details that must be used anytime they are willing to log-on to the system or access the organisation's network*" (PI-5). Password was the most referred to by respondents, as a means of ensuring access and restricting users. As explained in the study of Ahlmeyer & Chircu (2016), other authentication methods, asides password, being used by organisations are the Kerberos (used for verifying users) and X.509 (an encryption authenticator). These measures ensure that access is only granted to legitimate individuals who need access to the organisation's information and network.

Network Security Scan, Analysis and Assessment: Respondents did identify that it is important to carry out routine scan and assessment of the organisation's network and also of the organisation's trading network. One of the respondents explained that "*organisations should ensure continuous network scan and network analysis and security assessment. This is so as to be able to detect threats to the network before they cause any harm to the operation and processes within the business*" (PI-3). A system called SIEM (Security Information and Event Management) was identified by one of the respondents (PI-2) as being useful in the monitoring, assessing and analysing of security alerts. The respondent (i.e. PI-2) explained that the SIEM system pulls logs together and flags events such as an IP address being tried so many times on the firewall. Meaning that it is important for organisations to ensure that the network activities of their organisation, are logged (PI-10). It also means that the installation of monitoring systems that helps in flagging unauthorised access, failure to information systems etc. are necessary for the management and assessment of security threats to information.

The implementation of **Intrusion Detection System** (IDS) was identified by respondents as an important means of ensuring the analysis and assessment of organisations' network and the organisation's trading network. Similarly, according to Chauhan *et al.* (2013), IDS incorporates a full-fledged system and network analyser, which can scan and monitor organisations' IP addresses and their network activities. According to one of the directors in the ITCO that was interviewed, IDS is becoming pervasive, especially because of the fear of organisations that external threat and breach to their network can cause a severe consequence in term of data loss. IDS, as described in the study of Zargar *et al.* (2013), learns the normal behaviour and pattern of either the application-level or network/transport level traffic, through the use of artificial intelligence and data mining techniques.

Installation of Updates and Patches: Updates and patches were identified as being important because, with them, organisations are provided with new or updated codes that help in fixing bugs, and that also provides an additional protection mechanism that helps in the management of the security challenges to information systems and information. Similar use of patches and updates were also identified in the study of Issac *et al.* (2014), where it was stated that security updates and patches harden users' information systems against security breaches and attacks. They (i.e. security updates and patches) help protect organisations and their respective supply chain member organisations from being exposed to potential malware and cyber threats (Martin & Rice, 2011).

Some respondents explained that the problem with patches and updates is that they are not implemented by organisations as frequently as they should be. When in actual sense, they should be frequently installed. According to Bojanc & Jerman-Blažič (2008), the infrequent installation of updates and patches often leads to security breaches that could have been avoided or prevented if information systems and their hardware, software and applications are kept up-to-date with appropriate security updates and patches.

Use of Anti-Malware Software and System: Among the technical measures identified by respondents, the use of anti-virus was the second (i.e. after access control) most mentioned means of managing the possible threat intrusion into the organisations' network. While respondents indicated that several new breeds of malicious programs, which are getting more sophisticated and dangerous, are being introduced into the market. They also identified that anti-viruses and their continuous upgrades have been effective in dealing with the new breeds of malicious programs. In agreement to this, Sung *et al.* (2014) in their study, also stated that anti-viruses determine the immune level of software to viruses, and they also enhance the ability of software in being able to prevent emerging malware attacks.

It was explained by some of this study's participants that network intruders often use techniques such as packer and emulator detection to evade malware from being detected by anti-virus software. To manage such techniques, one of the respondents explained that "*anti-virus software that uses detection methods such as static analysis, permission-based analysis and behaviour checking in malware detection should be implemented by organisations*" (PI-6). These methods were also highlighted in the study of Hsieh *et al.* (2015). Gordineer (2003) in his study also stated that organisations can use multiple layers of anti-virus protection such as a gateway, server and even desktop, to manage these techniques. Another means of managing malware is to ensure that "*the anti-virus is always up-to-date*" (PI-9). Making sure anti-viruses are up-to-date, according to most of the study's participant, should be the responsibility of everyone within the organisation, especially on individual's workstations.

Vulnerability and Penetration Test: Penetration testing was identified as one of the means of being pro-active in detecting vulnerabilities and threats to organisations' network and information. This is as explained by one of the respondents that " *organisations need to be pro-active in the management of security challenges, and one of the ways of being pro-active is by carrying out continuous penetration testing*" (PS-4). Penetration testing, as described in the literature, involving the gathering of information about a target, then identifying the possible entry points into the targets' network, and then attempting to break into the network. The findings of the vulnerability and penetration test are then reported back to the organisation so that measures can be put in place. The main objective of vulnerability and penetration testing is to enable organisations to determine the security weaknesses of their business.

Use of Firewall: Respondents explained that firewall is an important network security control that can be used to separate the internal private network from an external public network. In the study of Tseng *et al.* (2016), its role (i.e. firewall) was also explained to be the same. In order to complement access controls, some of the participants in this study explained that firewall can be used. This viewpoint can be attributed to the idea, about firewall, presented in the study of Ifinedo (2014), which shows that firewall can help with perimeter defence, by monitoring and providing access control to organisations' inbound and outbound network connections and traffic. For trading networks, it was suggested by respondents that firewall should be deployed on either side of the servers of the trading organisations.

Non-Technical Controls

It was evident from the literature review that the management of information security challenges cannot be sufficiently done by only implementing technical controls. Hence, the literature, just as indicated by respondents in this study, emphasised the importance of non-technical controls in the management of information security challenges. The non-technical controls that were identified by respondents are presented below.

Policies: One of the security analysts that was interviewed stated that "*the security of information goes beyond the implementation of technical measures, it should also involve the development and implementation of policies that states the rules and regulation governing how information should be managed*" (PI-8). The partner interviewed in this study emphasised that "*policies and procedures are required in the governance of organisational structure. This is because, they help ensure compliance with regulations, good practices and controls*" (PI-1). Policy was the most discussed by respondents with regards to the non-technical means of managing information security challenges. Similarly, in the study of Xiao-yan *et al.* (2011), policies were identified as being an effective means of ensuring the confidentiality and reliability of information.

"*People must be made to adhere policies*" (PI-6). This is the response of one of the study's participants. It is also found in the literature that compliance to policy must be ensured. One of the security consultants explained that "*policies are only as good as their implementation/enforcement. Hence, having policies is one thing, properly implementing them and also enforcing them is another thing*" (PI-3). This viewpoint was also highlighted in the study of Wolden *et al.* (2015), where it was stated that the proper implementation of policies and the compliance to policy, is important in being able to effectively prevent or mitigate against the threats and risks of attacks on supply chains' information and information systems. In the study of Kolkowska & Dhillon (2013), it was explained that the use of an integrated system in facilitating the exchange of information can help ensure compliance with security policies and regulations.

Training and Education of Employees: Most respondents stipulated that one of the most prominent causes of information security violation is the lack of knowledge, training and awareness, which often leads to negligence among employees. Hence, the education, training and awareness of employees were one of the most prominent responses of respondents, with regards to the management of security issues relating to information. One of the security analysts stated that "*employees should be trained and educated, especially* *with regard to potential vulnerabilities and threats*" (PI-9). Similarly, in the study of Bulgurcu *et al.* (2010), it was stated that organisations can use three security countermeasures to address security threats. One of these measures is the security education, training and awareness (SETA) of employees.

The findings of this study show that the security education, training and awareness programs of employees, done by an organisation or done within the organisation's trading network should involve all the organisation's employees and their trading partners' employees, and such programs should be done on a continuous basis. Meaning that every employee in an organisation, irrespective of their position within the organisation, must be involved in the education, training and awareness programs of the organisation. Respondents explained that the training and education of employees makes it possible for employees to take the necessary actions against any potential or existing security threat and attack, while the awareness programs ensure that they do not fall victim of any potential threat or attack.

Audit: Auditing of the systems used within organisations was identified as being important in ensuring that systems are working as expected. One of the respondents explained that "*it is important to perform a walk-through on the systems used within the network. That is, checking to be certain that the entire system is working as expected*" (PI-4). The findings of this study also show that it is not only systems that should be audited, people and the environment in which they (i.e. people and system) operate should also be audited. Auditing of people is important because when people know they are being audited, they tend to ensure that they are compliant with the standards and policies within the organisation. Still on the point of auditing people, one of the respondents stated that "*performing an audit of each employee so as to determine which services they access, helps to ascertain if potentially harmful sites are being visited*" (PI-10). The same respondent further added that the auditing of employees also helps to determine which employee accesses a file (e.g. shared file), visits a certain website etc.

Another important finding of this study is that the processes within an organisation and the organisation's trading networks should also be audited, this is as emphasised by one of the participants in this study, who stated that "*processes has to be continuously audited*" (P1-4). This was also emphasised in the study of Axelrod (2011), where he stated that conducting an audit of each of the processes at each stage of a supply chain structure is important, especially, in order to provide some level of assurance for the supply chain members. The establishment and use of a risk or steering committee was also a theme that emerged in this study as a means of ensuring that audit is conducted thoroughly and on a continuous basis. One of the interviewed directors explained that "*the use of an IT steering* *committees where and when necessary is important in ensuring a continuous audit of the business process and systems*" (PI-2). Sharing the same opinion, another respondent stated that "*the establishment of a risk team that does an internal audit is necessary within the business*" (PS-9).

Access Control: The findings of this study shows that access control in the form of physical control measures are important in the management of information security challenges. Access control was identified as not being only towards technical control but also includes physical control. One of this study's participant stated that "*ensuring user access is controlled, is an important management measure in an organisation. This should, however, include the physical access of people into the organisation*" (PI-10). This was also echoed by another respondent who stated that "*security is irrelevant if an organisation has the most secure access controls e.g. biometric but have the doors leading into the organisation constantly open*" (PI-3).

Use of Standards: According to Blos *et al.* (2016), standards are important in the management of information security challenges because they guide organisations in the development and enforcement of information security practices. This was also highlighted in some of the interviews conducted with this study's participants. Participants, in their explanation, showed that standards can help reduce information loss, information distortion or any other possible risks that can disrupt the supply chain processes and operations. Different standards such as COBIT and ISO/IEC (already explained in section 4.5.2.2) were identified by respondents as being effective in ensuring that information is secured and properly managed.

Employing People with the right skills and competencies: The discussion of respondents with regards to this theme was centred on the fact that the effective use of information systems and the adequate protection of information requires that the right people be employed to be in charge of the installation and use of information systems. Hence, it was deduced from the responses of respondents that having people with the right skills and competencies is very important and helpful in ensuring that information system, and consequently, information, are well protected and managed.

Other means of managing information security challenges that emerged as themes in this study were the *backing up of information* and *the use of an integrated information management platform*. The backing up of information was considered important particularly in the case of natural occurrences (e.g. earthquakes, hurricane). Some respondent also identified the use of an integrated information management platform as being useful in the management of information when there are such occurrences (i.e. natural occurrences). Parker (2013) in his study also highlighted the importance of using an integrated information system to help with the synchronised coordination of information sharing during crisis situations. The importance of such system as explained by one of the respondents in this study is so as to enable trading partners to react flexibly to any disruptions to the flow of information, which could also be caused by natural disasters. In the study of Kolkowska & Dhillon (2013), it was also explained that the use of an integrated system in facilitating the exchange of information can help ensure compliance with security policies and regulations.

8.2.3.2 Ensuring Information Assurance within Supply chain

Providing assurance on the information and information systems used within supply chain was identified in this study, and was also identified in the literature as being an important element in sustaining the relationship between the organisations (and their activities) within the supply chain network. One of the security consultants that was interviewed in this study stated that *"assurance is helpful in ensuring that systems and information are doing what they are expected to be doing"* (PI-4). Another respondent stated that *"assurance should be provided on the IT Systems used within the supply chain"* (PS-2). This, according to him is so as to provide the organisations within the supply chain network some level of relief and certainty that the systems are working as expected and are also adequately protected.

Authors such as Ouedraogo *et al.* (2012), Cherdantseva & Hilton (2013) and Blos *et al.* (2016) have shown in their studies that security and assurance are related to each other. The literature have also shown that providing information assurance, requires an adequate understanding of information security. This study's findings also show that security and assurance are related and dependent on each other. To further confirm this, a word frequency query was run in the NVivo software, so as to determine if there are any similarities in participants' responses, between managing information security challenges and ensuring information assurance within the supply chain. As seen in the word cloud (Figure 8.4), the word frequency query shows that some words (in this case, ideas/concepts) were used commonly by respondents in describing how to manage information security challenges and how to ensure information assurance, within the supply chain.

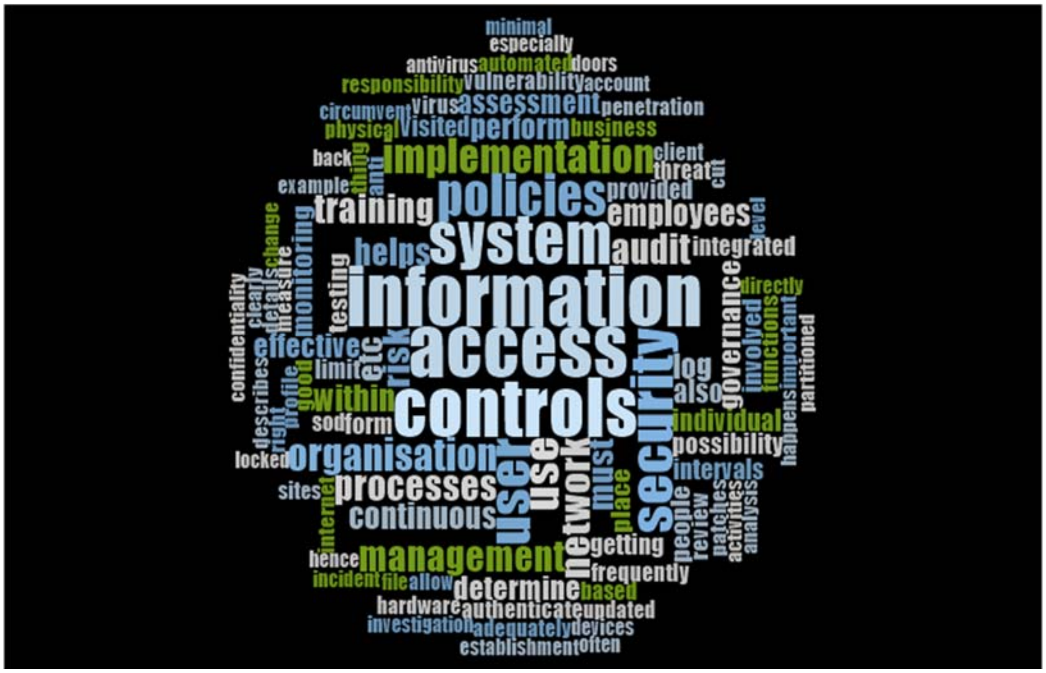


Figure 8.4: Word Cloud of Common Themes Used for Describing How to Manage Information Security Challenges and How to ensure Information Assurance, within supply chain

When respondents were asked about their perception of how information assurance can be ensured within the supply chain, most of their responses were similar to the responses they provided when asked about how they think information security challenges can be managed. From respondents' responses, six (6) findings (i.e. themes) emerged as means of ensuring information assurance within the supply chain. These findings are presented below.

Access Control:

As seen in the word cloud (Figure 8.4), access control was the most common means identified by respondents as being effective in the management of information security challenges and also in ensuring information assurance, within the supply chain. Access control has been discussed in section 8.2.3.1 (i.e. under the technical and non-technical controls). Respondents explained that in order to incorporate and ensure the provision of information assurance for protection, access control is very important within any trading network. One of the respondents stated that "*the motivation for protection is the continuous presence of threats on supply chain information. To protect the information, access controls are of utmost importance*" (PI-6). It was deduced from respondents' responses that the control of access is important because it also ensures that employees only deal with the information that concerns them. Furthermore, respondents' responses also show that if adequate protection measures on the physical environment of an organisation and on the organisation's network and information systems are put in place, the organisation and their trading partners' information can be protected from potential network or information breach.

Compliance with Policies:

The importance of policies in the management of security challenges has been discussed in section 8.2.3.1 (i.e. under the non-technical controls). Respondents emphasised that to guarantee that assurance objectives (i.e. availability, integrity, authentication, confidentiality and non-repudiation) are ensured on the information and information systems within supply chains, the employees within the supply chain network must be made to comply with the policies within the network. Some of such policies, as identified by respondents, include policy on incident management, policy on data loss prevention, policy on Internet access and information risk policy. These policies are, according to respondents, relevant in one way or the other, in order to ensure that assurance is provided on the information and information systems within any trading network.

Appropriate and Adequate use of Information System:

Information system, as shown in the word cloud (Figure 8.4), was identified by respondents as being an important tool in ensuring information assurance. In the interview discussions, respondents explained that the appropriate installation and the appropriate and adequate use of information system is very important in achieving information assurance objectives. As explained in section 8.2.2.2 (i.e. vulnerabilities to information within Supply chain), the misconfiguration of information system is one of the causes of information becoming vulnerable to threats. This, according to respondents is because such misconfigured information system creates a loophole for intruders to gain access to organisation's network and information. Respondents, likewise, pointed out that if the information system is appropriately installed and used, the provision for assurance objectives can be more guaranteed, as there will be fewer loopholes in the information system for intruders to exploit.

