Information Security Compliance Behaviour in Supply Chain Security

Ibrahim Shafiu

A thesis submitted to
Auckland University of Technology
in fulfilment of the requirements for the degree of
Doctor of Philosophy (PhD)

2015
Department of Business Information Systems
AUT Business School

Author's Declaration

I hereby declare that this submission is my own work and that, to the best of my knowledge and belief, it contains no material previously published or written by another person (except where explicitly referenced), no material which to a substantial extent has been submitted for the award of any other degree or diploma of a university or other institution of higher learning.

The following peer review paper relate to work undertaken for this thesis:

Shafiu, I., Wang, W. Y. C., & Singh, H. (2014). Mixed Method for New Scholars with Intrusive, Emerging and Complex Socio-Technical Topics, Knowledge Management in Organizations (pp. 255-266): Springer.

…….

Author's Signature

This dissertation was presented by

Ibrahim Shafiu

Under the supervision of

Primary Supervisor

Associate Professor William Yu Chung Wang
Business Information Systems
Auckland University of Technology

Secondary Supervisor

Senior Lecturer Dr. Harminder Singh
Business Information Systems
Auckland University of Technology

Defended on

20th May 2015

Examination Panel

Associate Professor David Pauleen
Dr Angela Lin
Dr Hing Kai Chan

Convener

Associate Professor Mark Janson

Abstract

Since the September 11, 2001, terrorist attacks on the United States of America the cross-border supply chain has been operating in a heightened security environment. As a result, supply chain security (SCS) has received more attention both academically and professionally. To ensure the secure and smooth operation within heightened security conditions, leading international trading nations have developed several SCS initiatives collectively known as the Global Supply Chain Security (GSCS) initiatives. The GSCS initiatives dictate or advocate several security standards and demand full compliance from trading partners. One of the most important requirements of these standards is information security compliance because one of the most critical tools in combating terrorism is the intelligence gathered from information relating to cargo and its conveyances. This calls for a complex understanding of the information security compliance behaviour of market stakeholders such as traders, freight forwarders and the customs brokers, something which the existing literature does not provide. In particular, this emerging area of SCS research has not fully examined SCS in the context of GSCS initiatives. This study accordingly develops a framework for understanding information security compliance behaviour (ISCB) by formulating an aggregated model using existing theoretical frameworks such as institutional theory and social exchange theory.

This study hypothesizes that there are three organizational perceptions that drive compliance behaviour: (1) perception of threats; (2) perception of norms; and (3) perception of benefits. Further, it was hypothesized that these drivers are influenced by five elements that belong to two distinctive groups, namely inter-organizational influences and rules and norms of social exchange. The inter-organizational influences consist of three elements: (1) regular demands, (2) market influence, and (3) peer pressure, while the rules and norms of social exchange are classified under reciprocity or fairness. As this is an emerging research context with limited relevant literature, a sequential mixed methods design was used to operationalize the study. The qualitative phase of this research evaluated the relevance of the constructs used in the model, which was tested in the quantitative phase. The qualitative phase was conducted with a set of interviews among 15 market stakeholders consisting of traders, freight forwarders and customs brokers. To test the quantitative model, 205 participants from the same categories were studied as the sample. To test the model partial least squares (PLS) regression analysis was applied to a structured equation model. The findings suggest that there are three significant drivers that affect ISCB, two of which lead to substantial compliance behaviour and the other

to symbolic compliance behaviour. Further, the study also reveals that four of the five identified elements are significant in influencing the drivers affecting compliance behaviour. This study has both significant theoretical and practical implications. The theoretical contributions include the development of an aggregated model which explains ISCB in an inter-organizational context. From the practical aspect, this study contributes by providing a framework to identify the effectiveness of the existing security regimes in enforcing ISCB in SCS, as well as ways to enhance this process.

Acknowledgements

I would like to acknowledge and thank the contributions of those who helped me to complete this thesis.

- To Dr. William Y.C. Wang, my primary supervisor, for his keen interest on the topic and the academic expertise and unconditional support provided throughout this very difficult journey. I thank him for his patience and tolerance. His style of guidance helped me to grow and develop as a researcher. My profound gratitude to Dr. William, thank you.

- To Dr. Harminder Singh for his profound guidance and support at every stage of this research. In particular, I am thankful for the opportunities he provided to showcase my work that helped build my confidence in the research area.

- To AUT Ethics Committee, for approving my ethical application and providing the needed guidance.

- To the fifteen interview participants who gave their precious time to sit with me and share their valuable knowledge and the 205 survey participants who took time to respond to my survey questions. I salute each and every one of them for giving so generously in the name of advancing knowledge. Thank you all.

- To my family and friends in Hamilton who have been a continuous source of support during my studies.

- To my father and mother, for always believing in me and their unconditional support for all what I do.

- To my sister Asima Ali and brother-in-law Mohamed Abbas for sponsoring me for my PhD studies. Their phone call with the generous offer would ring in my ears for the rest of my life, reminding me to never lose hope. Thank you both for believing in me.

- To my wife, and two sons for their patience and support throughout this journey. A special thank you to my wife who spent endless hours reading through my work.

Dedication

To my parents
for always supporting me

To my wife
for always encouraging me

To my two sons
for the continuous joy they bring me

Table of Contents

List of Figures

List of Tables

List of Abbreviations

AEO	Authorized Economic Operator
AVE	average variance extract
CBAFF	Customs Brokers and Freight Forwarders Federation
CMB	Common Method Bias
CSI	Container Security Initiative
C-TPAT	Customs Trader Partnership Against Terrorism
EU	European Union
GAO	Government Audit Office
GSCS	global supply chain security
ISCB	information security compliance behaviour
MRA	Mutual Recognition Agreement
MV	manifest variable
PLS	partial least square
SCM	supply chain management
SCS	supply chain security
SEM	structural equation modelling
SES	Secure Export Scheme
SET	social exchange theory
WCO	World Customs Organization
WMD	weapons of mass destruction

CHAPTER 1: INTRODUCTION

1.1 The Study

The major trading countries around the world fear that the global supply chain maybe under threat from terrorists using it to transport weapons of mass destruction (WMD) across national boundaries, which could potentially bring world trade to a halt (Bakshi & Gans, 2010; Lee & Whang, 2005; Sarathy, 2006). To prevent such a disastrous outcome, the major trading countries, along with relevant international organizations, have developed what are known as Global Supply Chain Security (GSCS) initiatives (Banomyong, 2005). The main goal of the GSCS initiatives, which are enforced by the border control authorities worldwide, is to stop terrorists using the cross-border supply chain to transport WMD (Bakshi & Gans, 2010; Lee & Whang, 2005; Sarathy, 2006). These initiatives require trading countries and their traders to comply with certain security related requirements, of which information security is one of the most important (Bichou, 2004; Chad & Bobbitt, 2008; Closs & McGarrell, 2004).