Regular Audit:

Audit, which was discussed in section 8.2.3.1 (i.e. under the non-technical controls), was also identified by respondents as being effective in ensuring the provision of information assurance, especially for the protection and detection of vulnerabilities and threats. Audit, as identified by respondents should include the people, network, information system and information within the organisation. Respondents explained that with auditing, organisations are able to detect possible gaps with the business, and subsequently, are able to apply necessary measures to cover up such gaps.

Training, Education and Awareness:

The training, education and awareness of every employee within the organisation were identified as being an effective means of ensuring the protection, detection, reaction and restoration of information. This, as discussed in section 8.2.3.1 (i.e. under the non-technical controls), is important because it enlightens employees on how to detect and avoid any potential threat to the organisation. With proper security training and education programs, employees are also able to know how to react and restore services to normal in the event of information breach or attack.

Risk Assessment and Management (Includes the establishment of risk team)

The establishment of a risk committee/team in the management of information security challenges and in providing assurance on information emerged in this study. Respondents explained that risk assessment and management is important in ensuring that assurance is provided on the information and information systems of the organisation, and to ensure an effective risk assessment and management, it is important to establish a risk team that looks into the risks (potential or existing) occurrences. According to some respondents, risk assessment and management is important because it helps organisations in being pro-active and reactive in the management of security challenges that are either from within the business or from outside the business. One of the respondents stated that risk assessment and management provides project and implementation assurance. The respondent explained that "*in the implementation of an IT system such as an ERP system. Ensuring that the risk involved in the implementation of such system has been adequately taken care of increases the assurance on such system, and also ensures that the implementation project is delivered within budget, on time and as expected*" (PI-4).

One of the interviewed directors explained that "*to ensure assurance, IT governance must be incorporated and integrated into the organisational structures and processes*" (PI-2). This, according to him is because, IT governance incorporates IT control frameworks and standards (e.g. COBIT, ITIL etc.). It also incorporates IT policy statements and procedures. All these, according to responses from most respondents, help in providing and ensuring the availability, integrity, authentication, confidentiality and non-repudiation of information and information systems. They also help in the provision of protection, detection, reaction and restoration measures necessary for the protection of information.

8.3 Other Emerged Themes

Three additional themes, as presented in section 7.4, emerged in this study. These themes and their relevance to this study are presented below.

Supply Chain Structure:

The findings of this study show that the supply chain structure is broad. According to one of the respondents, it incorporates "*the people, position, functions and the different processes and tasks that need to be performed within the supply chain*" (PS-2). Hence, one of the interviewed directors explained that "*organisations or a trading network without a well-defined structure risk the possibility of being exploited by threats. Similarly, less controls often happen on processes in organisations that are not well structured*" (PI-2). The broad scope of supply chain structures was also highlighted in the study of Piderit *et al.* (2011) and MacCarthy *et al.* (2016), where it was stated that the broad and geographical dispersion of modern supply chain structures are being affected by diverse economic and political factors, regulatory frameworks, strategic choices and different technological drivers.

The findings of this study also show that the structure within a supply chain supports the strategy within the supply chain network. According to one of the respondents, "*organisations should have a target operating model that should be supported by a structure that can deliver on the operating model, which then supports the overall organisational strategy*" (PI-1). A similar idea was also highlighted in the study of Huang *et al.* (2016), where it was stated that supply chain structures should be built as a model that can evaluate the level of services offered to customers.

It was also pointed out by one of the respondents that "*the organisational structure is important in the manner in which information is shared and protected*" (PI-5). Similar to this point is what was stated in the study of Ivanov *et al.* (2010), where it was stated that organisation's structure should be built to support the coordination of strategies that ensure that information is adequately and continuously shared between an organisation and their trading partners. Some of the respondents also indicated that the supply chain structure is important in determining the effectiveness of the supply chain structure. This was especially highlighted by one of the study's participants who stated that "*the structure within the supply chain oversees the functions (HR, Finance, IT etc.) of the respective organisations, within the trading network, that supports the organisational strategy and operating model*" (PI-1).

Supply Chain Processes:

One of the respondents explained that "e*ffective and robust supply chain processes make organisations become agile to the market and also makes it possible for them to be able to* *respond to changes in the market quickly, from a demand or crisis perspective*" (PI-1). It was also deduced from the respondents' responses that the effectiveness of the processes within the supply chain determines how resources such as information, material and funds will flow within the supply chain. The importance of having an effective process within the supply chain was also highlighted in the literature by authors such as Kolkowska & Dhillon (2013), Karimi & Davoudpour (2016) and Wiengarten *et al.* (2016).

One of the key findings of this study with regards to processes is that for processes to be kept effective and fully operational, it has to be continuously audited. The auditing of processes was considered important by respondents because they believe that the units within an organisation become more cautious of their respective processes within the overall structure of the organisation when they know their functional process will be audited. This also applies to the different organisations within the supply chain network. The auditing of processes, as identified by respondents, should also involve auditing the respective personnel that are tasked with performing the different processes within the organisation and also, within the supply chain network.

I.T Portfolio within Supply Chain:

The function of the IT unit within an organisation was identified by respondents as being important enough to earn a sit amongst the board. This, unfortunately, is not the case with most organisations, as identified by one of the respondents who stated that, "*IT is still seen as a unit that makes computers works when it should rather be seen as an enabler or a strategic component within the company, hence most organisations do not have a proper CIO or equivalent, within their businesses*" (PI-3). It was also explained by another respondent that, in most organisations, the IT manager reports to the finance manager, and this is not supposed to be the case. This is because the IT manager, who is a technical person is reporting to someone who only sees the business from a financial or business point of view.

"*The role of IT within the business should be elevated to the board/ decision-making level*" (PI-2). It should, according to another respondent "*be fully integrated into the organisational structures and process. This should be to the point where the head of IT should be a member of the board*" (PI-8). The general discussion of the study's respondents with regards to the role of IT shows that, when IT portfolio is elevated within the business, decisions around the provision of security controls for the management of information and information system is properly addressed and made. Also, issues of cost with regards to the implementation of general information security measures around the organisation are properly presented and adequately reviewed.

8.4 Validation of the SCIRM Framework

The Supply Chain Information Risk Management (SCIRM) framework presented in Table 6.4, was developed to help with the identification of vulnerabilities, threats and their severity on information and information exchange within supply chains. The framework takes into consideration the fact that “information risk cannot be regarded as being generic. This means that information risks are considered relative to different supply chains (i.e. the information risks of supply chain A might not be the same as that of supply chain B)” (Maharaj & Ajayi, 2011).

Respondents in this study were asked questions about the SCIRM framework so as to validate the components of the framework. Based on responses from the respondents, the original framework (Table 6.4) was adjusted. In the original framework, six threats were identified, but when respondents were asked about the framework, their suggestions necessitated that the threats be re-categorised. Five major threats, identified by the respondents in this study (that is, in section 8.2.2.1), were used to compute the adjusted framework. An example of a filled-in matrix in the adjusted framework is presented in Table 8.1.

Nodes	risk severity (0 – no risk, 1 – mild, 2- moderate, 3- high)					
	Employees	Hackers & Network Intruders	Malware	Social Engineering	Natural Events/Disasters	Total
H-H	3	0	0	1	1	$R_{HH} = 5$
H-S	3	2	1	1	1	$R_{HS} = 8$
S-S	3	3	2	2	1	$R_{SS} = 11$
S-H	3	2	0	1	1	$R_{SH} = 7$

Table 8.1: An Example of a filled-in Matrix of the SCIRM Framework

Table 8.1 presents the points (Nodes) through which information may be shared within an organisation and the organisation’s trading partners. These nodes are also considered the sources through which information is shared among trading partners. They are also considered the vulnerable points through which information could be exploited. The possible severity of the risks (i.e. the “Total” column) to information, when exploited by the identified threats (in this study), is presented in Table 8.1. The meaning of the notations used in the table is presented below:

H: Represents Human. This means using an employee as a means of capturing, processing, reporting and sharing information within the supply chain.

S: Represents System. This means using systems (e.g. ERP, EDI) as a means of capturing, processing, reporting and sharing information within the supply chain.

Hence:

H-H: refers to a situation where information is shared by a human to human. This could also be referred to as "Manual" information sharing.

H-S: refers to a situation where information is shared by a human to the system. This could also be referred to as "Semi-Automated" information sharing.

S-S: refers to a situation where information is shared from system to system. This could also be referred to as "Automated" information sharing.

S-H: refers to a situation where information is shared from system to human. This is also another type of "Semi-Automated" information sharing.

As explained in the original SCIRM framework, "the table is not symmetric in that R_{SH} is not the same as R_{HS}. As an illustration, consider that a human may pass a computer virus to a computer (via a memory stick, through bad browsing habits etc.) but a computer cannot pass a computer virus to a human" (Maharaj & Ajayi, 2011).

The 3's in the table indicates that there is a high risk, while the 0's indicates that there is no risk. So in the example presented in Table 8.1, it may be seen that the greatest risk to the supply chain is that arising from Human-System interface which scored 11 (higher numbers represent higher risk).

The SCIRM framework proposes that the total Risk (R) to information within a supply chain is the sum of the individual (R_i), where

$$R_i = \alpha_{ik} r_{ki}.$$

This equation may be written in full as:

$$R_1 = \alpha_{1k} r_{k1} = \alpha_{11} r_{11} + \alpha_{12} r_{21} + \alpha_{13} r_{31} + \alpha_{14} r_{41}$$

$$R_2 = \alpha_{2k} r_{k2} = \alpha_{21} r_{12} + \alpha_{22} r_{22} + \alpha_{23} r_{32} + \alpha_{24} r_{42}$$

$$R_3 = \alpha_{3k} r_{k3} = \alpha_{31} r_{13} + \alpha_{32} r_{23} + \alpha_{33} r_{33} + \alpha_{34} r_{43}$$

$$R_4 = \alpha_{4k} r_{k4} = \alpha_{41} r_{14} + \alpha_{42} r_{24} + \alpha_{43} r_{34} + \alpha_{44} r_{44}$$

Thus

$$R = R_1 + R_2 + R_3 + R_4$$

Note that “the r_{kj} are values that range from 0 to 3 and the α_{ik} are weights that will scale the relative importance of the particular risk vector for the supply chain in question. For example for a supply chain that that has to span the Indian Ocean during the Monsoon, the coefficient of environmental or natural event/disaster vector will be elevated. It is proposed that these coefficients range from 1 – Standard contribution, 2 – Heightened contribution, 3 – Significant (severe) contribution” (Maharaj & Ajayi, 2011).

As with other risk models, “the SCIRM framework proposes that a risk tolerance point is agreed upon and accepted by organisations for each of their supply chains. Thus, when the supply chain information risk is below the tolerance point, “Risk Acceptance” (as explained in section 4.3) as a risk management strategy can still be applied, but when the supply chain information risk exceeds the tolerance point, then “Risk Avoidance or Mitigation” (as explained in section 4.3) as a risk management strategy should be considered” (Maharaj & Ajayi, 2011).

8.5 The Proposed Model

The main objective of the study is to propose an information assurance model that can enable organisations to protect and sustain their respective information within the supply chain structures, and that can also enable them to minimise or prevent the risks that information within the supply chain processes could be exposed to. To achieve this main objective, four primary objectives, discussed in section 8.2.1 – 8.2.3, were developed. The finding of this study in relation to these four objectives has guided in the development of the study’s proposed model. The model is presented in Figure 8.5.

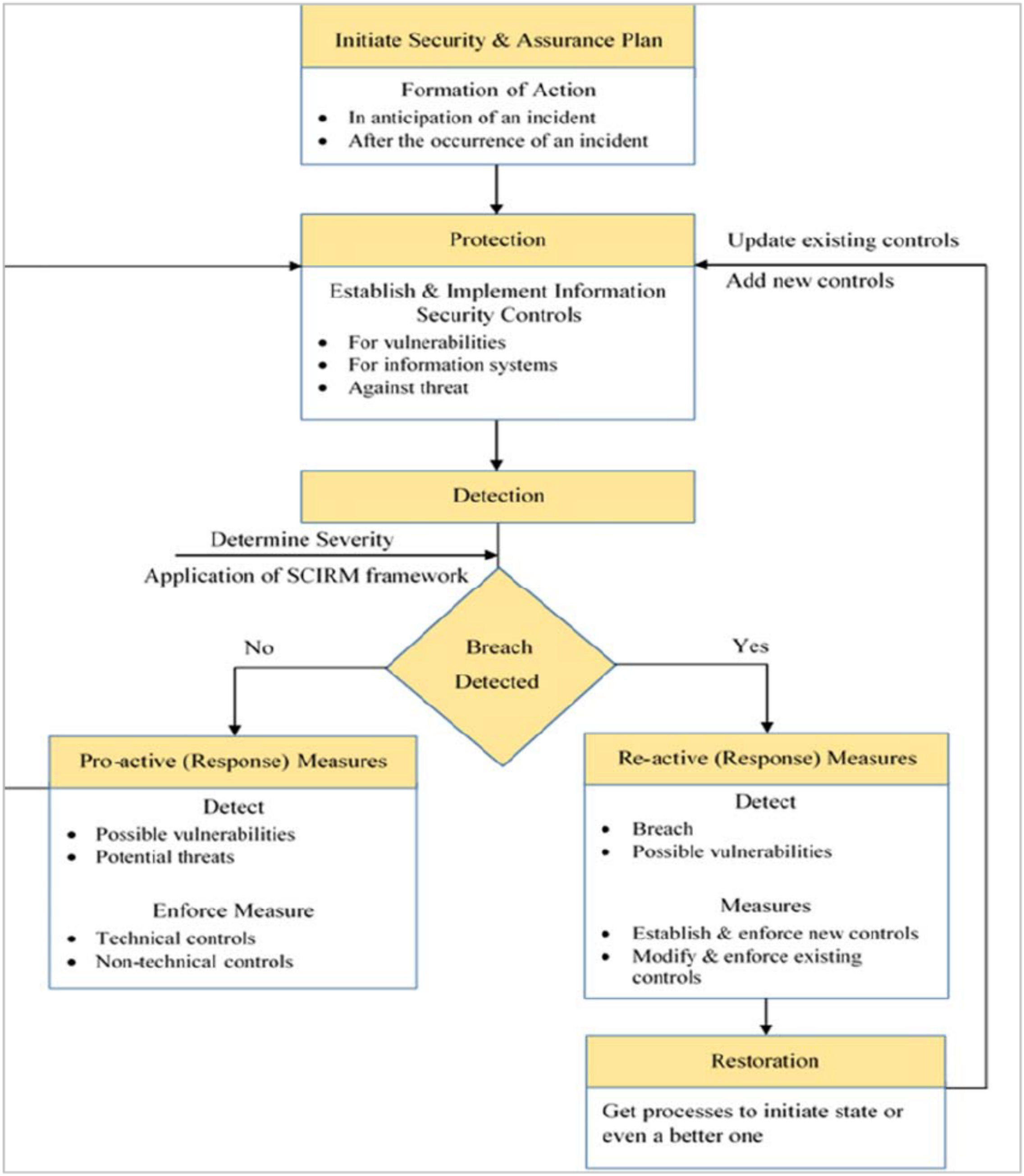

Initiate Security & Assurance Plan
Formation of Action
In anticipation of an incident
After the occurrence of an incident
Protection
Update existing controls
Add new controls
Establish & Implement Information Security Controls
For vulnerabilities
For information systems
Against threat
Detection
Determine Severity
Application of SCIRM framework
No
Breach Detected
Yes
Pro-active (Response) Measures
Detect
Possible vulnerabilities
Potential threats
Enforce Measure
Technical controls
Non-technical controls
Re-active (Response) Measures
Detect
Breach
Possible vulnerabilities
Measures
Establish & enforce new controls
Modify & enforce existing controls
Restoration
Get processes to initiate state or even a better one

Figure 8.5: Proposed Information Assurance Model for Supply Chain

8.5.1 Discussion of the Model's Components and Process

The IA model was developed based on the responses of this study's participants with regards to ensuring information assurance within supply chain and also, based on their responses on managing information security challenges within supply chain structures and processes. The components of the model and their relationship to each other are presented below.

Security & Assurance Plans

It was stated in section 8.2.3.2, that respondents in this study emphasised that security and assurance are very related and dependent on each other. This was also found in the literature, where different authors have shown that both concepts are much related. Hence, in the model both have been combined. The purpose of the model is to provide some sort of guidance on how the objectives of information assurance (i.e. availability, integrity, authentication, confidentiality, and non-repudiation) can be achieved and ensured on the information and information system with supply chains. To achieve these objectives, organisations need to formulate a plan of action that centres majorly on the management of incidents, either before their occurrences or after their occurrences. The security and assurance plan component of the model begins the process of managing information security challenges and also providing assurance on information.

Protection

The main objective of information security and assurance is to ensure that information and information systems are adequately protected. Hence, the initiation of the security and assurance plan is majorly focused on ensuring the protection of information. To ensure information is protected, organisations and their trading partners should establish and implement information security controls (section 8.2.3.1) against threats. These controls should also be capable of ensuring that vulnerable information and the information systems used within the business and the entire supply chain network are protected. The controls must include both technical and non-technical controls (section 8.2.3.1).

Detection

To ensure that information is adequately protected, organisations should conduct regular check (e.g. penetration testing, use of tiger team) of their network, information system and information. Hence, detection is an important component in the protection of information. Organisations and their trading partners should establish detection practices that allow for the determination of possible vulnerabilities, potential threats and breaches to the network, information system and information. When detection practices are completed, organisations should decide on the most appropriate "***response***" strategy to use in managing the outcome of the detection practice. The strategy should involve either applying pro-active measures (i.e. when no breach is detected) or re-active measures (i.e. when a breach is detected). The outcome of the detection practice should also help organisations determine if and when necessary to establish new controls or modify existing ones.

One of the key requirement at this stage of the model is that organisations and their trading partners must determine the severity of the vulnerabilities, potential threats and breach to their network and information, in order to be able to determine the appropriate control measure for managing information challenges. To determine the severity, the SCIRM framework (section 8.4) is a tool considered relevant, as it helps in determining the severity of the threats and risks to information and information system.

Restoration

In the event where re-active measures (i.e. when a breach is detected) was the appropriate strategy after the detection practice was completed, the restoration of processes and operation should be the next stage in the provision of information assurance. At this stage, if necessary, organisations should implement new controls or update existing one.

8.6 Conclusion

In this chapter, the findings from the data analysis in relation to the study's objectives was presented. The findings of this study show that information is an important resource within supply chains because it drives the effective use of the other supply chain resources. The findings of this chapter also show that in the protection of supply chain information and in also providing assurance on supply chain information and information system, it is important to identify, categorise based on severity and understand the different threats to information. It is also important to understand the causes of vulnerabilities to the information within supply chains. These are important, also because they provide an understanding and enable decision making, with regards to the appropriate security measures, mostly in the form of controls, which can be adopted and implemented in the management of information security challenges. The SCIRM framework, developed to help with the identification of vulnerabilities, threats and their severity on information within supply chains, was also presented in this chapter. The study's proposed model that could help organisations protect and sustain their respective information within the supply chain structures, and also enable them to minimise or prevent the risks that the information within supply chain processes could be exposed to, was also presented in this chapter.

CHAPTER 9: CONCLUSION

9.1 Introduction

Supply chain integrates the activities involved in the procurement of material, the transformation of the raw materials to final products and the distribution of the final products to consumers. In order to remain competitive, organisations, through supply chain innovations, are transforming their business models. These innovations include allowing consumers to participate in product design through the use of Internet platforms, using technology to automate the supply chain processes and connecting manufacturers to final consumers. This, therefore means that technology the Internet and technology is increasingly becoming an integral supply chain component. According to Pérez-Aróstegui *et al.* (2015), the competency of information systems and technology in enabling innovations in supply chains, is based on the following dimensions:

- ➢ The information system and technology infrastructure present in each of the organisation within the trading network
- ➢ The integration of information systems and technology with organisational strategy and across the organisation's trading network.
- ➢ The technical knowledge possessed by the employees of the organisation within the trading network

Supply chain organisations are using technology to enhance the easy acquisition and the smooth flow of information. They are also using it to develop effective communication channels and adequately plan their business activities. The introduction of technology is, however, also causing information to be exposed to different vulnerabilities, threats and risks. Organisations are therefore seeking means of managing information risks. They are also increasingly seeking assurance on the information and information systems within their supply chain network.

This study was conducted with the main aim of developing and proposing an information assurance model that can enable organisations to protect and sustain their respective information within the supply chain structures, and that can also enable them to minimise or prevent the risks that information within the supply chain processes could be exposed to. In doing so, the study investigated the following:

i. The role of information and information systems within supply chains.

ii. The impact of sharing information within the various processes and structures of the different components of supply chains. This was done by also investigating the information systems used for sharing information.

iii. The issues and challenges surrounding the security of information systems, and also, information, as it moves through the various supply chain structures and processes.

iv. Information assurance as a concept, and evaluated its objectives, and also, investigated how it can facilitate a smooth supply chain process and an efficient and effective supply chain structure.

In the previous chapter, the findings of this study, in relation to the objectives of the study was presented. This chapter presents a recap of the previous chapters.

9.2 Study's Conclusions

From the first chapter of this thesis, it may be concluded that today's global market environment is highly competitive and also present organisations with very volatile consumers' demands. The market environment is equally faced with the challenge of effectively sharing and managing resources such as information, funds and materials, among the increasingly geographically dispersed trading partners. The market is also faced with the challenge of increased vulnerabilities, threats and disruptions to these resources. To manage these challenges, organisations are demanding and continuously developing integrated structures and processes that are facilitating the establishment of trading networks that enhances the smooth flow of resources. These networks, which often consist of a number of players that share interdependent interactions, allows for the members to complement each other's deficiencies and share benefits and losses. The networks, if properly managed, also facilitate each member's capability to achieve quality performance and become resilient.

The second chapter of this thesis presented a review of literature on supply chain, supply chain network, structures and processes. The chapter also discusses supply chain disruptions, risks and management. From the review and discussion, it may be concluded that supply chains have evolved from being linear to becoming a value web that connects different organisations to diverse trading networks. It may also be concluded that the basis of competition in the global market has shifted towards a service oriented approach where organisations competitiveness is determined by the strength of their supply chain network and also by the network's ability to flexibly and quickly respond to market fluctuations and developments. Thus, making it important for organisations to consider their supply chains as not only a process but also a structure and a strategic function that should be headed by someone who reports directly to the board.

Sourcing for raw materials from different geographical locations, establishing production facilities across different geographical location and serving consumers that are of different geographical location are some of the important elements and contributing factors influencing modern supply chain structures and processes. This is because they affect how information is shared, how responsibilities are allocated and how decisions are made within supply chains. The literature also shows that the structure of the supply chain and its member organisations determines the agility of the supply chain. It also determines the ease of organisations' access to resources. Although, according to Gunasekaran *et al.* (2015), the complexities existing within most modern supply chains, is a function of the structures and processes within the supply chains.

The second chapter further shows that supply chains have become long and complex, and as a result, are constantly vulnerable and continuously being exposed to different disruptions and risks that are of high severity. To deal with the disruptions and risks, authors such as Mizgier *et al.* (2015), Foulds (2015) and Lemmens *et al.* (2016) have suggested that trading organisations should create resilient supply chains that can anticipate disruptions, limit the impact of disruptions, and quickly return the activities and processes of the supply chain to its previous or even a better state. Furthermore, they also suggested that the overall supply chain be adequately managed, so as to ensure the smooth flow of resources, while at the same time, enhancing the productivity and profitability of the supply chain members. The chapter, however, also shows that there are no single strategy, method or approach for managing supply chain risks. Rather, supply chain risk management depends on the characteristics and context of the situation leading to the risk or the environment surrounding the risk.

A review of the literature on the role of information and the importance of sharing information among trading partners was presented in chapter three. The chapter also focuses on some of the prominent information systems and technologies that are facilitating the acquisition, storage, processing and sharing of information within supply chains. From the review of the literature, based on the chapter, it can be established that the supply chain is a system, in which information is an important requirement in connecting the different organisations in the system, in both the upstream and downstream directions. The importance of the access to real-time information as being a factor in reducing information asymmetry was also presented in the chapter. The chapter also establishes that the increase in information complexity and the distortion to information can cause a drop in the ability of organisations and their respective trading partners to make quality decisions. Hence, information need to be adequately managed and protected.

Chapter three also establishes that, today's complex supply chain networks have necessitated the need for more frequent, efficient and effective information sharing among trading partners. Furthermore, the chapter establishes that in order to collaborate and also be able to create a resilient and agile supply chain, organisations must share information. This is because information sharing improves the coordination of supply chain and also help organisations to effectively respond to threats from the market environment. It also helps improve inventory stability, forecasting and decision making. Although, according to Tong & Crosno (2016), the sharing of information could also lead to a possible decrease in supply chain performance. This happens when trading organisations share incomplete or inaccurate information, as a result of lack of trust, misalignment of information or simply, unwillingness to share information.

Organisations are increasingly understanding that their “ability to transmit information in electronic format improves supply chain operations considerably” (Hinkka *et al.*, 2013, p.1145). Hence, information systems and different technologies are increasingly being used for the acquisition, storing, processing and sharing of information within supply chains. In chapter three, researchers’ view on the fact that information systems and technologies are important in improving information quality, operational efficiency, service level and the agility of supply chains, is presented. The chapter also shows that leading supply chains are known to be aggressive in acquiring technical capabilities through the use of information systems and technologies such as VMI, EDI, RFID, CRM, ERP, Cloud Computing etc. It was however, also established in the chapter that the use of information systems often requires significant investment which not all the parties in a trading network can always afford.

The importance of securing information and providing assurance on the information within supply chains was presented in chapter four. The discussion in the chapter reveals that in the protection (provision of guardians) of supply chain information, it is important for organisations and researchers alike, to identify and understand the threats to information within the supply chain, the vulnerabilities of information within the supply chain’s structures and processes, and the guardians or protective measures that can be provided or adopted to protect information. The chapter also reveals that threats, if not properly managed, adversely affect the confidentiality and integrity of information and the availability of information systems. Reasons such as financial gains, unparalleled trusts and lack of up-to-date skills and knowledge of employees, are identified in this chapter, as being some of the factors causing a continuous increase in the degree and extent of security breaches and threats on supply chain information.

Chapter four further reveals that the vulnerabilities and threats to supply chain information often exposes the supply chain to different risks that ultimately cause a decline in the supply chain performance. The realisation of the negative effects of threats and risks to supply chain information has made the management and security of supply chain information and information systems, become a concept of growing interest to researchers and practitioners. It is revealed in the chapter that organisations are constantly looking for means of securing the information within their supply chain. To do so, they are implementing security measures that include technical and non-technical measures. Some of the technical measures being implemented include the use of antivirus, IDS, firewall etc. While some of the non-technical measures being implemented include the establishment of policies, the adoption of standards, audit etc.

The importance of providing assurance on the information within supply chains was also presented in chapter four. The chapter reveals that most organisations do not give information the same protection, or request for similar assurance, as they do with their organisational finances. This should, however, not be the case, because information assurance ensures the "ability of an organisation to manage the risk to the governance, compliance, confidentiality, integrity and availability of its information at all times" (Bunker, 2012, p.21). To provide assurance, the chapter establishes that the audit of each of the activities and information at each stage of the supply chain should be frequently performed. Continuous assessment, monitoring of critical processes and the validation that standards are followed should also be performed frequently throughout the supply chain, in order to provide the needed assurance on the supply chain information and on the overall supply chain activities.

The methodology underpinning this study was presented in the chapter five of this thesis. In the chapter, the study's research design and approach, data collection method and instrument, the population and sample of interest, the recruitment and selection of the study's participants and the data analysis technique employed in the study were presented. In the chapter, it was indicated that this study adopted the interpretivist philosophical assumption and the epistemology dimension. These were adopted because they guided the researcher in obtaining explanations and experiences, with detailed examples, from the study's participants. It was also established in the chapter that the exploratory research design and the case study approach were the most befitting for achieving this study's objectives. In addition, it was shown in the chapter that a qualitative research method was more appropriate for the study. Since a qualitative research method was adopted, semi-structured interviews was chosen as the primary means of data collection.

The rationale and criteria considered in determining the sample of the study was established in chapter five. Furthermore, the data analysis process that detailed the interview process, the interview transcription process, the generation of themes, the use of NVivo to further enhance data management and the process of data analysis, were all also presented in the chapter. The manner in which the trustworthiness (which includes the credibility, transferability, dependability, confirmability) of the study was achieved, was also detailed in the chapter. Finally, in the chapter, the ethical considerations that covers how the anonymity, privacy and confidentiality of the study's participant, and how informed consent was obtained from the study's participants, was also presented.

The frameworks adopted to help in identifying the starting point of the research problem and to also help in establishing a direction for addressing the problem was presented in the chapter six of this thesis. In the chapter, the alignment of the study's research questions to the study's adopted frameworks was also presented. As identified and explained in the chapter, the "Information

Systems (IS) Research Framework" developed by Hevner *et al.* (2004) was adapted to this study, because it has been identified by different researchers as being useful and practical in solving identified research or organisational problems relating to IT or IS. The supply chain security framework developed by Speier *et al.* (2011), and the SCIRM framework developed by Maharaj & Ajayi (2011) that were also adapted and adopted, respectively, to this study was also presented in the chapter.

Chapter seven presents the analysis of the transcribed interviews. In the same chapter, the demographics of the study's participant and the type (i.e. category) of organisations they represented was also presented. The generated themes (both main and sub themes) from the analysis of the transcribed interviews was also presented in this chapter. Finally, in the chapter, the link between the generated themes and the main research questions was established.

The findings and the discussion surrounding the findings of this study was presented in chapter eight. In the discussion of the findings, supporting evidence in the form of quotations from the transcribed data, and also from the literature was used to further explain and justify the findings. The chapter also presented the relationship between the study's research objectives and the generated themes. The developed model to help provide information assurance, which is the main objective of this study, is also presented in this chapter. From the discussion of the study's findings in chapter eight, it may be concluded that information is one of the most important element to any organisation and the organisation's trading partners, hence, losing it is one of the worst thing that can happen to any organisation. It may also be concluded that, the concern of organisations, with regards to information, centers mostly on maintaining the integrity and availability of information.

The discussion in chapter eight shows that information is mostly shared among trading partners either through electronic means or through call centres. Furthermore, from the discussion in the chapter, it can be concluded that information is important in enhancing collaborative-relationships between organisations, in facilitating trend analysis and in providing competitive advantage. Similarly, information systems are also identified to be important in the capturing, processing, use and management of the information within supply chain. The chapter presents the major information security threats which are employees, hackers & network intruders, malware, social engineering and natural disasters, which were identified from the analysed transcribed interviews. These threats, if not adequately managed, can cause disruptions that exposes the supply chain information to different kind of risks.

The application of control measures was identified in the findings of this study as being important in the management of information security challenges within supply chains, and also, in ensuring information assurance within supply chains. These control measures, as presented in chapter eight include the establishment and application of access controls and restrictions (i.e. technical and non-technical), penetration testing and network scan, installation of updates and patches, establishment and enforcement of policies, training and education of employees, employing people with the right skills and competencies etc. In the same chapter, the validation of the SCIRM framework and the developed model (i.e. the main objective of the study) from the findings of the study were also presented. The model shows that in order to ensure security and assurance on supply chain information, organisations must initiate security and assurance plans, which helps in the formation of action against the occurrence of unwanted incidents. They must also initiate protection activities which should include the detection of vulnerabilities and threats to information and information systems. Then, where and when necessary, apply pro-active or re-active measures that ensures the restoration of the supply chain structures and processes to their initial or even a better state.

9.3 Contributions of the Study

The contribution of this study are mainly two. The first being the Supply Chain Information Risk Management (SCIRM) framework that can help in identifying and understanding the severity of threats to information within supply chains' structures and processes. This framework is presented in section 8.4. The framework is useful in the identification of vulnerabilities, threats and their severity on information and information exchange within supply chains. The framework takes into consideration the fact that information risk is relative and hence cannot be regarded as being generic. This is because the risk to information within an organisation or within a supply chain are not necessarily the same within another organisation or supply chain. The framework identifies common nodes through which information may be shared within an organisation and between an organisation and its trading partners. These nodes, which are presented in section 8.4, also represents vulnerable points through which information could be exploited.

The SCIRM framework proposes that the total Risk to information within a supply chain is the sum of the individual within the supply chain. This therefore means that the risk that the information of a supply chain member organisation is exposed to, could be a risk that affects the organisation's entire supply chain network. Furthermore, the SCIRM framework proposes that a risk tolerance point is agreed upon and accepted by all the organisations within a supply chain network. Thus, when the supply chain information risk is below the tolerance point, risk acceptance as a risk management strategy can still be applied, but when the supply chain information risk exceeds the tolerance point, then risk avoidance or mitigation as a risk management strategy should be considered.

The second contribution of this study is the development and proposal of an information assurance (IA) model that can enable organisations protect and sustain their respective information within the supply chain structures, and that can also enable them to minimise or prevent the risks that information within the supply chain processes could be exposed to. This IA model is presented in section 8.5. The IA model consist of four main components, which are: Security & Assurance Plans, Protection, Detection and Restoration. The first component which is security & assurance plans, indicates that there is a need for organisations and their trading partners to form an action plan in anticipation of an incident and also, in the occurrence an incident. This component of the IA model begins the process of managing information security challenges and also begins the process of providing assurance on information and information systems. The second component of the model which is protection, indicates that the adequate protection of information and information systems is an important objective of information security and assurance. To ensure information and information systems are protected, organisations and their trading partners should establish and implement security controls against threats. These controls must include both technical and non-technical controls (discussed in section 8.2.3.1).

Detection, which is the third component of the IA model, indicates that to ensure that information is adequately protected, organisations and their trading partners should conduct regular checks (e.g. penetration testing, use of tiger team) of their network, information system and information, so as to be able to determine any possible vulnerabilities, potential threats and breach. Included in this component is the determination of the appropriate "response" strategy that may be employed to manage the outcome of the detection practice. The response strategy (presented in Figure 8.5) should involve either the application of pro-active measures (i.e. when no breach is detected) or re-active measures (i.e. when a breach is detected). At this stage of the IA model, the SCIRM framework is considered relevant in the determination of the severity of the vulnerabilities, threats and risks to the information and information systems within the overall supply chain network.