However, the information security compliance requirements demanded from market stakeholders by the authorities enforcing GSCS initiatives are not being met in all cases (Dahlman et al., 2005). Existing research shows that strategic alliances and business partnerships, similar to what GSCS initiatives advocate, may be operating under forged acceptable operating practices (Mei & Dinwoodie, 2005). If the intended outcomes of these security initiatives are not achieved, the supply chain may still be vulnerable to serious threats to cross-border trade in terms of theft, sabotage, or terrorist attacks. The existing academic literature falls short in explaining the compliance behaviour of market stakeholders under the prevailing heavy regulatory requirements and other such institutional pressures experienced in the 21st century. This knowledge is deemed important for ensuring the smooth and secure flow of goods across international borders and through the international supply chain. As such, the purpose of this study is to understand and explain the information security compliance behaviour (ISCB) in SCS within the context of the GSCS initiatives. Accordingly, this study focuses on the compliance behaviour of market stakeholders such as traders, freight forwarders and customs brokers towards the information security requirements demanded by non-market stakeholders such as border control authorities.

1.2 Motivation of the Study

When the United States was attacked by terrorists on September 11, 2001, I was an officer working in the Information Technology Department of the Maldives Customs Service. The border control activities around major international ports changed overnight. Suddenly there was an increased emphasis on security. Several international conferences organized by the World Customs Organization (WCO) were held in all regions to find ways and means to conduct business smoothly and safely across international supply chains. One main concern was the physical inspection of cargo arriving at ports. The costs were escalating due to the delays caused by physical inspection of each and every cargo. To overcome delays, advanced electronic information relating to the cargo started to be used as a way to identify potentially harmful cargo. To fulfil this critical task, the information received by the authorities had to satisfy the fundamental characteristics of information security. That is, the information transmitted by the market stakeholders (customs brokers, freight forwarders and traders) should have characteristics such as reliability, integrity and continuity. SCS is an emerging area of focus when it comes to combating terrorism. In the past, when the term security was used in the context of the supply chain, it was used in discussions related to only theft and sabotage. Today, SCS also relates to the security of information exchanged in the supply chain. This poses serious questions about the reliability of the information used for such a critical task.

In the prevailing supply chain environment, discussions on enforcing SCS are very common and in a practical sense several measures are being implemented. However, there are several unanswered questions, the answers to which are important in enhancing the effectiveness of the security initiatives currently in force. One important question is how market stakeholders are responding to the pressures of emerging security requirements, both from other market stakeholders such as their customers and from non-market stakeholders (public organizations) like the border control authorities. Further, are mechanisms put in place by non-market stakeholders sufficient to motivate the market stakeholders to respond in a positive manner? The answers to these questions would enlighten non-market stakeholders on the efficiency and the sufficiency of the GCSC initiatives in protecting the cross-border supply chain from a terrorist attack. Hence, I was motivated to understand ISCB in the SCS context, and this motivation led to the undertaking of this research.

1.3 SCS and GSCS Initiatives

SCS is an emerging field of research within supply chain management (SCM). Academia treats SCS as a subcomponent of the overall risk management strategy of the supply chain. The academic literature identifies information sharing, information security, and gathering information for intelligence as significant elements of SCS. This study focuses on SCS from the angle of the information security requirements of the GSCS initiatives.

The global supply chain is an environment that has had its activities under heavy security scrutiny after the September 11, 2001, terrorist attacks on the United States. Since those attacks, the global supply chain has been operating in what is described as a heightened security environment (Sarathy, 2006). To be able to operate in this environment, stakeholders must take into account various GSCS initiatives, some of which are voluntary and some are mandatory (Closs & McGarrell, 2004; Lee & Whang, 2005; Urciuoli, 2010). GSCS initiatives are a set of guidelines enforced by various countries and international organizations to prevent the use of the supply chain for terrorist activity (Ke & Wei, 2008; Sarathy, 2006; Wagner, Coley, & Lindemann, 2011). One of the main requirements of these security initiatives is the sending of advance electronic information relating to the cargo and its conveyances to the border authorities of the destination port (Bichou, 2004). This information is then run through complex risk analysis algorithms to assess potentially risky cargo, which is targeted and selected for physical inspection, as physical inspection of all cargo arriving at a port would be an impossible task. Therefore, the information reaching the border control authorities needs to be accurate and secure from any undesired interventions.

1.4 Literature Review and the Research Gap

Technical aspects of information security have mostly been at the forefront of academic research (Dhillon & Torkzadeh, 2006), leaving a research gap with regard to behavioural aspects. This trend though is changing; during the past decade researchers have begun to focus on the socio-technical behavioural aspects of information security (Boss, et al., 2009). However, socio-technical research has been quite general in its focus on informing compliance behaviour – general in the sense that the findings reported are not industry-specific. For instance, there are many studies that have reported on the compliance behaviour of organizational information security policies. The question then is whether that behaviour applies to organizations operating in different environments. Would the compliance behaviour in an organization operating in the health sector be the same as in an organization operating in

the trade sector? A further question is how the compliance behaviour would be similar or different at an inter-organizational level. In this regard, this research focuses on the ISCB of organizations operating in a SCS environment in relation to inter-organizational information security compliance requirements enforced under GSCS initiatives.

An extensive literature review revealed several aspects of ISCB in a general context. A similar review of the SCS literature revealed a set of implications due to the GSCS initiatives. These two sets of findings, combined with existing relevant theoretical frameworks, are utilized to formulate a conceptual model to understand ISCB, the drivers that influence that behaviour, and the extent to which those drivers influence the behaviour.

1.5 Research Objectives and Research Questions

The purpose of this research is to understand and explain the ISCB in SCS under the influence of the GSCS initiatives. Accordingly, the research objectives are to:

1 Ascertain the prevailing academic knowledge from extant literature and formulate a conceptual model to explain ISCB. This would be significant in understanding the knowledge gap and the opportunities for academic contributions.

2 Verify the conceptual model in the given research context for its relevance in explaining the compliance behaviour. This would be significant in understanding the social-technical complexity of the research environment and stakeholder behaviour before embarking on the data collection.

3 Extend the understanding, underpinned by theoretical and socio-technical aspects, on the behaviour of the market stakeholders of the supply chain in complying with non-market stakeholder's information security requirements. This would be significant in enlightening non-market stakeholders concerning the prevailing behaviour and make assessments on the desired goals and actual outcomes.

4 Extend the understanding of the impact and implications of the existing drivers of ISCB among market stakeholders. This would be significant in identifying the required course of action to bring about the desired behaviour for keeping a secure and safer supply chain environment.

In order to address the research gap and achieve the research objectives, the following research questions are posed:

The overarching research question:

How do the supply chain security stakeholders comply with information security requirements mandated by the GSCS initiatives?

Sub research questions

[RQ1] What are the drivers of ISCB and how do they impact the compliance behaviour exhibited by the stakeholders?

[RQ2] What factors influence inter-organizational ISCB in the context of the GSCS initiatives?

1.6 Research Context

This study was conducted in New Zealand, which is an important trading partner of major economies such as the United States and the United Kingdom. Thus the context of the study is the international trading supply chain of New Zealand. New Zealand has special mutual agreements signed between major advocates of GSCS initiatives such as the United States in addition to its own security program called the New Zealand Secure Export Scheme. Hence, New Zealand's supply chain stakeholders are fully aware of, and play a key role in GSCS.

1.7 Methodology

It was decided that the research questions posed would be best answered using a sequential mixed method approach with emphasis on a quantitative survey. SCS is an emerging field with limited literature and no studies on ISCB conducted in this context were identified by the researcher. In this respect, it was important to validate the constructs identified from the literature before testing the model. Though mixing both qualitative and quantitative methods in a sequential manner is usually done for triangulation, in this study the application of an early qualitative phase is simply used for verification of the constructs and not for triangulation. Hence, it was decided that a qualitative study would be a used for the verification of the constructs followed by a quantitative study for validation of the proposed model, resulting in a sequential mixed methods study (Creswell, 2012).

The qualitative study was conducted among 15 members selected from the Customs Brokers and Freight Forwarders Federation (CBAFF) of New Zealand. The qualitative study also paved the way for recruiting more participants via snowballing. Based on the outcome of the qualitative analysis, the conceptual model was developed into a research model using existing

constructs from literature. The quantitative survey was conducted using a self-administered questionnaire hosted online on a free online survey website called Qualtrics. A total of 205 participants from 77 firms completed the survey. The participants were all boundary-spanning personnel of the 77 firms. As the study was inter-organizational in nature, the systematic inquiry into the role-sets of these boundary personnel will shed light on inter-organizational relations (Evan, 1965). The survey was analysed using the PLS-SEM software SmartPLS.

1.8 Structure of the thesis

This thesis is presented as ten chapters. This first chapter gives a brief background to the research including the motivation of the study, research objectives, and research questions. Chapter 2 is dedicated to the research context. Though the chapter is relatively short, it was deemed important to dedicate a chapter to the research context as supply chain security is an emerging field. This chapter presents a detailed description of the current global supply chain security initiatives in force and the role New Zealand plays in it.

To understand the link between supply chain security and information security and also to identify the research gap, an in-depth literature review was conducted. Chapter 3 presents the findings of this literature review classified into various categories. Chapter 4 presents the research questions and the conceptual model formulated for the research, including a discussion of the relevant theoretical frameworks. The research methodology is then described in Chapter 5. The main discussion is based on the sequential mixed method approach and its suitability to the study. In this sense the chapter outlines a qualitative phase to verify the constructs of the research model followed by a quantitative phase to validate these constructs. This chapter will instil the popularity of this sequential approach in information system studies where a qualitative phase is conducted initially to verify the constructs of the quantitative study rather than to provide a set of findings to triangulate with the findings of the quantitative study.

Chapter 6 provides the specific details of the qualitative study conducted in Phase 1, and the findings from this phase. Discussions in this chapter include how the findings help to ensure that the foundational understanding informed by the literature is relevant to the research context, as well as reveal any new themes that may not have been covered in the literature. In Chapter 7, the conceptual model presented in Chapter 4 is extended to a research model. This chapter present the links between the findings of the qualitative inquiry and the relationships that exist among the aspects of the conceptual model. This chapter then goes to present the

arguments in developing the research hypotheses posited to establish the significance of these relationships.

Chapter 8 provides details of Phase 2 of the research, the quantitative phase, including the measures used, the data collection process, the analysis conducted using partial least square structural equation modelling (PLS-SEM), how verifications and validations were achieved, and the findings from the survey. Following this, Chapter 9 provides a detailed discussion of the key research findings presented in Chapter 8. This discussion is focused on answering the two research questions and is based on the individual predictive and explanatory power of the elements that directly and indirectly influence compliance behaviour.

The final chapter, Chapter 10, summarizes the research journey, covering the purpose of the study, the process of identification of the research gap, the research questions, methodology, and the findings of the surveys. The contributions of the study to both academia and industry are also discussed, followed by the limitations of the study and directions for future research. An outline of the structure of the thesis is presented in Figure 1.