The last component of the IA model is the restoration plan in the event where re-active measures (i.e. when a breach is detected) are considered the appropriate strategy, after the detection practice is completed. This component is important in the provision of assurance on information and information systems. This is because, organisations often need the assurance that if anything were to go wrong within their organisational or supply chain network, the activities in the network will be quickly returned to their previous or even a better state. At this stage of the IA model, if necessary, new controls or updating of existing controls should be considered.

9.4 Study’s Challenge and Limitation

Each organisation, after agreeing to their employees being interviewed for the study, indicated that only between 2 to 4 of their employees can be made available to participate in the study. This was mainly because of the tight schedule and limited availability of their employees. They all (i.e. the organisations), however, allowed the participants to be determined by the researcher. Hence, giving the researcher some level of control over who to participate in the study. To overcome this challenge, participants were drawn from three different organisations from each of the two categories of organisations considered as the point of data collection in this study. This allowed for a diverse respondents that can present broad views on the subject being investigated.

The insufficient availability of literature on information assurance, especially information assurance within supply chain was a limitation in this study. To manage this limitation, the literature on information security, information risk management and supply chain information was used to complement the discussion presented in this study on information assurance. The reason for this is because the preliminary review of the literature and pilot interaction with information security experts showed that information security and assurance are closely related. Another limitation in this study was the access to the selected participants in the study, especially since they were from diverse organisations. This limitation was also combined with the busy time schedule of the participants. These limitations affected the time (i.e. duration) it took in completing this study’s data collection. To manage these limitations, most of the participants had to be met at their most convenient time. That, however, was only possible on the days they are not visiting the client site or not busy attending to organisational issues, which are not so common days for most of the participants of this study.

9.5 Recommendations

In order to secure and provide assurance on information, the following are the recommendations of the study.

Organisations should ensure that they:

- Establish an effective means of sharing information between them and their trading partners.
- Identify the vulnerable information within their business structures and processes.
- Identify and rank the threats to the information and information systems within their business structures and processes.
- Employ the use of information system in the acquisition, storage, processing and sharing of information.

- Manage information security challenges and ensure information assurance within their business structures and processes, by combining and implementing any of the technical and non-technical control measures presented in this study (i.e. section 8.2.3.1).
- If and when necessary, adopt security and assurance standards, policies, models and frameworks that can be effective in ensuring the availability, integrity, authentication, confidentiality and non-repudiation of information and also ensure the continuous availability of information systems.

9.6 Future Research

The review of the literature and the findings of this study shows that some areas relating to information and supply chain still need to be explored. These areas include:

- The investigation of the impact of the continuous evolution technology on supply chain networks.
- The investigation of how to extract meaning and knowledge from the large amount of supply chain data presently existing.
- The investigation of how the understanding of supply chain network as a complex adaptive system can enables supply chain collaboration and optimisation.

REFERENCES

Accorsi, R., Manzini, R., & Maranesi, F. (2014). A decision-support system for the design and management of warehousing systems. *Computers in Industry, 65*(1), 175-186. doi: https://doi.org/10.1016/j.compind.2013.08.007

Ahlmeyer, M., & Chircu, A. M. (2016). Securing the internet of things: A review. *Issues in Information Systems, 17*(4).

Ajayi, N., & Maharaj, M. (2010). *Effects of information sharing within supply chains.* Paper presented at the Proceeding to SACLA.

Al-jawazneh, B. E. (2016). The prospects of cloud computing in supply chain management (a theoretical perspective). *Journal of Management Research, 8*(4), 145-158.

Alyahya, S., Wang, Q., & Bennett, N. (2016). Application and integration of an rfid-enabled warehousing management system – a feasibility study. *Journal of Industrial Information Integration, 4*, 15-25. doi: https://doi.org/10.1016/j.jii.2016.08.001

Amoo Durowoju, O., Kai Chan, H., & Wang, X. (2012). Entropy assessment of supply chain disruption. *Journal of Manufacturing Technology Management, 23*(8), 998-1014. doi: doi:10.1108/17410381211276844

Angeles, R. (2009). Anticipated it infrastructure and supply chain integration capabilities for rfid and their associated deployment outcomes. *International Journal of Information Management, 29*(3), 219-231. doi: http://dx.doi.org/10.1016/j.ijinfomgt.2008.09.001

Ardalan, Z., Karimi, S., Naderi, B., & Arshadi Khamseh, A. (2016). Supply chain networks design with multi-mode demand satisfaction policy. *Computers & Industrial Engineering, 96*, 108-117. doi: http://dx.doi.org/10.1016/j.cie.2016.03.006

Atieh, A. M., Kaylani, H., Al-abdallat, Y., Qaderi, A., Ghoul, L., Jaradat, L., & Hdairis, I. (2016). Performance improvement of inventory management system processes by an automated warehouse management system. *Procedia CIRP, 41*, 568-572. doi: https://doi.org/10.1016/j.procir.2015.12.122

Avram, M. G. (2014). Advantages and challenges of adopting cloud computing from an enterprise perspective. *Procedia Technology, 12*, 529-534. doi: http://dx.doi.org/10.1016/j.protcy.2013.12.525

Axelrod, C. W. (2011, 15-17 Nov. 2011). *Assuring software and hardware security and integrity throughout the supply chain.* Paper presented at the 2011 IEEE International Conference on Technologies for Homeland Security (HST).

Baldini, G., Oliveri, F., Braun, M., Seuschek, H., & Hess, E. (2012). Securing disaster supply chains with cryptography enhanced rfid. *Disaster Prevention and Management: An International Journal, 21*(1), 51-70. doi: doi:10.1108/09653561211202700

Bang, Y., Lee, D.-J., Bae, Y.-S., & Ahn, J.-H. (2012). Improving information security management: An analysis of id–password usage and a new login vulnerability measure. *International Journal of Information Management, 32*(5), 409-418. doi: http://dx.doi.org/10.1016/j.ijinfomgt.2012.01.001

Baxter, P., & Jack, S. (2008). Qualitative case study methodology: Study design and implementation for novice researchers. *The Qualitative Report, 13*(4), 544-559.

Bazeley, P. (2009). Analysing qualitative data: More than 'identifying themes'. *Malaysian Journal of Qualitative Research, 2*(2), 6-22.

Bazeley, P., & Jackson, K. (2013). *Qualitative data analysis with nvivo*: Sage Publications Limited.

Bian, W., Shang, J., & Zhang, J. (2016). Two-way information sharing under supply chain competition. *International Journal of Production Economics, 178*, 82-94. doi: http://dx.doi.org/10.1016/j.ijpe.2016.04.025

Blos, M. F., Hoeflich, S. L., Dias, E. M., & Wee, H.-M. (2016). A note on supply chain risk classification: Discussion and proposal. *International Journal of Production Research, 54*(5), 1568-1569. doi: 10.1080/00207543.2015.1067375

Bojanc, R., & Jerman-Blažič, B. (2008). An economic modelling approach to information security risk management. *International Journal of Information Management, 28*(5), 413-422. doi: http://dx.doi.org/10.1016/j.ijinfomgt.2008.02.002

Borum, R., Felker, J., Kern, S., Dennesen, K., & Feyes, T. (2015). Strategic cyber intelligence. *Information and Computer Security, 23*(3), 317-332. doi: doi:10.1108/ICS-09-2014-0064

Bottazzi, G., & Italiano, G. F. (2015, 26-28 Oct. 2015). *Fast mining of large-scale logs for botnet detection: A field study.* Paper presented at the 2015 IEEE International Conference on Computer and Information Technology; Ubiquitous Computing and Communications; Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Computing.

Bowen, G. A. (2005). Preparing a qualitative research-based dissertation: Lessons learned. *The Qualitative Report, 10*(2), 208-222.

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology, 3*(2), 77-101. doi: 10.1191/1478088706qp063oa

Braziotis, C., Bourlakis, M., Rogers, H., & Tannock, J. (2013). Supply chains and supply networks: Distinctions and overlaps. *Supply Chain Management: An International Journal, 18*(6), 644-652. doi: doi:10.1108/SCM-07-2012-0260

Brink, H. (1993). Validity and reliability in qualitative research. *Curationis, 16*(2), 35-38.

Bruccoleri, M., Cannella, S., & Porta, G. L. (2014). Inventory record inaccuracy in supply chains: The role of workers' behavior. *International Journal of Physical Distribution & Logistics Management, 44*(10), 796-819. doi: doi:10.1108/IJPDLM-09-2013-0240

Bruque-Cámara, S., Moyano-Fuentes, J., & Maqueira-Marín, J. M. (2016). Supply chain integration through community cloud: Effects on operational performance. *Journal of Purchasing and Supply Management, 22*(2), 141-153. doi: http://dx.doi.org/10.1016/j.pursup.2016.04.003

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly, 34*(3), 523-548.

Bunker, G. (2012). Technology is not enough: Taking a holistic view for information assurance. *Information Security Technical Report, 17*(1–2), 19-25. doi: http://dx.doi.org/10.1016/j.istr.2011.12.002

Burnett, G. (2012). Research paradigm choices made by postgraduate students with pacific education research interests in new zealand. *Higher Education Research & Development, 31*(4), 479-492. doi: 10.1080/07294360.2011.559196

Caballero, J., Grier, C., Kreibich, C., & Paxson, V. (2011). *Measuring pay-per-install: The commoditization of malware distribution.* Paper presented at the Usenix security symposium.

Capaldo, A., & Giannoccaro, I. (2015). Interdependence and network-level trust in supply chain networks: A computational study. *Industrial Marketing Management, 44*, 180-195. doi: http://dx.doi.org/10.1016/j.indmarman.2014.10.001

Carlsson, S. A. (2006). *Towards an information systems design research framework: A critical realist perspective.* Paper presented at the Proceedings of the First International Conference on Design Science Research in Information Systems and Technology, Claremont, CA.

CESG. (2010). Busy reader guide for improving information assurance at the enterprise level. 1.0. Retrieved on 08 October, 2015, from https://www.cesg.gov.uk/Pages/Search.aspx?k=improving%20IA

Chang, V., Walters, R. J., & Wills, G. (2013). The development that leads to the cloud computing business framework. *International Journal of Information Management, 33*(3), 524-538. doi: http://dx.doi.org/10.1016/j.ijinfomgt.2013.01.005

Chang, W., Ellinger, A. E., & Blackhurst, J. (2015). A contextual approach to supply chain risk mitigation. *The International Journal of Logistics Management, 26*(3), 642-656. doi: doi:10.1108/IJLM-02-2014-0026

Chauhan, P., Singh, N., & Chandra, N. (2013, 27-29 Sept. 2013). *Security breaches in an organization and their countermeasures.* Paper presented at the 2013 5th International Conference and Computational Intelligence and Communication Networks.

Cheah, K. B. (2015). *Effects of cyber supply chain risk management on supply chain performance.* Universiti Sains Malaysia.

Chen, C.-S., Liang, W.-Y., & Hsu, H.-Y. (2015). A cloud computing platform for erp applications. *Applied Soft Computing, 27*, 127-136. doi: http://dx.doi.org/10.1016/j.asoc.2014.11.009

Chenail, R. J. (2009). Interviewing the investigator: Strategies for addressing instrumentation and researcher bias concerns in qualitative research. *The Qualitative Report, 13*(4), 14-21.

Cherdantseva, Y., & Hilton, J. (2013). *A reference model of information assurance & security.* Paper presented at the Availability, Reliability and Security (ARES), 2013 Eighth International Conference on.

Cherdantseva, Y., & Hilton, J. (2014). Information security and information assurance: Discussion about the meaning, scope, and goals. In P. Irene Maria & A. Fernando (Eds.), *Organizational, legal, and technological dimensions of information system administration* (pp. 167-198). Hershey, PA, USA: IGI Global.

Choi, T. Y., Dooley, K. J., & Rungtusanatham, M. (2001). Supply networks and complex adaptive systems: Control versus emergence. *Journal of Operations Management, 19*(3), 351-366. doi: http://dx.doi.org/10.1016/S0272-6963(00)00068-1

Choo, K.-K. R. (2011). The cyber threat landscape: Challenges and future research directions. *Computers & Security, 30*(8), 719-731. doi: http://dx.doi.org/10.1016/j.cose.2011.08.004

Chopra, S., & Sodhi, M. S. (2004). Managing risk to avoid supply-chain breakdown. *MIT Sloan management review, 46*(1), 53.

Clark, L. S. (2014). Critical theory and constructivism. Retrieved on 16 May, 2017, from http://www.ihrcs.ch/?p=92

Clemons, R., & Slotnick, S. A. (2016). The effect of supply-chain disruption, quality and knowledge transfer on firm strategy. *International Journal of Production Economics, 178*, 169-186. doi: http://dx.doi.org/10.1016/j.ijpe.2016.05.012

Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American sociological review*, 588-608.

Costantino, F., Di Gravio, G., Shaban, A., & Tronci, M. (2015). The impact of information sharing on ordering policies to improve supply chain performances. *Computers & Industrial Engineering, 82*, 127-142. doi: http://dx.doi.org/10.1016/j.cie.2015.01.024

Cousin, G. (2005). Case study research. *Journal of Geography in Higher Education, 29*(3), 421-427. doi: 10.1080/03098260500290967

Cronholm, S., & Göbel, H. (2016). Evaluation of the information systems research framework: Empirical evidence from a design science research project. *Electronic Journal of Information Systems Evaluation, 19*(3), 157-167.

Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M., & Baskerville, R. (2013). Future directions for behavioral information security research. *Computers & Security, 32*, 90-101. doi: http://dx.doi.org/10.1016/j.cose.2012.09.010

Da Veiga, A., & Eloff, J. H. P. (2010). A framework and assessment instrument for information security culture. *Computers & Security, 29*(2), 196-207. doi: http://dx.doi.org/10.1016/j.cose.2009.09.002

Dai, H., Li, J., Yan, N., & Zhou, W. (2016). Bullwhip effect and supply chain costs with low- and high-quality information on inventory shrinkage. *European Journal of Operational Research, 250*(2), 457-469. doi: http://dx.doi.org/10.1016/j.ejor.2015.11.004

Day, J. M. (2014). Fostering emergent resilience: The complex adaptive supply network of disaster relief. *International Journal of Production Research, 52*(7), 1970-1988. doi: 10.1080/00207543.2013.787496

de Mel, S., Herath, D., McKenzie, D., & Pathak, Y. (2016). Radio frequency (un)identification: Results from a proof-of-concept trial of the use of rfid technology to measure microenterprise turnover in sri lanka. *Development Engineering, 1*, 4-11. doi: http://dx.doi.org/10.1016/j.deveng.2015.06.001

de Oliveira, U. R., Marins, F. A. S., Rocha, H. M., & Salomon, V. A. P. (2017). The iso 31000 standard in supply chain risk management. *Journal of Cleaner Production, 151*, 616-633. doi: http://dx.doi.org/10.1016/j.jclepro.2017.03.054

De Ryck, P., Nikiforakis, N., Desmet, L., Piessens, F., & Joosen, W. (2012). Serene: Self-reliant client-side protection against session fixation. In K. M. Göschka & S. Haridi (Eds.), *Distributed applications and interoperable systems: 12th ifip wg 6.1 international conference, dais 2012, stockholm, sweden, june 13-16, 2012. Proceedings* (pp. 59-72). Berlin, Heidelberg: Springer Berlin Heidelberg.

Denolf, J. M., Trienekens, J. H., Wognum, P. M., van der Vorst, J. G. A. J., & Omta, S. W. F. (2015). Towards a framework of critical success factors for implementing supply chain information systems. *Computers in Industry, 68*, 16-26. doi: http://dx.doi.org/10.1016/j.compind.2014.12.012

Díaz, M., Martín, C., & Rubio, B. (2016). State-of-the-art, challenges, and open issues in the integration of internet of things and cloud computing. *Journal of Network and Computer Applications, 67*, 99-117. doi: http://dx.doi.org/10.1016/j.jnca.2016.01.010

Disney, S. M., & Towill, D. R. (2003). The effect of vendor managed inventory (vmi) dynamics on the bullwhip effect in supply chains. *International Journal of Production Economics, 85*(2), 199-215. doi: http://dx.doi.org/10.1016/S0925-5273(03)00110-5

Dowling, C. (2014). A big 4 firm's use of information technology to control the audit process: How an audit support system is changing auditor behavior. *Contemporary Accounting Research, 31*(1), 230-252.