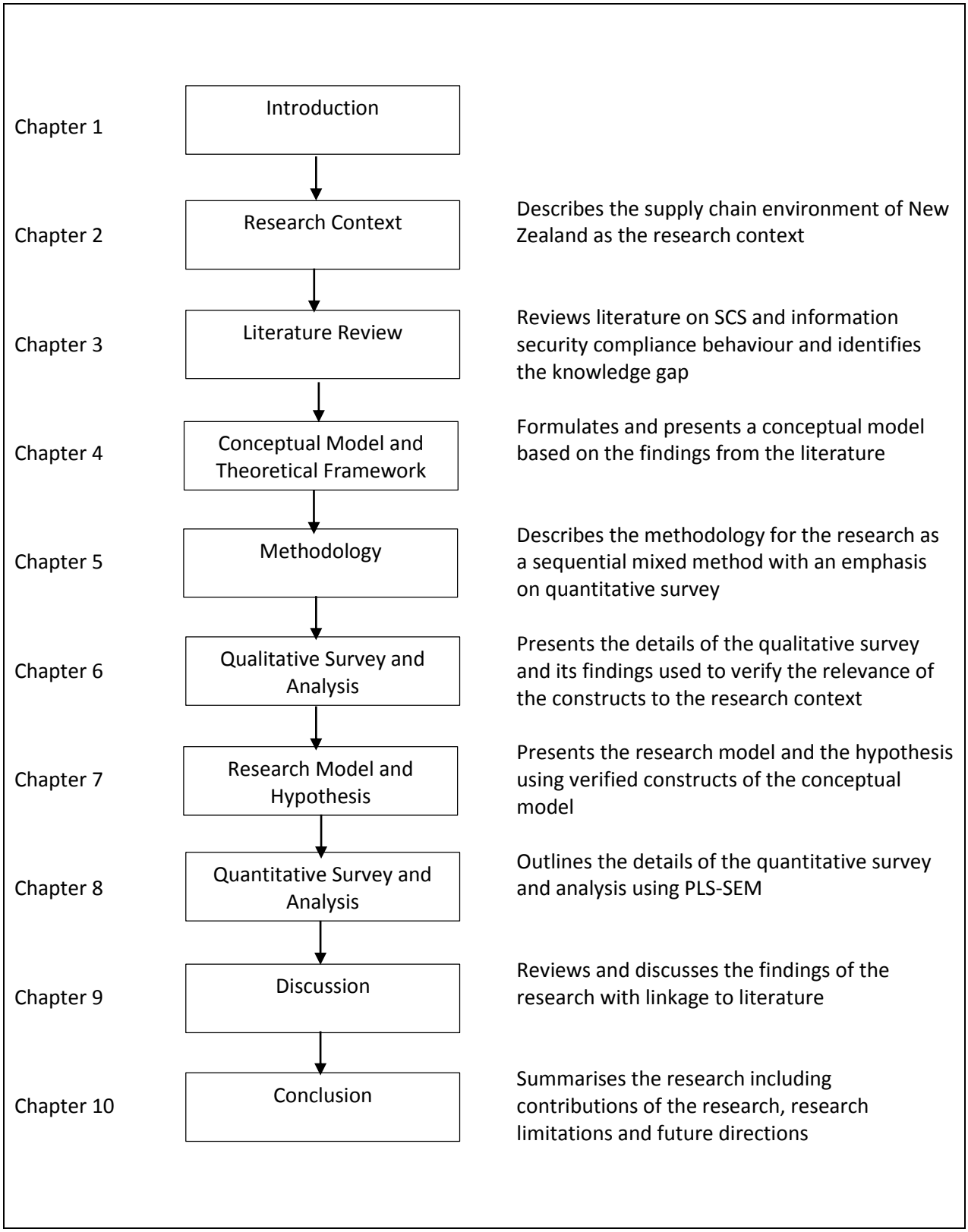

Figure 1: The structure of the thesis

CHAPTER 2: RESEARCH CONTEXT

2.1 Chapter Overview

The purpose of this chapter is to provide an understanding of the research context: the Global Supply Chain Security (GSCS) initiatives and the SCS environment within international trade in New Zealand. To achieve this purpose, a general overview of the GSCS initiatives and the international trade activities of New Zealand in relation to world supply chain will be discussed. The aim of this discussion will be to establish the fact that New Zealand plays an active role both locally and globally in securing the supply chain, thus demonstrating the relevance of this research to the New Zealand context.

2.2 GSCS Initiatives

The terrorist attacks on the United States on September 11, 2001, brought SCS to the forefront of international trade (Cohen, Mou, & Trope, 2014). One fear was that terrorist groups might use shipping containers to transport WMD (Sarathy, 2006). It was believed that the supply chain, linking international borders across the globe from very troubled ports to ports of superpowers, was vulnerable to such activity (Cohen, et al., 2014). The United States was the only victim of the horrendous September 11 attacks and, being the leading global importer, they were the first to come up with security initiatives to secure the global supply chain (Cohen, et al., 2014). These security initiatives became global as firms along with their supply chain partners across the globe and the corresponding governments agreed to collaboratively monitor and securitize all points of the cross-border cargo movement (Sarathy, 2006).

The United States' strategic move effectively extended its borders to the shores of all their trading partners. This was achieved by stationing US Customs and Border Control officers at trading ports. This initiative is called the Container Security Initiative (CSI). Under this initiative, the United States made bilateral partnership agreements with their trading partners, which provided for United States officers to be stationed at these ports to inspect cargo destined for the United States before it left the source ports (Burgess, Singh, & Koroglu, 2006). Homeland Security reports 58 foreign ports are currently participating in the CSI program, which accounts for 85% of container traffic bound for the United States. By participating in this program, the advantage for exporting countries is the uninterrupted flow of goods through the border with minimal or no physical inspection when it reaches the United States, thereby speeding up the clearance process at United States borders, which otherwise might take an

average of three to four days depending on the size of the shipment. The disadvantage for local traders of these exporting countries is that once a shipment is targeted for inspection, the cost of de-stuffing and re-stuffing the container for inspection has to be borne by the exporter, whereas if the inspection was needed at the destination border the cost of inspection will be borne by the buyer (Sarathy, 2006).