Eamonn, K., & Kelly, M. (2015). Supply chains and value webs. *Business Trends series.* Retrieved on 10 March, 2016, from http://dupress.com/articles/supply-chains-to-value-webs-business-trends/

Eckstein, D., Goellner, M., Blome, C., & Henke, M. (2015). The performance impact of supply chain agility and supply chain adaptability: The moderating effect of product complexity. *International Journal of Production Research, 53*(10), 3028-3046. doi: 10.1080/00207543.2014.970707

Elena, C. A. (2016). Social media – a strategy in developing customer relationship management. *Procedia Economics and Finance, 39*, 785-790. doi: http://dx.doi.org/10.1016/S2212-5671(16)30266-0

Erdil, A., & Öztürk, A. (2016). Improvement a quality oriented model for customer relationship management: A case study for shipment industry in turkey. *Procedia - Social and Behavioral Sciences, 229*, 346-353. doi: http://dx.doi.org/10.1016/j.sbspro.2016.07.145

Eskandarpour, M., Dejax, P., Miemczyk, J., & Péton, O. (2015). Sustainable supply chain network design: An optimization-oriented review. *Omega, 54*, 11-32. doi: http://dx.doi.org/10.1016/j.omega.2015.01.006

Fang, Y., & Shou, B. (2015). Managing supply uncertainty under supply chain cournot competition. *European Journal of Operational Research, 243*(1), 156-176. doi: http://dx.doi.org/10.1016/j.ejor.2014.11.038

Feild, L., Pruchno, R. A., Bewley, J., Edward P. Lemay, J., & Levinsky, N. G. (2006). Using probability vs. Nonprobability sampling to identify hard-to-access participants for health-related research. *Journal of Aging and Health, 18*(4), 565-583. doi: doi:10.1177/0898264306291420

Foulds, S. (2015). Understanding supply chain capabilities: Supply chain logistics. *Transport World Africa, 13*(1), 24-25.

Freedman, K. (1999). Laudan's naturalistic axiology. *Philosophy of Science, 66*, S526-S537.

Fu, Q., & Zhu, K. (2010). Endogenous information acquisition in supply chain management. *European Journal of Operational Research, 201*(2), 454-462. doi: http://dx.doi.org/10.1016/j.ejor.2009.03.019

Fu, X., Dong, M., Liu, S., & Han, G. (2016). Trust based decisions in supply chains with an agent. *Decision Support Systems, 82*, 35-46. doi: http://dx.doi.org/10.1016/j.dss.2015.11.004

Fuchs, L., Pernul, G., & Sandhu, R. (2011). Roles in information security – a survey and classification of the research area. *Computers & Security, 30*(8), 748-769. doi: http://dx.doi.org/10.1016/j.cose.2011.08.002

Fusch, P. I., & Ness, L. R. (2015). Are we there yet? Data saturation in qualitative research. *Qualitative Report, The, 20*(9), 1408.

Ghalenooie, M. B., & Sarvestani, H. K. (2016). Evaluating human factors in customer relationship management case study: Private banks of shiraz city. *Procedia Economics and Finance, 36*, 363-373. doi: http://dx.doi.org/10.1016/S2212-5671(16)30048-X

Ghannam, M. Z. (2017). Challenges and opportunities of having an it disaster recovery plan.

Giddings, L. S., & Grant, B. M. (2006). Mixed methods research for the novice researcher. *Contemporary Nurse, 23*(1), 3-11. doi: 10.5172/conu.2006.23.1.3

Goel, R. (2015). Trusted supply chains: Surveying competitive value of the cloud. *International Journal of Management & Information Systems (Online), 19*(1), 43.

Golafshani, N. (2003). Understanding reliability and validity in qualitative research. *The Qualitative Report, 8*(4), 597-606.

Gordineer, J. (2003). Blended threats: A new era in anti-virus protection. *Information Systems Security, 12*(3), 45-47. doi: 10.1201/1086/43327.12.3.20030701/43626.7

Govindan, K., & Fattahi, M. (2015). Investigating risk and robustness measures for supply chain network design under demand uncertainty: A case study of glass supply chain. *International Journal of Production Economics*.

Greasley, A., & Wang, Y. (2016). Building the hybrid organisation through erp and enterprise social software. *Computers in Industry, 82*, 69-81. doi: http://dx.doi.org/10.1016/j.compind.2016.05.007

Guba, E. G. (1990). *The paradigm dialog*: Sage Publications.

Guba, E. G., & Lincoln, Y. S. (1994). Competing paradigms in qualitative research. *Handbook of qualitative research, 2*(163-194), 105.

Gunasekaran, A., Lai, K.-h., & Edwin Cheng, T. C. (2008). Responsive supply chain: A competitive strategy in a networked economy. *Omega, 36*(4), 549-564. doi: http://dx.doi.org/10.1016/j.omega.2006.12.002

Gunasekaran, A., Papadopoulos, T., Dubey, R., Wamba, S. F., Childe, S. J., Hazen, B., & Akter, S. (2016). Big data and predictive analytics for supply chain and organizational performance. *Journal of Business Research*.

Gunasekaran, A., Subramanian, N., & Rahman, S. (2015). Supply chain resilience: Role of complexities and strategies. *International Journal of Production Research, 53*(22), 6809-6819. doi: 10.1080/00207543.2015.1093667

Gupta, P., Seetharaman, A., & Raj, J. R. (2013). The usage and adoption of cloud computing by small and medium businesses. *International Journal of Information Management, 33*(5), 861-874. doi: http://dx.doi.org/10.1016/j.ijinfomgt.2013.07.001

Hamill, J. T., Deckro, R. F., & Kloeber Jr, J. M. (2005). Evaluating information assurance strategies. *Decision Support Systems, 39*(3), 463-484. doi: http://dx.doi.org/10.1016/j.dss.2003.11.004

Hammersley, M. (2010). Reproducing or constructing? Some questions about transcription in social research. *Qualitative Research, 10*(5), 553-569. doi: 10.1177/1468794110375230

Hariga, M., Gumus, M., & Daghfous, A. (2014). Storage constrained vendor managed inventory models with unequal shipment frequencies. *Omega, 48*, 94-106. doi: http://dx.doi.org/10.1016/j.omega.2013.11.003

Hasani, A., & Khosrojerdi, A. (2016). Robust global supply chain network design under disruption and uncertainty considering resilience strategies: A parallel memetic algorithm for a real-life case study. *Transportation Research Part E: Logistics and Transportation Review, 87*, 20-52. doi: http://dx.doi.org/10.1016/j.tre.2015.12.009

Hathaway, O. A., Crootof, R., Levitz, P., Nix, H., Nowlan, A., Perdue, W., & Spiegel, J. (2012). The law of cyber-attack. *California Law Review, 100*(4), 817-885.

Heartfield, R., & Loukas, G. (2013). On the feasibility of automated semantic attacks in the cloud. In E. Gelenbe & R. Lent (Eds.), *Computer and information sciences iii: 27th international symposium on computer and information sciences* (pp. 343-351). London: Springer London.

Heckmann, I., Comes, T., & Nickel, S. (2015). A critical review on supply chain risk – definition, measure and modeling. *Omega, 52*(0), 119-132. doi: http://dx.doi.org/10.1016/j.omega.2014.10.004

Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design science in information systems research. *MIS Quarterly, 28*(1), 75-105. doi: 10.2307/25148625

Hiba, J. H., Ammar, H. S., Sarah, H., & Azizahbt, H. A. (2015). Big data and five v's characteristics. *International Journal of Advances in Electronics and Computer Science, 2*(1), 16-23.

Hinkka, V., Främling, K., & Tätilä, J. (2013). Supply chain tracking: Aligning buyer and supplier incentives. *Industrial Management & Data Systems, 113*(8), 1133-1148. doi: doi:10.1108/IMDS-12-2012-0439

Ho, W., Zheng, T., Yildiz, H., & Talluri, S. (2015). Supply chain risk management: A literature review. *International Journal of Production Research, 53*(16), 5031-5069. doi: 10.1080/00207543.2015.1030467

Hohenstein, N.-O., Feisel, E., Hartmann, E., & Giunipero, L. (2015). Research on the phenomenon of supply chain resilience: A systematic review and paths for further investigation. *International Journal of Physical Distribution & Logistics Management, 45*(1/2), 90-117. doi: doi:10.1108/IJPDLM-05-2013-0128

Holweg, M., & Pil, F. K. (2008). Theoretical perspectives on the coordination of supply chains. *Journal of Operations Management, 26*(3), 389-406. doi: http://dx.doi.org/10.1016/j.jom.2007.08.003

Hsieh, H.-F., & Shannon, S. E. (2005). Three approaches to qualitative content analysis. *Qualitative health research, 15*(9), 1277-1288.

Hsieh, W. C., Wu, C. C., & Kao, Y. W. (2015, 21-24 Sept. 2015). *A study of android malware detection technology evolution.* Paper presented at the 2015 International Carnahan Conference on Security Technology (ICCST).

Huang, Y.-S., Li, M.-C., & Ho, J.-W. (2016). Determination of the optimal degree of information sharing in a two-echelon supply chain. *International Journal of Production Research, 54*(5), 1518-1534. doi: 10.1080/00207543.2015.1092615

Hugos, M. H. (2010). *Essentials of supply chain management*: Wiley.

Humphrey, C. (2013). A paradigmatic map of professional education research. *Social Work Education, 32*(1), 3-16. doi: 10.1080/02615479.2011.643863

Hunton, P. (2012). Data attack of the cybercriminal: Investigating the digital currency of cybercrime. *Computer Law & Security Review, 28*(2), 201-207. doi: http://dx.doi.org/10.1016/j.clsr.2012.01.007

Ifinedo, P. (2014). Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition. *Information & Management, 51*(1), 69-79. doi: http://dx.doi.org/10.1016/j.im.2013.10.001

Iñigo, E. A., & Albareda, L. (2016). Understanding sustainable innovation as a complex adaptive system: A systemic approach to the firm. *Journal of Cleaner Production, 126*, 1-20. doi: http://dx.doi.org/10.1016/j.jclepro.2016.03.036

Isaksson, O. H. D., & Seifert, R. W. (2016). Quantifying the bullwhip effect using two-echelon data: A cross-industry empirical investigation. *International Journal of Production Economics, 171, Part 3*, 311-320. doi: http://dx.doi.org/10.1016/j.ijpe.2015.08.027

Issac, B., Chiong, R., & Jacob, S. M. (2014). Analysis of phishing attacks and countermeasures. *arXiv preprint arXiv:1410.4672.*

Ivanov, D., Sokolov, B., & Dolgui, A. (2014). The ripple effect in supply chains: Trade-off 'efficiency-flexibility-resilience' in disruption management. *International*

Journal of Production Research, 52(7), 2154-2172. doi: 10.1080/00207543.2013.858836

Ivanov, D., Sokolov, B., & Kaeschel, J. (2010). A multi-structural framework for adaptive supply chain planning and operations control with structure dynamics considerations. *European Journal of Operational Research, 200*(2), 409-420. doi: http://dx.doi.org/10.1016/j.ejor.2009.01.002

Jain, V., Wadhwa, S., & Deshmukh, S. G. (2009). Revisiting information systems to support a dynamic supply chain: Issues and perspectives. *Production Planning & Control, 20*(1), 17-29. doi: 10.1080/09537280802608019

Jajoo, P., Singh, G., & Nehra, M. S. (2013). Identification and forensic investigation of network intruders based on honeynet. *Network, 3*(6), 240-246.

James, M., Grosvenor, R., & Prickett, P. (2004). E-distribution: Internet-based management of a merchandiser supply chain. *Supply Chain Management: An International Journal, 9*(1), 7-15. doi: doi:10.1108/13598540410517539

Jardini, B., Kyal, M. E., & Amri, M. (2016, 23-25 May 2016). *The management of the supply chain by the jit system (just in time) and the edi technology (electronic data interchange).* Paper presented at the 2016 3rd International Conference on Logistics Operations Management (GOL).

Jayawickrama, U., Liu, S., & Hudson Smith, M. (2016). Empirical evidence of an integrative knowledge competence framework for erp systems implementation in uk industries. *Computers in Industry, 82*, 205-223. doi: http://dx.doi.org/10.1016/j.compind.2016.07.005

Jede, A., & Teuteberg, F. (2015). Integrating cloud computing in supply chain processes: A comprehensive literature review. *Journal of Enterprise Information Management, 28*(6), 872-904.

Johnson, B. E. (2011). The speed and accuracy of voice recognition software-assisted transcription versus the listen-and-type method: A research note. *Qualitative Research, 11*(1), 91-97.

Jomaa, D., Monteiro, T., & Besombes, B. (2013). Design and development of a forecasting module: Case of a warehouse management system. *IFAC Proceedings Volumes, 46*(24), 177-182. doi: https://doi.org/10.3182/20130911-3-BR-3021.00013

Jordan, E., Gross, M. E., Javernick-Will, A. N., & Garvin, M. J. (2011). Use and misuse of qualitative comparative analysis. *Construction Management and Economics, 29*(11), 1159-1173. doi: 10.1080/01446193.2011.640339

Jouini, M., Rabai, L. B. A., & Aissa, A. B. (2014). Classification of security threats in information systems. *Procedia Computer Science, 32*, 489-496. doi: http://dx.doi.org/10.1016/j.procs.2014.05.452

Kandananond, K. (2014). A roadmap to green supply chain system through enterprise resource planning (erp) implementation. *Procedia Engineering, 69*, 377-382. doi: http://dx.doi.org/10.1016/j.proeng.2014.03.002

Karabacak, B., & Sogukpinar, I. (2005). Isram: Information security risk analysis method. *Computers & Security, 24*(2), 147-159. doi: http://dx.doi.org/10.1016/j.cose.2004.07.004

Karimi, N., & Davoudpour, H. (2016). Integrated production and delivery scheduling for multi-factory supply chain with stage-dependent inventory holding cost. *Computational and Applied Mathematics*, 1-16. doi: 10.1007/s40314-016-0305-0

Kembro, J., & Selviaridis, K. (2015). Exploring information sharing in the extended supply chain: An interdependence perspective. *Supply Chain Management: An International Journal, 20*(4), 455-470. doi: doi:10.1108/SCM-07-2014-0252

Kenyon, G. N., Meixell, M. J., & Westfall, P. H. (2016). Production outsourcing and operational performance: An empirical study using secondary data. *International Journal of Production Economics, 171, Part 3*, 336-349. doi: http://dx.doi.org/10.1016/j.ijpe.2015.09.017

Khalifehzadeh, S., Seifbarghy, M., & Naderi, B. (2015). A four-echelon supply chain network design with shortage: Mathematical modeling and solution methods. *Journal of Manufacturing Systems, 35*, 164-175. doi: http://dx.doi.org/10.1016/j.jmsy.2014.12.002

Khan, S. A. R., Li, D. Q., & Yu, M. Z. (2015). Analysis and usage: Cloud computing technology in the supply chain management. *Life science journal, Zhengzhou University, 12*.

Ko, C.-H., Pan, N.-F., & Chiou, C.-C. (2013). Web-based radio frequency identification facility management systems. *Structure and Infrastructure Engineering, 9*(5), 465-480. doi: 10.1080/15732479.2010.546804

Koçoğlu, İ., İmamoğlu, S. Z., İnce, H., & Keskin, H. (2011). The effect of supply chain integration on information sharing:Enhancing the supply chain performance. *Procedia - Social and Behavioral Sciences, 24*(0), 1630-1649. doi: http://dx.doi.org/10.1016/j.sbspro.2011.09.016

Kolkowska, E., & Dhillon, G. (2013). Organizational power and information security rule compliance. *Computers & Security, 33*, 3-11. doi: http://dx.doi.org/10.1016/j.cose.2012.07.001

Koppell, J. (2011). International organization for standardization. *Handb. Transnatl. Gov. Inst. Innov, 41*(8), 289.

Krishna, G. J., & Ravi, V. (2016). Evolutionary computing applied to customer relationship management: A survey. *Engineering Applications of Artificial Intelligence, 56*, 30-59. doi: http://dx.doi.org/10.1016/j.engappai.2016.08.012

Lacey, A., & Luff, D. (2009). *Qualitative data analysis*: Trent Focus Sheffield.

Lam, H. Y., Choy, K. L., Ho, G. T. S., Cheng, S. W. Y., & Lee, C. K. M. (2015). A knowledge-based logistics operations planning system for mitigating risk in warehouse order fulfillment. *International Journal of Production Economics, 170, Part C*, 763-779. doi: http://dx.doi.org/10.1016/j.ijpe.2015.01.005

Lambert, D. M., & Cooper, M. C. (2000). Issues in supply chain management. *Industrial Marketing Management, 29*(1), 65-83. doi: 10.1016/s0019-8501(99)00113-3

Lee, J.-Y., Cho, R. K., & Paik, S.-K. (2016). Supply chain coordination in vendor-managed inventory systems with stockout-cost sharing under limited storage capacity. *European Journal of Operational Research, 248*(1), 95-106. doi: http://dx.doi.org/10.1016/j.ejor.2015.06.080

Lehner, O. M., & Kansikas, J. (2013). Pre-paradigmatic status of social entrepreneurship research: A systematic literature review. *Journal of Social Entrepreneurship, 4*(2), 198-219. doi: 10.1080/19420676.2013.777360

Lei, Q., Chen, J., Wei, X., & Lu, S. (2015). Supply chain coordination under asymmetric production cost information and inventory inaccuracy. *International Journal of Production Economics, 170, Part A*, 204-218. doi: http://dx.doi.org/10.1016/j.ijpe.2015.09.015

Lemmens, S., Decouttere, C., Vandaele, N., & Bernuzzi, M. (2016). A review of integrated supply chain network design models: Key issues for vaccine supply chains. *Chemical Engineering Research and Design, 109*, 366-384. doi: http://dx.doi.org/10.1016/j.cherd.2016.02.015

Li, G., Fan, H., Lee, P. K. C., & Cheng, T. C. E. (2015). Joint supply chain risk management: An agency and collaboration perspective. *International Journal of*

Production Economics, 164, 83-94. doi: http://dx.doi.org/10.1016/j.ijpe.2015.02.021

Li, G., Ji, P., Sun, L. Y., & Lee, W. B. (2009). Modeling and simulation of supply network evolution based on complex adaptive system and fitness landscape. *Computers & Industrial Engineering, 56*(3), 839-853. doi: http://dx.doi.org/10.1016/j.cie.2008.09.039

Li, G., Yang, H., Sun, L., Ji, P., & Feng, L. (2010). The evolutionary complexity of complex adaptive supply networks: A simulation and case study. *International Journal of Production Economics, 124*(2), 310-330. doi: http://dx.doi.org/10.1016/j.ijpe.2009.11.027

Li, S., & Lin, B. (2006). Accessing information sharing and information quality in supply chain management. *Decision Support Systems, 42*(3), 1641-1656. doi: http://dx.doi.org/10.1016/j.dss.2006.02.011

Li, W., Yin, J., & Chen, H. (2016, 28-30 Sept. 2016). *Targeting key data breach services in underground supply chain.* Paper presented at the 2016 IEEE Conference on Intelligence and Security Informatics (ISI).