The second initiative that came into force after September 11 is the 24 Hours Manifest Rule. Under this initiative each cargo-carrying vessel destined for the United States has to electronically send its manifest 24 hours prior to its departure from its source port (Meares & Kahan, 1998). This is a mandatory requirement, which if not complied with could lead to the vessel being refused entry to the United States, causing massive financial losses (Banomyong, 2005).

The third initiative is a voluntary initiative called Customs-Traders Partnership Against Terrorism (C-TPAT). This initiative encourages local traders to join and receive privileges such as minimum physical inspection and expedited customs procedures, thereby achieving quick movement through border customs (Ke, Liu, Wei, Gu, & Chen, 2009). This partnership is offered to United States-based traders, but foreign suppliers also have to ensure that the compliance requirements demanded by C-TPAT are met as there is the fear of losing their US buyers to a supplier who is more willing to comply.

While enforcing these SCS initiatives, the United States was also playing a pivot role in advocating them as best practices for GSCS. This effort was supported by the WCO and the European Union (EU), which introduced their own programs based on the US initiatives. The WCO's program, which was adopted in June 2005, is called the Framework of Standards to Secure and Facilitate Global Trade (SAFE Framework) (Johnson & Onwuegbuzie, 2004). According to the WCO, this framework would act as a deterrent to international terrorism, secure revenue collection, and promote trade facilitation. The EU amended its Council Regulation on April 13, 2005, to introduce the Authorized Economic Operator (AEO) program (Götz, Liehr-Gobbers, & Krafft, 2010). The AEO, which is comparable to the United States' C-TPAT program, is a voluntary program for EU members that allows AEO licensed traders to access simplified customs rules and benefit from facilitation of customs controls relating to safety and security.

2.3 Information Security in GSCS Initiatives

The most common definition for information security found in literature states that it covers the confidentiality, integrity and availability of information (Akbulut-Bailey, 2011). One common and significant requirement of the GSCS initiatives is information security. This is evident from the emphasis given and the stringent requirements on information security set out in the widely advocated GSCS initiatives such as the container security initiative, advance manifest rule and also in the SAFE framework. The WCO's SAFE framework and the EU's AEO both specifically call for information security requirements to identify high risk cargos and transport conveyances. In addition, the express purpose of the 24 Hour Manifest Rule is to collect advance information electronically, so that risky or suspicious cargo can be identified and selected for physical inspection, well before the vessels arrive at the destination port. Hence, to achieve this purpose, information security is essential. Compliance with GSCS initiatives is interesting because there is little reciprocal benefit from providing information – one partner could be seen as behaving opportunistically and no efficiency gains accrue to the other partner by complying with the information-providing obligation. Given this situation, the effective and efficient implementation of the security initiatives depends significantly on the level of compliance from the information providers. If the information provided lacks the principles of information security due to lack of compliance, the whole objective of the GSCS initiatives is compromised. The flow of information in the context of GSCS is presented in Figure 3.

2.4 Supply Chain Security in New Zealand

2.4.1 New Zealand and Global Trade

According to the trade statistics of New Zealand for the year 2012 (see Figure 2), some of its top trading partners include top advocates and promoters of GSCS initiatives, such as the United States, United Kingdom and Australia. This means that New Zealand exporters have to be fully aware and be in compliance with the requirements of these trading partners in terms of SCS.

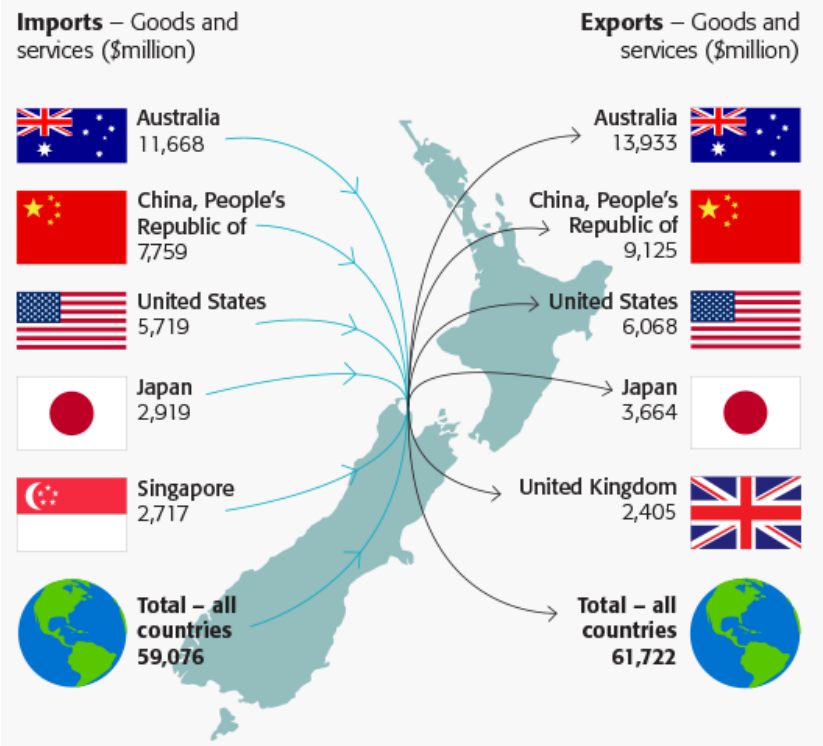

Figure 2: Main trading partners of New Zealand 2013

Source: http://www.stats.govt.nz

2.4.2 Secure Exports Scheme

New Zealand has its own SCS strategy to reduce risk through voluntary agreements with industry called the Secure Exports Scheme (SES), which ensures that goods exported under the scheme are packed and conveyed securely, without interference, to the place of shipment. Further, the members of the SES benefit from reduced export entry fees, lower intervention levels by customs, and the ability to demonstrate to overseas customers their security practices meet internationally recognized standards (Ministry of Business, Innovation and Employment, 2012) According to the Minister of Customs, one common element with respect to security requirements of other initiatives and customs administrations around the world is advance supply of electronic information for the purpose of risk analysis and risk management to avoid any terrorist attacks (Ministry of Business, Innovation and Employment, 2012) .

New Zealand promotes this scheme by (1) ensuring participants quick turnaround time of their shipments during export by reducing the likelihood of examination for security purposes, (2) assuring foreign trade partners that the participant is in compliance with international security standards such as the WCO's SAFE framework, (3) reducing fees for the lodgement of all export entries, (4) enhancing border clearances with other foreign borders with Mutual

Recognition Arrangements (MRA), and (5) advising and assisting participants to solve unexpected issues at borders of other countries with MRAs. This scheme had more than 120 registered exporters in 2012 (Ministry of Business, Innovation and Employment, 2012).

The most important expectation from the participants is that they are responsible for securing logistical operations and for monitoring and maintaining an agreed level of security and data integrity. The integrity of data should be assured by providing accurate advance export information (Ministry of Business, Innovation and Employment, 2012).

2.5 The Flow of Information in SCS

The diagram in Figure 3 shows the flow of information within the segment of the supply chain on which this study is based. The selection of this segment is purely strategic rather than opportunistic. First, the main requirement is that the group of entities within the context should constitute a segment of the supply chain; second, they should be sharing information that is relevant to the security of the supply chain. Hence, the entities can be selected from the set of organizations identified in the report by European Commission on Common Assessment and Analysis of Risk in Global Supply Chains as being highly relevant to the establishment of SCS (Nidjham, 2012). These organizations include both private organizations (traders, logistics providers and customs brokers) and public organizations (customs and port authorities). This study refers to the private organizations in the supply chain network as market stakeholders and the public organizations as non-market stakeholders.

Consider a scenario of information exchange within this segment of the supply chain. The trader, who is a supplier to a foreign country, will submit documents to the customs broker and the logistics operator. The customs broker prepares the export documents as required by customs. The logistics operator prepares the shipping documents required by the port authority. These documents are then submitted to the relevant authorities for verification and endorsement. As required by the security initiatives of the importing countries, such as the 24 Hour Manifest Rule of the United States, these verified documents are sent to the border control authorities of the

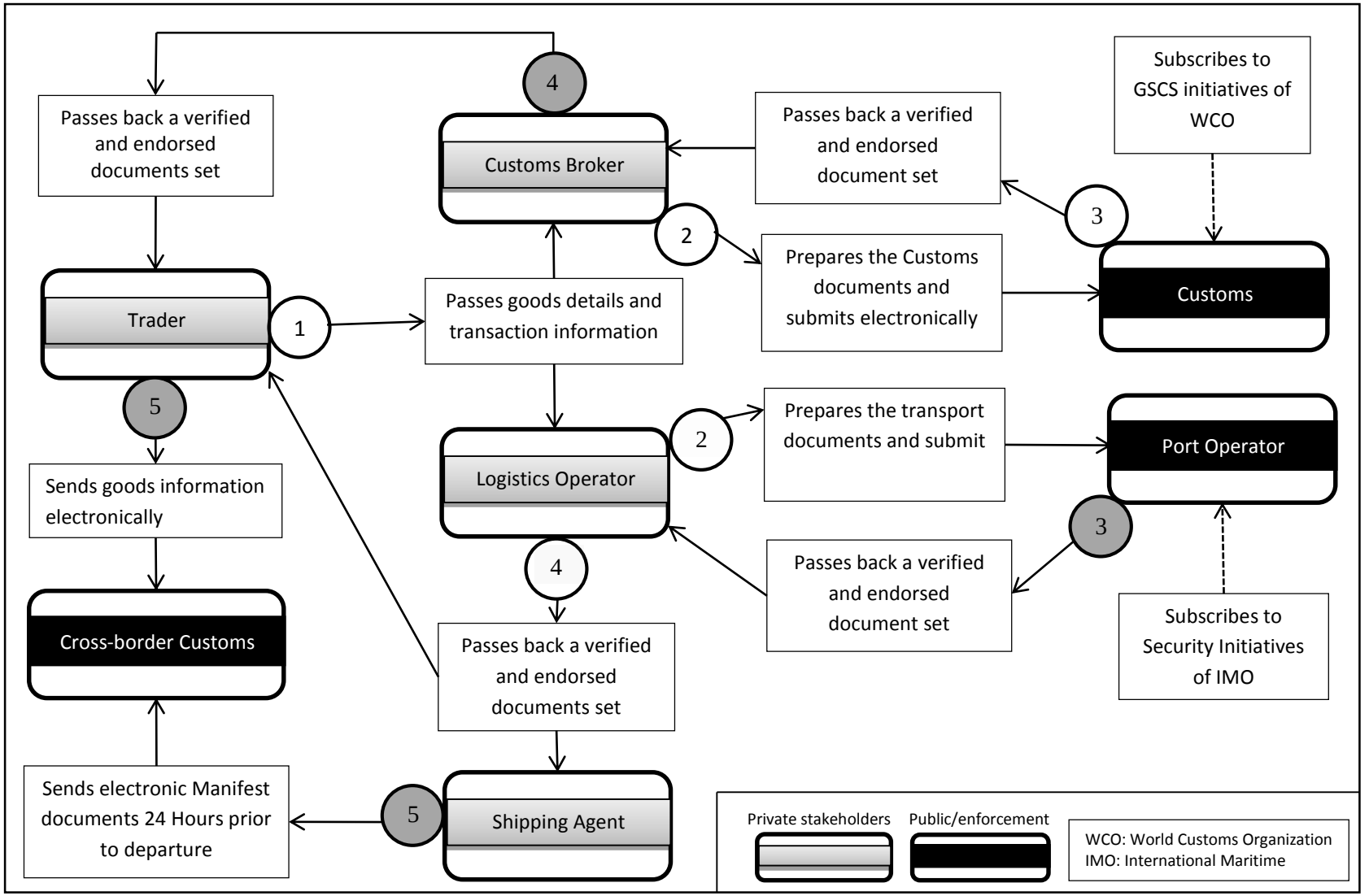

Figure 3: Information flow within a global supply chain in a SCS context

importing country. Based on the information sent in advance, the border control authorities conduct targeting and selective exercises to identify potentially threatening cargo for physical inspection (Lee & Whang, 2005). If the information provided in this situation lacks integrity or has been tampered with, the exercise of targeting and selectivity would fail. Hence, the integrity of the information shared between organizations becomes very significant.