Lichtman, M. (2013). Chapter 12: Making meaning from your data. In M. Lichtman (Ed.), *Qualitative research in education: A user's guide* (3rd ed ed., pp. 241-268). Thousand Oaks, Calif: SAGE Publications.

Lin, I.-C., Hsu, H.-H., & Cheng, C.-Y. (2015). A cloud-based authentication protocol for rfid supply chain systems. *Journal of Network and Systems Management, 23*(4), 978-997.

Lysne, O., Hole, K. J., Otterstad, C., Ø, Y., Aarseth, R., & Tellnes, J. (2016). Vendor malware: Detection limits and mitigation. *Computer, 49*(8), 62-69. doi: 10.1109/MC.2016.227

MacCarthy, B. L., Blome, C., Olhager, J., Srai, J. S., & Zhao, X. (2016). Supply chain evolution–theory, concepts and science. *International Journal of Operations and Production Management.*

Macharia, C. W., & Ismail, N. (2015). Role of electronic data interchange on supply chain performance in manufacturing sector in kenya: A case of bidco oil refinery. *International Academic Journal of Procurement and Supply Chain Management, 1*(4), 1-11.

Maconachy, W. V., Schou, C. D., Ragsdale, D., & Welch, D. (2001). *A model for information assurance: An integrated approach.* Paper presented at the Proceedings of the 2001 IEEE Workshop on Information Assurance and Security.

Maharaj, M., & Ajayi, N. (2011). *Information risk management within supply chains.* (Master's Degree Thesis), University of KwaZulu-Natal. Retrieved from http://researchspace.ukzn.ac.za/handle/10413/9650

March, S. T., & Smith, G. F. (1995). Design and natural science research on information technology. *Decision Support Systems, 15*(4), 251-266. doi: http://dx.doi.org/10.1016/0167-9236(94)00041-2

Margaret, R., Sharon, Z., & Jeff, C. (2014, October 2014). Electronic data interchange (edi). *TechTarget.* Retrieved on 5 October, 2016, from http://searchdatacenter.techtarget.com/definition/EDI

Marinagi, C., Trivellas, P., & Sakas, D. P. (2014). The impact of information technology on the development of supply chain competitive advantage. *Procedia - Social and Behavioral Sciences, 147*, 586-591. doi: http://dx.doi.org/10.1016/j.sbspro.2014.07.161

Martin, N., & Rice, J. (2011). Cybercrime: Understanding and addressing the concerns of stakeholders. *Computers & Security, 30*(8), 803-814. doi: http://dx.doi.org/10.1016/j.cose.2011.07.003

Mateen, A., & Chatterjee, A. K. (2015). Vendor managed inventory for single-vendor multi-retailer supply chains. *Decision Support Systems, 70*, 31-41. doi: http://dx.doi.org/10.1016/j.dss.2014.12.002

McCormack, K., Wilkerson, T., Marrow, D., Davey, M., Shah, M., & Yee, D. (2008). Managing risk in your organization with the scor methodology. *The Supply Chain Council Risk Research Team, 0*(0).

Merriam, S. (1995). What can you tell from an n ofl?: Issues of validity and reliability in qualitative research. *PAACE Journal of lifelong learning, 4*, 50-60.

Miller, F., & Drake, A. (2016). Using information asymmetry to mitigate hold-ups in supply chains. *Management Accounting Research, 32*, 16-26. doi: http://dx.doi.org/10.1016/j.mar.2015.11.001

Mitchell, E. M., & Kovach, J. V. (2016). Improving supply chain information sharing using design for six sigma. *European Research on Management and Business Economics, 22*(3), 147-154. doi: http://dx.doi.org/10.1016/j.iedee.2015.02.002

Mittelstädt, V., Brauner, P., Blum, M., & Ziefle, M. (2015). On the visual design of erp systems the – role of information complexity, presentation and human factors. *Procedia Manufacturing, 3*, 448-455. doi: http://dx.doi.org/10.1016/j.promfg.2015.07.207

Mizgier, K. J., Wagner, S. M., & Jüttner, M. P. (2015). Disentangling diversification in supply chain networks. *International Journal of Production Economics, 162*(0), 115-124. doi: http://dx.doi.org/10.1016/j.ijpe.2015.01.007

Montesdioca, G. P. Z., & Maçada, A. C. G. (2015). Measuring user satisfaction with information security practices. *Computers & Security, 48*, 267-280. doi: http://dx.doi.org/10.1016/j.cose.2014.10.015

Morris, B., Tanner, C., & Alessandro, J. D. (2010, 12-14 April 2010). *Enabling trust through continuous compliance assurance.* Paper presented at the 2010 Seventh International Conference on Information Technology: New Generations.

Morse, J. M., Barrett, M., Mayan, M., Olson, K., & Spiers, J. (2002). Verification strategies for establishing reliability and validity in qualitative research. *International Journal of Qualitative Methods, 1*(2), 13-22. doi: doi:10.1177/160940690200100202

Mujeye, S., Levy, Y., & Mattord, H. (2016). Empirical results of an experimental study on the role of password strength and cognitive load on employee productivity. *Online Journal of Applied Knowledge Management, 4*(1), 99.

Musawa, M. S., & Wahab, E. (2012). The adoption of electronic data interchange (edi) technology by nigerian smes: A conceptual framework. *Journal of Business Management and Economics, 3*(2), 055-068.

Nagamalai, D., Dhinakaran, B. C., Ozcan, A., Okatan, A., & Lee, J.-K. (2014). Empirical study of email security threats and countermeasures *Networks and communications (netcom2013)* (pp. 229-242): Springer.

Nalzaro, L. (2012, June 9, 2012). Theoretical & conceptual framework. Retrieved on 5 February, 2017, from https://www.slideshare.net/ludymae/chapter-6theoretical-conceptual-framework

Narasimhan, R., & Talluri, S. (2009). Perspectives on risk management in supply chains. *Journal of Operations Management, 27*(2), 114-118. doi: http://dx.doi.org/10.1016/j.jom.2009.02.001

Netessine, S., & Rudi, N. (2004). *Supply chain structures on the internet and the role of marketingoperations interaction. In "handbook of quantitative supply chain analysis: Modeling in the ebusiness era," d. Simchi-levi, sd wu and m. Shen, eds*: Kluwer.

Neureuther, B. D., & Kenyon, G. (2009). Mitigating supply chain vulnerability. *Journal of Marketing Channels, 16*(3), 245-263. doi: 10.1080/10466690902934532

Nishat Faisal, M., Banwet, D. K., & Shankar, R. (2007). Information risks management in supply chains: An assessment and mitigation framework. *Journal of Enterprise Information Management, 20*(6), 677-699. doi: doi:10.1108/17410390710830727

Noble, H., & Smith, J. (2015). Issues of validity and reliability in qualitative research. *Evidence Based Nursing*. doi: 10.1136/eb-2015-102054

Olivier, C., von Solms, R., & Cowley, L. (2006). Information integrity assurance for networks: Let's learn from the financial model. *Computer Fraud & Security, 2006*(8), 7-14. doi: http://dx.doi.org/10.1016/S1361-3723(06)70409-2

Omar, B., & Ballal, T. (2009). Intelligent wireless web services: Context-aware computing in construction-logistics supply chain. *ITcon, 14*(Specia), 289-308.

Ouedraogo, M., Khadraoui, D., Mouratidis, H., & Dubois, E. (2012). Appraisal and reporting of security assurance at operational systems level. *Journal of Systems and Software, 85*(1), 193-208. doi: http://dx.doi.org/10.1016/j.jss.2011.08.013

Park, K., Min, H., & Min, S. (2016). Inter-relationship among risk taking propensity, supply chain security practices, and supply chain disruption occurrence. *Journal of Purchasing and Supply Management, 22*(2), 120-130. doi: http://dx.doi.org/10.1016/j.pursup.2015.12.001

Park, Y., Hong, P., & Roh, J. J. (2013). Supply chain lessons from the catastrophic natural disaster in japan. *Business Horizons, 56*(1), 75-85. doi: http://doi.org/10.1016/j.bushor.2012.09.008

Parker, I. (2013). Discourse analysis: Dimensions of critique in psychology. *Qualitative Research in Psychology, 10*(3), 223-239. doi: 10.1080/14780887.2012.741509

Pasandideh, S. H. R., Niaki, S. T. A., & Asadi, K. (2015). Optimizing a bi-objective multi-product multi-period three echelon supply chain network with warehouse reliability. *Expert Systems with Applications, 42*(5), 2615-2623. doi: http://dx.doi.org/10.1016/j.eswa.2014.11.018

Patel, S. (2015, July 15, 2015). The research paradigm – methodology, epistemology and ontology – explained in simple language. Retrieved on 08 May, 2017, from http://salmapatel.co.uk/academia/the-research-paradigm-methodology-epistemology-and-ontology-explained-in-simple-language

Patil, Y. R. (2016). Feasibility study of just in time inventory management on construction project. *International Research Journal of Multidisciplinary Studies, 2*(3).

Pawar, K., & Rogers, H. (2013). Contextualising the holistic cost of uncertainty in outsourcing manufacturing supply chains. *Production Planning & Control, 24*(7), 607-620. doi: 10.1080/09537287.2012.659872

Pedroso, M. C., & Nakano, D. (2009). Knowledge and information flows in supply chains: A study on pharmaceutical companies. *International Journal of Production Economics, 122*(1), 376-384. doi: http://dx.doi.org/10.1016/j.ijpe.2009.06.012

Peffers, K., Tuunanen, T., Rothenberger, M. A., & Chatterjee, S. (2007). A design science research methodology for information systems research. *Journal of Management Information Systems, 24*(3), 45-77. doi: 10.2307/40398896

Pérez-Aróstegui, M. N., Bustinza-Sánchez, F., & Barrales-Molina, V. (2015). Exploring the relationship between information technology competence and quality management. *BRQ Business Research Quarterly, 18*(1), 4-17. doi: http://dx.doi.org/10.1016/j.brq.2013.11.003

Perez-Castillo, R., & Piattini, M. (2013). *Information audit training in computer science as a serious game.* Paper presented at the EDULEARN13 Proceedings.

Petersen, H. L., & Lemke, F. (2015). Mitigating reputational risks in supply chains. *Supply Chain Management: An International Journal, 20*(5), 495-510. doi: doi:10.1108/SCM-09-2014-0320

Pfeiffer, H. K. (2012). *The diffusion of electronic data interchange*: Springer Science & Business Media.

Philip Chen, C. L., & Zhang, C.-Y. (2014). Data-intensive applications, challenges, techniques and technologies: A survey on big data. *Information Sciences, 275*, 314-347. doi: http://dx.doi.org/10.1016/j.ins.2014.01.015

Piderit, R., Flowerday, S., & Von Solms, R. (2011). Enabling information sharing by establishing trust in supply chains: A case study in the south african automotive industry: Original research. *South African Journal of Information Management, 13*(1), 1-8.

Pop, P. C., Pintea, C.-M., Pop Sitar, C., & Hajdu-Măcelaru, M. (2015). An efficient reverse distribution system for solving sustainable supply chain network design problem. *Journal of Applied Logic, 13*(2, Part A), 105-113. doi: http://dx.doi.org/10.1016/j.jal.2014.11.004

Porterfield, T. E., Macdonald, J. R., & Griffis, S. E. (2012). An exploration of the relational effects of supply chain disruptions. *Transportation Journal, 51*(4), 399-427.

Prajogo, D., Oke, A., & Olhager, J. (2016). Supply chain processes: Linking supply logistics integration, supply performance, lean processes and competitive performance. *International Journal of Operations & Production Management, 36*(2), 220-238. doi: doi:10.1108/IJOPM-03-2014-0129

Protopappa-Sieke, M., Sieke, M. A., & Thonemann, U. W. (2016). Optimal two-period inventory allocation under multiple service level contracts. *European Journal of Operational Research, 252*(1), 145-155. doi: http://dx.doi.org/10.1016/j.ejor.2016.01.013

Qrunfleh, S., & Tarafdar, M. (2013). Lean and agile supply chain strategies and supply chain responsiveness: The role of strategic supplier partnership and postponement. *Supply Chain Management: An International Journal, 18*(6), 571-582. doi: doi:10.1108/SCM-01-2013-0015

Rached, M., Bahroun, Z., & Campagne, J.-P. (2015). Assessing the value of information sharing and its impact on the performance of the various partners in supply chains. *Computers & Industrial Engineering, 88*, 237-253. doi: http://dx.doi.org/10.1016/j.cie.2015.07.007

Rajesh, B., Reddy, Y. J., & Reddy, B. D. K. (2015). A survey paper on malicous computer worms. *International Journal of Advanced Research in Computer Science and Technology, 3*.

Ramdeen, C. D., Santos, J., & Chatfield, H. K. (2011). The usage of electronic data interchange in the hotel industry. *International Journal of Hospitality & Tourism Administration, 12*(2), 95-122. doi: 10.1080/15256480.2011.564491

Regattieri, A., & Santarelli, G. (2013). *Manufacturing logistics and packaging management using rfid.*

Ritchie, J., Lewis, J., Nicholls, C. M., & Ormston, R. (2003). *Qualitative research practice: A guide for social science students and researchers*: Sage.

Romi, I. M. (2014). Information reach and range impact on interorganizational systems platforms. *Intelligent Information Management, 6*(1), 1-7.

Rosenthal, M. (2016). Qualitative research methods: Why, when, and how to conduct interviews and focus groups in pharmacy research. *Currents in Pharmacy Teaching and Learning, 8*(4), 509-516. doi: http://dx.doi.org/10.1016/j.cptl.2016.03.021

Roy, A., Gupta, A. D., & Deshmukh, S. G. (2012, 10-13 Dec. 2012). *Information security in supply chains; a process framework.* Paper presented at the 2012 IEEE International Conference on Industrial Engineering and Engineering Management.

Roy, A., & Kundu, A. (2012). Management of information security in supply chains-a process framework. *CIE42 Proceedings*, 16-18.

Ryan, A. B. (2006). Methodology: Analysing qualitative data and writing up your findings. *Researching and Writing your thesis: a guide for postgraduate students*, 92-108.

Ryu, S.-J., Tsukishima, T., & Onari, H. (2009). A study on evaluation of demand information-sharing methods in supply chain. *International Journal of Production Economics, 120*(1), 162-175.

Sabitha, D., Rajendran, C., Kalpakam, S., & Ziegler, H. (2016). The value of information sharing in a serial supply chain with ar(1) demand and non-zero replenishment lead times. *European Journal of Operational Research, 255*(3), 758-777. doi: http://dx.doi.org/10.1016/j.ejor.2016.05.016

Schoenherr, T. (2010). Outsourcing decisions in global supply chains: An exploratory multi-country survey. *International Journal of Production Research, 48*(2), 343-378. doi: 10.1080/00207540903174908

Sekaran, U. (2006). *Research methods for business: A skill building approach, 4th ed*: Wiley India Pvt. Limited.

Seth, M., Goyal, D. P., & Kiran, R. (2015). Development of a model for successful implementation of supply chain management information system in indian automotive industry. *Vision: The Journal of Business Perspective, 19*(3), 248-262. doi: 10.1177/0972262915599465

Shao, X.-F. (2013). Supply chain characteristics and disruption mitigation capability: An empirical investigation in china. *International Journal of Logistics Research and Applications, 16*(4), 277-295. doi: 10.1080/13675567.2013.815695

Siddiqui, A. W., & Raza, S. A. (2015). Electronic supply chains: Status & perspective. *Computers & Industrial Engineering, 88*, 536-556. doi: http://dx.doi.org/10.1016/j.cie.2015.08.012

Simchi-Levi, D., Kaminsky, P., & Simchi-Levi, E. (2004). *Managing the supply chain: Definitive guide*: McGraw-Hill Education (India) Pvt Limited.