2.6 Summary

New Zealand exporters have to be fully aware and be in compliance with the requirements of its global trading partners in terms of SCS. The country boasts its own SCS program known as the Secure Exports Scheme which is based on the WCO's SAFE framework This scheme had more than 120 registered exporters in 2012 (Ministry of Business, Innovation and Employment, 2012). On top of this, New Zealand's top trading partners such as the United States and United Kingdom are countries which demand very high security requirements through their own SCS initiatives. In order for New Zealand businesses to successfully trade with these countries, they must be fully aware of their security requirements and comply accordingly. Hence, New Zealand can be considered as an acceptable research context for the study the ISCB within the SCS environment. The next chapter reviews the existing academic literature on SCS and information security in order to identify the research gap which this study is designed to fill.

CHAPTER 3: LITERATURE REVIEW

3.1 Chapter Overview

This chapter reviews the literature on SCS and its relation to information security in order to identify the research gap. SCS is considered one of the risk management aspects of SCM. SCS can be divided into two subsections: security of cargo and security of information. Thus, the review is focused on the SCS literature that covers aspects of information security. In parallel, aspects of information security within the Information Management literature will also be investigated. Unlike SCS, has area has been the subject of academic focus for some time and therefore has a broader coverage of issues compared to the SCS literature. Within the Information Management literature, information security is also divided into two subsections: technical aspects and socio-technical or behavioural aspects. The focus of this review is on literature on the behavioural aspects of information security, specifically those related to compliance.

It can be inferred from Jarvenpaa and Staples (2000) that information sharing is part of information management in organizations. Issues related to information security increase when there is a need to share information among organizations (Gordon, Loeb, & Lucyshyn, 2003). In this sense, information security comprises of two main broad categories of technical and behavioural aspects (Warkentin & Willison, 2009). As far as SCS is concerned, it is an emerging field of research within SCM and is a subcomponent of the overall risk management strategy of the supply chain (Closs & McGarrell, 2004; Toosi, Calheiros, & Buyya, 2014). The linkages between the different areas of the literature relevant to this study is summarised in Figure 4 and the shaded boxes represents the focus in each specific area of the literature covered in this review, which ultimately leads to the identification of the research gap.

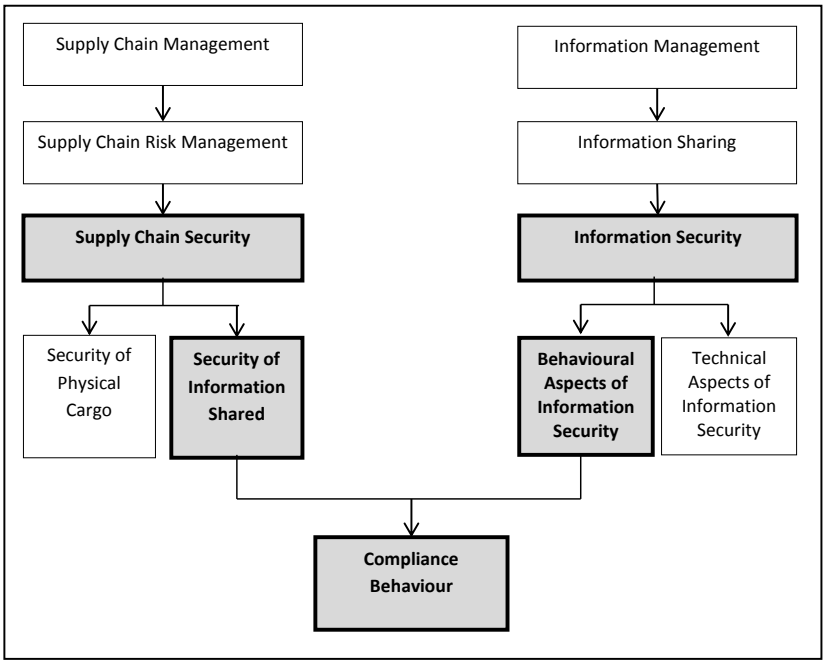

Figure 4: Major topics covered

3.2 Socio-Technical Systems

As mentioned above, this study is focused on studying the behavioural aspects within a socio-technical system. Socio-technical systems are systems that encompass both technology and society (Geels, 2004), According to Geels (2004) the society is surrounded by technologies which shape the perceptions, behavioural patterns and activities, thereby forming a structuring context for human action. This structuring context maybe a complex organizational structure intertwined with equally complex technologies (Vespignani, 2012). Hence, the concept of the socio-technical system emerged to enforce the reciprocal inter-relation between humans and machines to promote the program of shaping both the technical and social conditions of work, thereby aligning efficiency and humanity without any contradictions (Ropohl, 1999). In this sense, studying a socio-technical system focuses on the way interactions between humans restrict or shape interactions between humans and technology (Coiera, 2007). Thus, this study of information security compliance behaviour is such a study of socio-technical systems where the social nature of humans is analysed as they function within inter-organizational structures that are governed by processes highly interlinked with information systems.

3.3 Information Security

While information security studies were based on opinion, anecdotal evidence, or experience in the past (Kotulic & Clark, 2004), and were functional and technocratic (Dhillon & Torkzadeh, 2006), this trend has changed and today increasing numbers of academic researchers are paying attention to information security (Boss, et al., 2009). Information security research is one of the most intrusive types of organizational research (Kotulic & Clark, 2004), and a trusted relationship between the researcher and the organization is needed to conduct empirical research in this field.

Topics examined in the literature on information security include: access to information; communication and effectiveness; security management; costs and evaluation of investments; and design, development and alignment of policy. According to (Dhillon & Torkzadeh, 2006), information security research fall into four categories: checklists, risk analysis, formal approaches, and soft approaches. Many of these issues are studied as technical issues and solved using mathematical approaches, as summarized in Table 1. However, it is suggested that other theories, for example from psychology, sociology, semiotics, and philosophy, should be used to study security management and the development of secure information systems (Siponen & Oinas-Kukkonen, 2007), as overreliance on technical solutions without solving the underlying behavioural causes may prove ineffective (Posey, Roberts, Lowry, & Hightower, 2014).