Simon, M. (2011). Analysis of qualitative data. *Dissertation and Scholarly Research: Recipes for Succees. Seattle: LLC.*

Sindhuja, P. (2014). Impact of information security initiatives on supply chain performance: An empirical investigation. *Information Management & Computer Security, 22*(5), 450-473. doi: doi:10.1108/IMCS-05-2013-0035

Sindhuja, P. N., & Kunnathur, A. S. (2015). Information security in supply chains: A management control perspective. *Information and Computer Security, 23*(5), 476-496. doi: doi:10.1108/ICS-07-2014-0050

Singh, A., Mishra, N., Ali, S. I., Shukla, N., & Shankar, R. (2015). Cloud computing technology: Reducing carbon footprint in beef supply chain. *International Journal of Production Economics, 164*, 462-471. doi: http://dx.doi.org/10.1016/j.ijpe.2014.09.019

Singh, A., & Teng, J. T. C. (2016). Enhancing supply chain outcomes through information technology and trust. *Computers in Human Behavior, 54*, 290-300. doi: http://dx.doi.org/10.1016/j.chb.2015.07.051

Singh, A. N., Gupta, M. P., & Ojha, A. (2014). Identifying factors of "organizational information security management". *Journal of Enterprise Information Management, 27*(5), 644-667. doi: doi:10.1108/JEIM-07-2013-0052

Smith, J. A. (2015). *Qualitative psychology: A practical guide to research methods*: Sage.

Soltani, Z., & Navimipour, N. J. (2016). Customer relationship management mechanisms: A systematic review of the state of the art literature and recommendations for future research. *Computers in Human Behavior, 61*, 667-688. doi: http://dx.doi.org/10.1016/j.chb.2016.03.008

Son, I., Lee, D., Lee, J.-N., & Chang, Y. B. (2014). Market perception on cloud computing initiatives in organizations: An extended resource-based view. *Information & Management, 51*(6), 653-669. doi: http://dx.doi.org/10.1016/j.im.2014.05.006

Souto-Manning, M. (2014). Critical narrative analysis: The interplay of critical discourse and narrative analyses. *International Journal of Qualitative Studies in Education, 27*(2), 159-180. doi: 10.1080/09518398.2012.737046

Speier, C., Whipple, J. M., Closs, D. J., & Voss, M. D. (2011). Global supply chain design considerations: Mitigating product safety and security risks. *Journal of Operations Management, 29*(7–8), 721-736. doi: http://dx.doi.org/10.1016/j.jom.2011.06.003

Spekman, R., Davis, E. W., & Ellinger, A. (2016). The extended enterprise: A decade later. *International Journal of Physical Distribution & Logistics Management, 46*(1).

Stefansson, G. (2002). Business-to-business data sharing: A source for integration of supply chains. *International Journal of Production Economics, 75*(1–2), 135-146. doi: http://dx.doi.org/10.1016/S0925-5273(01)00187-6

Stevens, G. C., & Johnson, M. (2016). Integrating the supply chain … 25 years on. *International Journal of Physical Distribution & Logistics Management, 46*(1), 19-42. doi: doi:10.1108/IJPDLM-07-2015-0175

Stokes, J. W., Karampatziakis, N., Platt, J. C., Thomas, A. F., & Marinescu, A. M. (2014). Graph-based malware classification based on file relationships: Google Patents.

Stroud, R. (2014). Vendor risk management using cobit 5. *EDPACS, 50*(1), 11-17. doi: 10.1080/07366981.2014.922837

Sulaiman, M. A., Baharum, M. A. A., & Ridzuan, A. (2014). Customer relationship management (crm) strategies practices in malaysia retailers. *Procedia - Social and Behavioral Sciences, 130*, 354-361. doi: http://dx.doi.org/10.1016/j.sbspro.2014.04.042

Sung, P.-C., Ku, C.-Y., & Su, C.-Y. (2014). Understanding the propagation dynamics of multipartite computer virus. *Industrial Management & Data Systems, 114*(1), 86-106. doi: doi:10.1108/IMDS-04-2013-0197

Surana, A., Kumara *, S., Greaves, M., & Raghavan, U. N. (2005). Supply-chain networks: A complex adaptive systems perspective. *International Journal of Production Research, 43*(20), 4235-4265. doi: 10.1080/00207540500142274

Surbhi, S. (2016). Difference between probability and non-probability sampling. *Key Differences.* Retrieved on 12 June, 2017, from http://keydifferences.com/difference-between-probability-and-non-probability-sampling.html

Syntetos, A. A., Babai, Z., Boylan, J. E., Kolassa, S., & Nikolopoulos, K. (2016). Supply chain forecasting: Theory, practice, their gap and the future. *European Journal of Operational Research, 252*(1), 1-26. doi: http://dx.doi.org/10.1016/j.ejor.2015.11.010

Tan, K. C. (2001). A framework of supply chain management literature. *European Journal of Purchasing & Supply Management, Vol. 7*, 39-48.

Tang, C., & Tomlin, B. (2008). The power of flexibility for mitigating supply chain risks. *International Journal of Production Economics, 116*(1), 12-27. doi: http://dx.doi.org/10.1016/j.ijpe.2008.07.008

Tang, C. S. (2006). Perspectives in supply chain risk management. *International Journal of Production Economics, 103*(2), 451-488. doi: http://dx.doi.org/10.1016/j.ijpe.2005.12.006

Tatoglu, E., Bayraktar, E., Golgeci, I., Koh, S. C. L., Demirbag, M., & Zaim, S. (2016). How do supply chain management and information systems practices influence operational performance? Evidence from emerging country smes. *International Journal of Logistics Research and Applications, 19*(3), 181-199. doi: 10.1080/13675567.2015.1065802

Thakur, R., & Workman, L. (2016). Customer portfolio management (cpm) for improved customer relationship management (crm): Are your customers platinum, gold, silver, or bronze? *Journal of Business Research, 69*(10), 4095-4102. doi: http://dx.doi.org/10.1016/j.jbusres.2016.03.042

Thomas, P. (2010). Research methodology and design (pp. 291-334). University of South Africa.

Thomé, A. M. T., Scavarda, L. F., Scavarda, A., & Thomé, F. E. S. d. S. (2016). Similarities and contrasts of complexity, uncertainty, risks, and resilience in supply chains and temporary multi-organization projects. *International Journal of Project Management, 34*(7), 1328-1346. doi: http://dx.doi.org/10.1016/j.ijproman.2015.10.012

Todo, Y., Nakajima, K., & Matous, P. (2015). How do supply chain networks affect the resilience of firms to natural disasters? Evidence from the great east japan earthquake. *Journal of Regional Science, 55*(2), 209-229. doi: 10.1111/jors.12119

Tong, P. Y., & Crosno, J. L. (2016). Are information asymmetry and sharing good, bad, or context dependent? A meta-analytic review. *Industrial Marketing Management, 56*, 167-180. doi: http://dx.doi.org/10.1016/j.indmarman.2015.11.004

Trifonas, P. P. (2009). Deconstructing research: Paradigms lost. *International Journal of Research & Method in Education, 32*(3), 297-308. doi: 10.1080/17437270903259824

Triznova, M., Maťova, H., Dvoracek, J., & Sadek, S. (2015). Customer relationship management based on employees and corporate culture. *Procedia Economics and Finance, 26*, 953-959. doi: http://dx.doi.org/10.1016/S2212-5671(15)00914-4

Tseng, K.-K., Lo, J., Liu, Y., Chang, S.-H., Merabti, M., Ng, F. C. K., & Wu, C. H. (2016). A feasibility study of stateful automaton packet inspection for streaming application detection systems. *Enterprise Information Systems*, 1-20. doi: 10.1080/17517575.2016.1234070

Tuncel, G., & Alpan, G. (2010). Risk assessment and management for supply chain networks: A case study. *Computers in Industry, 61*(3), 250-259. doi: http://dx.doi.org/10.1016/j.compind.2009.09.008

Vilko, J., Ritala, P., & Edelmann, J. (2014). On uncertainty in supply chain risk management. *The International Journal of Logistics Management, 25*(1), 3-19. doi: doi:10.1108/IJLM-10-2012-0126

Wagner, S. M., & Bode, C. (2006). An empirical investigation into supply chain vulnerability. *Journal of Purchasing and Supply Management, 12*(6), 301-312. doi: http://dx.doi.org/10.1016/j.pursup.2007.01.004

Wakolbinger, T., & Cruz, J. M. (2011). Supply chain disruption risk management through strategic information acquisition and sharing and risk-sharing contracts. *International Journal of Production Research, 49*(13), 4063-4084. doi: 10.1080/00207543.2010.501550

Wang, G., Gunasekaran, A., Ngai, E. W. T., & Papadopoulos, T. (2016a). Big data analytics in logistics and supply chain management: Certain investigations for research and applications. *International Journal of Production Economics, 176*, 98-110. doi: http://dx.doi.org/10.1016/j.ijpe.2016.03.014

Wang, H., Mastragostino, R., & Swartz, C. L. E. (2016b). Flexibility analysis of process supply chain networks. *Computers & Chemical Engineering, 84*, 409-421. doi: http://dx.doi.org/10.1016/j.compchemeng.2015.07.016

Wang, N., Liang, H., Jia, Y., Ge, S., Xue, Y., & Wang, Z. (2016c). Cloud computing research in the is discipline: A citation/co-citation analysis. *Decision Support Systems, 86*, 35-47. doi: http://dx.doi.org/10.1016/j.dss.2016.03.006

Wang, N., Lu, J., Feng, G., Ma, Y., & Liang, H. (2016d). The bullwhip effect on inventory under different information sharing settings based on price-sensitive demand. *International Journal of Production Research, 54*(13), 4043-4064. doi: 10.1080/00207543.2016.1171418

Wang, X., & Disney, S. M. (2016). The bullwhip effect: Progress, trends and directions. *European Journal of Operational Research, 250*(3), 691-701. doi: http://dx.doi.org/10.1016/j.ejor.2015.07.022

Wiengarten, F., Humphreys, P., Gimenez, C., & McIvor, R. (2016). Risk, risk management practices, and the success of supply chain integration. *International Journal of Production Economics, 171, Part 3*, 361-370. doi: http://dx.doi.org/10.1016/j.ijpe.2015.03.020

Windelberg, M. (2016). Objectives for managing cyber supply chain risk. *International Journal of Critical Infrastructure Protection, 12*, 4-11. doi: http://dx.doi.org/10.1016/j.ijcip.2015.11.003

Wolden, M., Valverde, R., & Talla, M. (2015). The effectiveness of cobit 5 information security framework for reducing cyber attacks on supply chain management system. *IFAC-PapersOnLine, 48*(3), 1846-1852.

Workman, M., Bommer, W. H., & Straub, D. (2008). Security lapses and the omission of information security measures: A threat control model and empirical test. *Computers in Human Behavior, 24*(6), 2799-2816. doi: http://dx.doi.org/10.1016/j.chb.2008.04.005

Wu, X., & Subramaniam, C. (2011). Understanding and predicting radio frequency identification (rfid) adoption in supply chains. *Journal of Organizational Computing and Electronic Commerce, 21*(4), 348-367. doi: 10.1080/10919392.2011.614203

Xiao-yan, G., Yu-qing, Y., & Li-lei, L. (2011). An information security maturity evaluation mode. *Procedia Engineering, 24*, 335-339. doi: http://dx.doi.org/10.1016/j.proeng.2011.11.2652

Xing, K., Qian, W., & Zaman, A. U. (2016). Development of a cloud-based platform for footprint assessment in green supply chain management. *Journal of Cleaner Production, 139*, 191-203. doi: http://dx.doi.org/10.1016/j.jclepro.2016.08.042

Xue, L., Zhang, C., Ling, H., & Zhao, X. (2013). Risk mitigation in supply chain digitization: System modularity and information technology governance. *Journal of Management Information Systems, 30*(1), 325-352. doi: 10.2753/MIS0742-1222300110

Yang, C., Huang, Q., Li, Z., Liu, K., & Hu, F. (2016). Big data and cloud computing: Innovation opportunities and challenges. *International Journal of Digital Earth*, 1-41. doi: 10.1080/17538947.2016.1239771

Yang, C. C., & Wei, H. H. (2013). The effect of supply chain security management on security performance in container shipping operations. *Supply Chain Management: An International Journal, 18*(1), 74-85. doi: doi:10.1108/13598541311293195

Yaqoob, I., Hashem, I. A. T., Gani, A., Mokhtar, S., Ahmed, E., Anuar, N. B., & Vasilakos, A. V. (2016). Big data: From beginning to future. *International Journal of Information Management, 36*(6, Part B), 1231-1247. doi: http://dx.doi.org/10.1016/j.ijinfomgt.2016.07.009

Yin, R. K. (2003). Case study research design and methods third edition. *Applied social research methods series, 5*.

Yu, M.-M., Ting, S.-C., & Chen, M.-C. (2010). Evaluating the cross-efficiency of information sharing in supply chains. *Expert Systems with Applications, 37*(4), 2891-2897. doi: http://dx.doi.org/10.1016/j.eswa.2009.09.048

Yuvaraj, M. (2015). Security threats, risks and open source cloud computing security solutions for libraries. *Library Hi Tech News, 32*(7), 16-18. doi: doi:10.1108/LHTN-04-2015-0026

Zailani, S. H., Seva Subaramaniam, K., Iranmanesh, M., & Shaharudin, M. R. (2015). The impact of supply chain security practices on security operational performance among logistics service providers in an emerging economy: Security culture as moderator. *International Journal of Physical Distribution & Logistics Management, 45*(7), 652-673. doi: doi:10.1108/IJPDLM-12-2013-0286

Zargar, S. T., Joshi, J., & Tipper, D. (2013). A survey of defense mechanisms against distributed denial of service (ddos) flooding attacks. *IEEE Communications Surveys & Tutorials, 15*(4), 2046-2069. doi: 10.1109/SURV.2013.031413.00127

Zhang, H. (2014). *Detecting network intruders by examining packet crossovers in connections.*

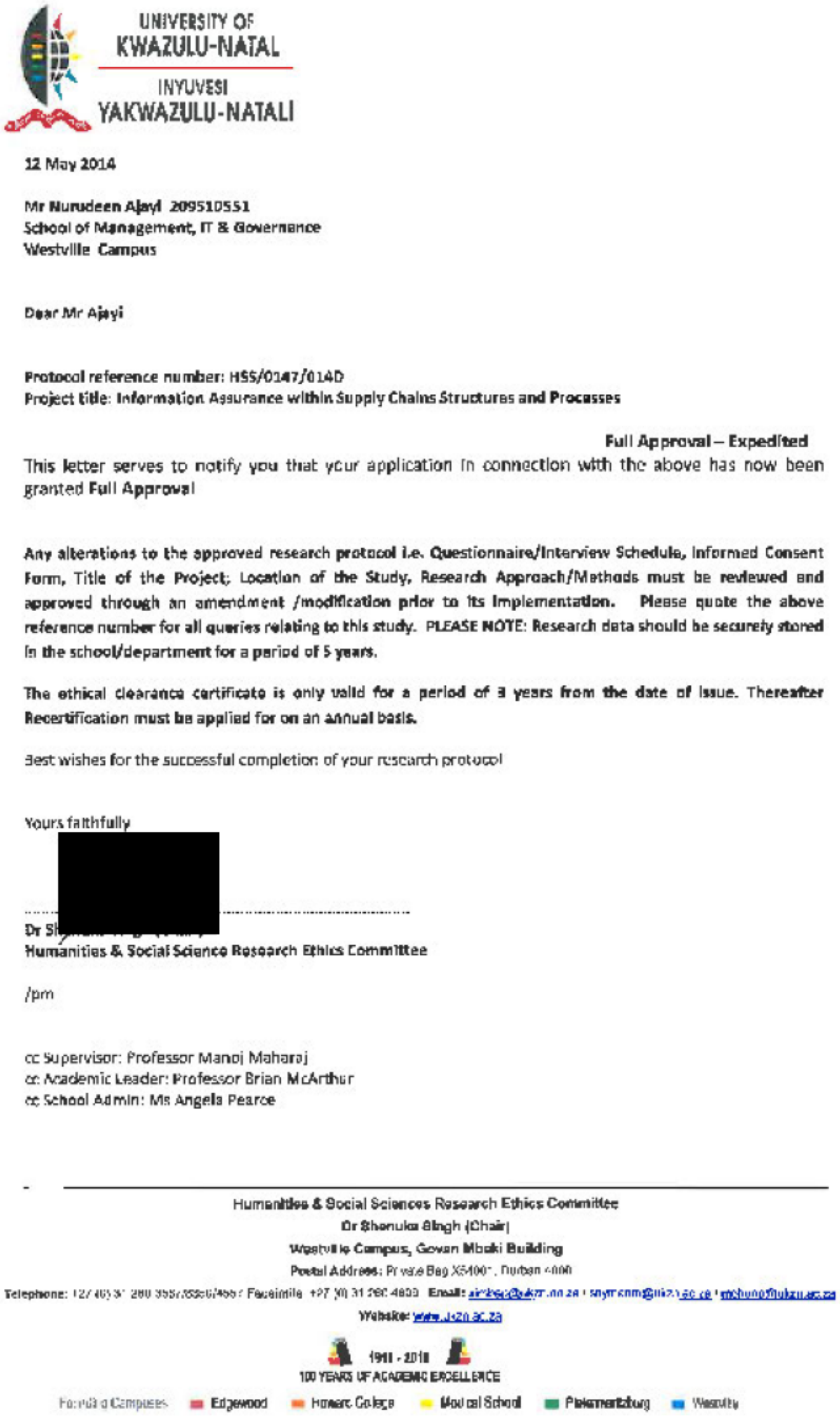
Zhang, J., & Chen, J. (2013). Coordination of information sharing in a supply chain. *International Journal of Production Economics, 143*(1), 178-187. doi: http://dx.doi.org/10.1016/j.ijpe.2013.01.005

Zhang, S., Yan, H., & Chen, X. (2012). Research on key technologies of cloud computing. *Physics Procedia, 33*, 1791-1797. doi: http://dx.doi.org/10.1016/j.phpro.2012.05.286

Zhu, X. (2016). Managing the risks of outsourcing: Time, quality and correlated costs. *Transportation Research Part E: Logistics and Transportation Review, 90*, 121-133. doi: http://dx.doi.org/10.1016/j.tre.2015.06.005

APPENDICES

Appendix A – Ethical Clearance



UNIVERSITY OF
KWAZULU-NATAL
INYUVESI
YAKWAZULU-NATALI

12 May 2014

Mr Nurudeen Ajayi 209510551
School of Management, IT & Governance
Westville Campus

Dear Mr Ajayi

Protocol reference number: HSS/0147/014D
Project title: Information Assurance within Supply Chains Structures and Processes

Full Approval – Expedited

This letter serves to notify you that your application in connection with the above has now been granted **Full Approval**

Any alterations to the approved research protocol i.e. Questionnaire/Interview Schedule, Informed Consent Form, Title of the Project, Location of the Study, Research Approach/Methods must be reviewed and approved through an amendment /modification prior to its implementation. Please quote the above reference number for all queries relating to this study. PLEASE NOTE: Research data should be securely stored in the school/department for a period of 5 years.

The ethical clearance certificate is only valid for a period of 3 years from the date of issue. Thereafter Recertification must be applied for on an annual basis.

Best wishes for the successful completion of your research protocol

Yours faithfully

[redacted]

Dr [redacted]
Humanities & Social Science Research Ethics Committee

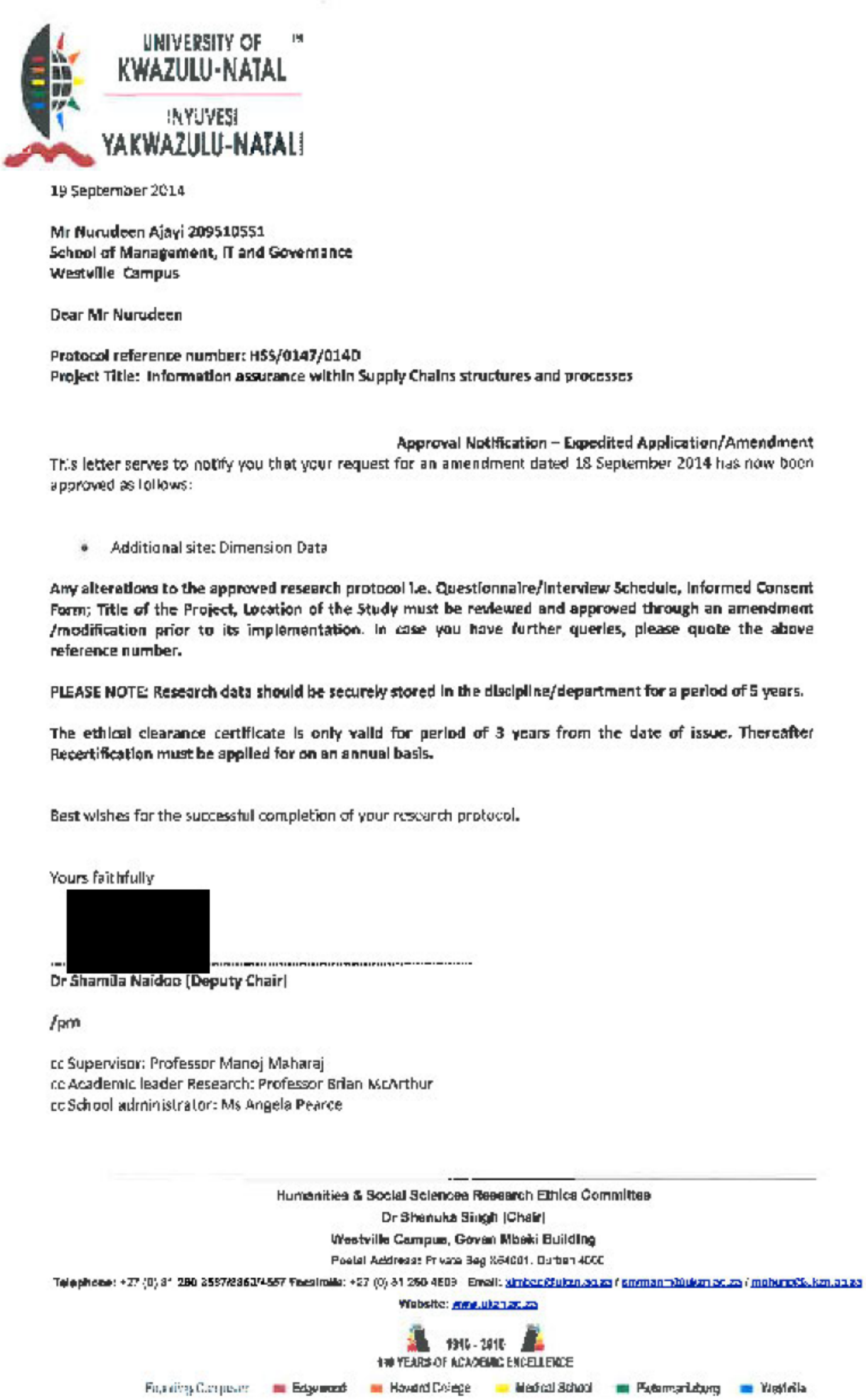
/pm

cc Supervisor: Professor Manoj Maharaj
cc Academic Leader: Professor Brian McArthur
cc School Admin: Ms Angela Pearce

Humanities & Social Sciences Research Ethics Committee
Dr Shenuka Singh (Chair)
Westville Campus, Govan Mbeki Building
Postal Address: Private Bag X54001, Durban 4000
Telephone: +27 (0) 31 260 3587/8350/4557 Facsimile: +27 (0) 31 260 4609 **Email:** ximbap@ukzn.ac.za / snymanm@ukzn.ac.za / mohunp@ukzn.ac.za
Website: www.ukzn.ac.za

1910 - 2010
100 YEARS OF ACADEMIC EXCELLENCE

Founding Campuses: 🟥 Edgewood 🟧 Howard College 🟨 Medical School 🟩 Pietermaritzburg 🟦 Westville



UNIVERSITY OF KWAZULU-NATAL

INYUVESI YAKWAZULU-NATALI

19 September 2014

Mr Nurudeen Ajayi 209510551
School of Management, IT and Governance
Westville Campus

Dear Mr Nurudeen

Protocol reference number: HSS/0147/014D
Project Title: Information assurance within Supply Chains structures and processes

Approval Notification – Expedited Application/Amendment

This letter serves to notify you that your request for an amendment dated 18 September 2014 has now been approved as follows:

- Additional site: Dimension Data

Any alterations to the approved research protocol i.e. Questionnaire/Interview Schedule, Informed Consent Form; Title of the Project, Location of the Study must be reviewed and approved through an amendment /modification prior to its implementation. In case you have further queries, please quote the above reference number.

PLEASE NOTE: Research data should be securely stored in the discipline/department for a period of 5 years.

The ethical clearance certificate is only valid for period of 3 years from the date of issue. Thereafter Recertification must be applied for on an annual basis.

Best wishes for the successful completion of your research protocol.

Yours faithfully

[redacted]

Dr Shamila Naidoo (Deputy Chair)

/pm

cc Supervisor: Professor Manoj Maharaj
cc Academic leader Research: Professor Brian McArthur
cc School administrator: Ms Angela Pearce

Humanities & Social Sciences Research Ethics Committee
Dr Shenuka Singh (Chair)
Westville Campus, Govan Mbeki Building
Postal Address: Private Bag X54001, Durban 4000
Telephone: +27 (0) 31 260 3587/8350/4557 **Facsimile:** +27 (0) 31 260 4609 **Email:** ximbap@ukzn.ac.za / snymanm@ukzn.ac.za / mohunp@ukzn.ac.za
Website: www.ukzn.ac.za

1910 - 2010
100 YEARS OF ACADEMIC EXCELLENCE

Founding Campuses: 🟥 Edgewood 🟧 Howard College 🟨 Medical School 🟩 Pietermaritzburg 🟦 Westville

Appendix B – Interview Schedule

INTERVIEW SCHEDULE

Topic: Information Assurance within Supply Chains' Structures and Processes

PhD Research Project
Discipline of Information Systems & Technology
School of Management, Information Technology & Governance
University of KwaZulu-Natal

Researcher: Nurudeen Ajayi (0793147203) **Supervisor**: Prof. Manoj Maharaj (031-2607051)

Introduction

My name is Nurudeen Ajayi. I am a PhD candidate in the Discipline of Information Systems & Technology, in the School of Management, Information Technology & Governance, at the University of KwaZulu-Natal.

I will like to ask you some questions about the information and information systems used within your organization's supply chain, and to also ask you some questions regarding the Security and Assurance of Information and Information Systems within the Supply Chain. This is to enable me gain insight into how information and information systems are used within supply chains, and to also gain insight into how Security and Assurance of Information and Information Systems are provided and managed.

I hope to use the gathered information to propose a Supply Chain Information Assurance Model that would enable organizations within Supply Chains to sustain their respective functions, enhance their processes and structures, manage their information and information systems, provide and manage security and assurance of information and information systems, and hence increase their organizations' value.

In this interview, the following keywords will be used:

Information System: An organized set of interrelated components that manage information e.g. Enterprise Resource Planning (ERP), Data Warehouse etc.

Information Security: The process and act of protecting Information and Information Systems from unauthorized access, usage, disruption and destruction.

Information Assurance: Practices that protect and audit Information and Information Systems by providing for their restoration through incorporating detection, reaction and protection capabilities.

Supply Chain: An integrated process wherein various business entities (suppliers, manufacturers, distributors, and retailers) work together to: acquire raw materials, convert these raw materials into specified final products, and deliver these final products to consumers.

Supply Chain Structure: A system wherein various business entities make decisions concerning their respective function within the supply chain.

Supply Chain Process: Activities that involves Decision Making and Planning within the supply chain structure.

The interview should take about 40 minutes.

The Organization & Supply Chain

1) Could you please tell me about what you do in the organization?
2) Could you please tell me about the supply chain(s) of your organization?
3) How does your organization fit into the supply chain?
4) Could you please tell me about the structures in place within the supply chain?
5) Kindly explain the processes (e.g. decision making process, information sharing processes) involved in the supply chain.

Information & Information Systems

6) Tell me the types of Information *gathered*, *stored* and *shared* within the Supply Chain?
7) Could you please briefly explain how the Information is used within the Supply Chain?
8) Kindly explain how Information is shared within the Supply Chain.
9) Could you please explain the role of Information in the Supply Chain processes?
   - ➢ Are Information Systems used to support the achievement of those roles?
10) Could you please explain the roles of Information in the Supply Chain Structure?
   - ➢ Are Information Systems used to support the achievement of those roles?
11) What are the Information Systems used within the Supply Chain?
   - ➢ Kindly explain what those Information Systems are used for.
   - ➢ Could you also explain how they are used?

- *If no Information Systems are used*, then, how is Information *gathered*, *stored* or *shared* within the Supply Chain?

Security & Assurance

12) Could you please explain how the protection of the Information used within the Supply Chain is ensured?
13) Could you please explain how the protection of the Information Systems used within the Supply Chain is ensured?
14) A supply chain is only as strong as its weakest link… (*Interlude*…)
    Could you please explain the possible Vulnerabilities to Information, which has been exploited in the past, within the Supply Chain?

    - Kindly explain how those Information vulnerabilities were detected?
    - Kindly explain how those vulnerabilities were managed after detection?
    - *If no vulnerabilities were identified (Q14), ask;* Please explain how the Supply Chain prevents information Vulnerabilities.

15) Due to Information activities within the Supply Chain and among its partners, what are the possible Information vulnerabilities that you foresee? Please explain.
16) Could you please explain the possible Vulnerabilities to Information Systems, which has been exploited in the past, within the Supply Chain?

    - Kindly explain how the vulnerabilities were detected?
    - Kindly explain how the vulnerabilities were managed after detection?
    - *If no vulnerabilities where identified (Q16), ask;* Please explain how the Supply Chain prevents Information Systems Vulnerabilities.

17) Could you please tell me about any Information threats or attacks (e.g. Malware, Espionage etc.) the Supply Chain has experienced in the past?

    - How were the threats or attacks detected?
    - How was the threat or attack managed?
    - *If no threats or attacks were identified (Q17), ask*; Please explain how the Supply Chain has been able to prevent threats or attacks on Information.
    - Please explain how potential threats or attacks on Information within the Supply Chain are being prevented.

18) Due to the activities of the Supply Chain and its partners, do you foresee any potential threats or attacks on Information within the Supply Chain? If yes, please explain.

19) What are the measures in place to manage any potential threats or attacks on Information within the Supply Chain?

20) Could you please tell me about any Information Systems threats or attacks the Supply Chain has experienced in the past?

   - ➢ How were the threats or attacks detected?
   - ➢ How was the threat or attack managed?
   - ➢ *If no threats or attacks were identified (Q20), ask*; Please explain how the Supply Chain has been able to prevent threats or attacks on Information Systems.
   - ➢ Please explain how potential threats or attacks on Information Systems within the Supply Chain are being prevented.

21) Do you foresee any potential threats or attacks on the Information Systems within the Supply Chain? If yes, please explain.

22) What are the measures in place to manage any potential threats or attacks on the Information Systems within the Supply Chain?

23) What are the measures in place within the Supply Chain to ensure the following:

   a) That Information access is prevented from an unauthorized access?
   b) That Information Systems are prevented from unauthorized access?
   c) Ensures the accuracy of Information as it flows through the Supply Chain?
   d) Ensures the consistency of Information as it flows through the Supply Chain?
   e) Ensures that Information is available at all times?
   f) Ensures that Information Systems are available at all times?
   g) Ensures the authenticity (authentication) of information?

24) Could you please explain how the measures (Question 23a-g) are implemented?

25) Are there policies that ensure the implementation and usage of the measure in Q23a-g within the Supply Chain? If Yes, Please briefly explain them to me.

Finally, is there anything you would like to add?

Thank you for your time – it is highly appreciated!!!

Appendix C – Informed Consent

UNIVERSITY OF KWAZULU-NATAL
Discipline of Information Systems & Technology
School of Management, Information Technology & Governance

PhD Research Project

Researcher: Nurudeen Ajayi (0793147203)

Supervisor: Prof. Manoj Maharaj (031-2607051)

Research Office: Ms P Ximba (031-2603587)

Dear Respondent,

My name is Nurudeen Ajayi. I am a PhD candidate in the Discipline of Information Systems & Technology, in the School of Management, Information Technology & Governance, at the University of KwaZulu-Natal. I hereby invite you to please participate in a research project titled "**Information Assurance within Supply Chains' Structures and Processes**". The main aim of the study is:

- To propose an information assurance model that can enable organisations protect and sustain their respective information within the supply chain structures, and that can also enable them to minimise or prevent the risks that information within the supply chain processes could be exposed to.

To accomplish the main aim, the study has four primary objectives which are:

- To understand the role of information and information systems within supply chains.
- To understand how information is shared, and also, the impact of sharing information within the various processes and structures of the different components of supply chains. This was done by also investigating the information systems used for sharing information.
- To identify and understand the issues and challenges surrounding the security of information systems, and also, information, as it moves through the various supply chain structures and processes.
- To understand information assurance as a concept and evaluate its objectives, and also identify how it can facilitate a smooth supply chain process and an efficient and effective supply chain structure.

Through your participation I hope to understand how security and assurance of information and information systems within the supply chain can be provided. The results of this research are intended to contribute to the security, assurance and risk management of information and information systems within supply chains.

Your participation in this project is voluntary and you may refuse to participate or withdraw from the project at any time with no negative consequence. There will be no monetary gain from participating in this research project.

Confidentiality and anonymity of records identifying you as a participant in this project will be maintained by the school of Management, Information Technology & Governance, UKZN.

If you have any questions or concerns about the study, or about participating in the study, please contact me or my supervisor at the numbers listed above.

Please note:

- ➢ *The interview should take about 40 minutes to complete.*
- ➢ *The questionnaire should take about 15 minutes to complete.*

Thank you for your willingness to participating!

Sincerely

Investigator’s signature : __________ Date : __________

UNIVERSITY OF KWAZULU-NATAL
Discipline of Information Systems & Technology
School of Management, Information Technology & Governance

PhD Research Project

Researcher: Nurudeen Ajayi (0793147203)

Supervisor: Prof. Manoj Maharaj (031-2607051)

Research Office: Ms P Ximba (031-2603587)

CONSENT

I____ (full names of participant) hereby confirm that I understand the contents of this document and the nature of the research project, and I consent to participating in the research project. I understand that I am at liberty to withdraw from the project at any time, should I so desire.

For Interview**:**

I consent □ / do not consent □ **to having this interview audio- recorded**

____________________ ____________________

Signature of Participant Date