Since the context of this research is socio-organizational, the rest of this section will be focused on reviewing literature that examines information security issues from a socio-organizational perspective. Five main areas were identified in this literature: (1) perceived importance of information security, (2) deterring threats, (3) risk management and analysis, (4) user behaviour and compliance, and (5) organization information security behaviour. Summary tables of the literature on these areas are included in Appendix F. The following subsections report the findings under each of these categories, and conclude with a discussion on the identified research gap.

Table 1: Information security literature on technical and theoretical aspects

Category	Subcategory	Reference
Software	Testing	(Mouratidis & Giorgini, 2007)
	Modelling	(Mouratidis, Giorgini, & Manson, 2005)
	Applications development	(Woon & Kankanhalli, 2007)

Workflow systems		(Wainer, Kumar, & Barthelmess, 2007)
Database	Architecture	(H.Rex, 1981)
	Data mining	(Yi & Zhang, 2009)
	Warehousing	(Fernández-Medina, Trujillo, & Piattini, 2007)
	Security in general	(Bertino, Jajodia, & Samarati, 1995)
Access control	Authentication	(Kuber & Yu, 2010; Vu et al., 2007)
	Cryptography	(Chang, Hwang, & Wu, 1992)
	PKI	(Beckles, Welch, & Basney, 2005)
e-commerce		(Khalifa & Liu, 2007)
email		(Roth, Straub, & Richter, 2005)
Decision support systems		
	Security planning	(El-Gayar & Fritz, 2010)
	Risk management	(Yue, Çakanyıldırım, Ryu, & Liu, 2007)
	Risk planning	(Rees, Deane, Rakes, & Baker, 2011)
User interface		(Maxion & Reeder, 2005)
Grid computing		(Cody, Sharman, Rao, & Upadhyaya, 2008)
Consumer information		(Lee, Kauffman, & Sougstad, 2011)

3.3.1 The Perceived Importance of Information Security

During the 1990s information systems managers, while they appreciated the pivotal role of information systems in the business process, failed to invest in information systems security (Straub Jr, 1990). A survey of the top information issues in the United States in the 1990s did not list information security among the top 10 issues; instead it ranked 19th out of the 20 issues identified (Niederman, Brancheau, & Wetherbe, 1991). This might have been because users lacked security awareness at the time (Goodhue & Straub, 1991). There was a gap between the use of modern technology and the understanding of the threats posed by the evolution from mainframe to client-server computing. This was apparent in the information systems managers ranking intentional threats by employees and competitors as the least likely threats during the 1990s (Loch, Carr, & Warkentin, 1992). However, a study by Warkentin and Willison (2009) from a survey of 1400 companies in 50 countries claims that currently one of the greatest threats to information security is believed to be insider threat. Insiders, defined as internal perpetrators

(Wang, Gupta, & Raj, 2015) are motivated to commit computer related crimes due to personal factors, work conditions, and opportunities available to them (Dhillon & Moores, 2001). Further, due to the increasing exposure and vulnerability of information systems to various types of security attacks since the 1990s, information security is now considered a holistic and organizational concern (El-Gayar & Fritz, 2010) and there is considerable awareness among ordinary users of threats posed by hackers, and Internet threats like viruses, worms and Trojan horses (Siponen, et al., 2014). Figure 5 illustrates the change in perspectives from the 1990s to the 2000s.

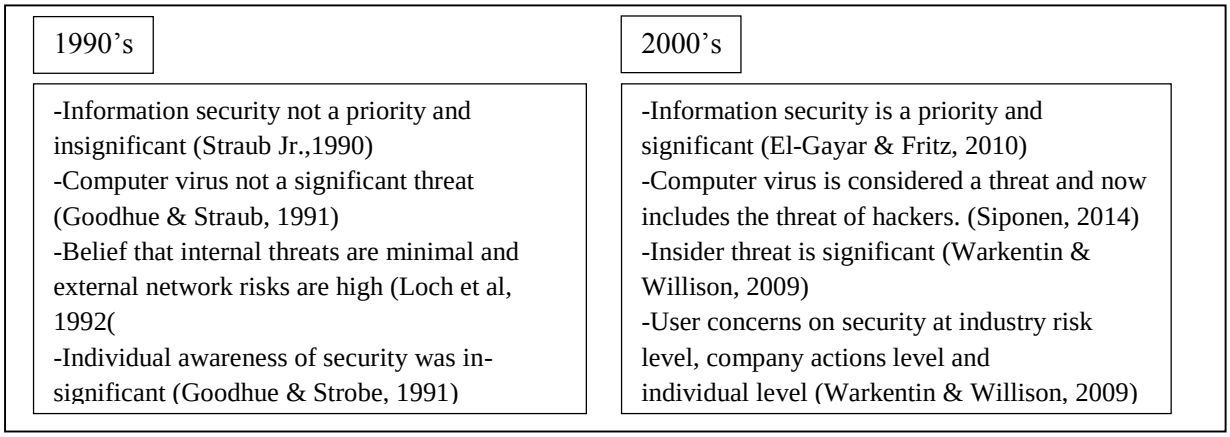

Figure 5: The change of perception from the 1990s to the 2000s

3.3.2 Deterrence

Deterrence is a mechanism which uses punishment as a threat to people who may abuse an information system (D'Arcy, Hovav and Galletta, 2009). Straub (1990) argues that the collection of activities and controls that deter computer abuse can be termed security countermeasures which can result in significantly lower computer abuse Security countermeasures used for deterrence include firewalls, intrusion detection systems and antivirus software (Wang, et al., 2015). From the behavioural angle, information system managers should be able to perform deterrent and preventive actions, detective actions, and disciplinary actions as countermeasures of information security. In this regard, Straub and Nance (1990) presented a normative model of the detection and discipline process. The authors claim that this model could be incorporated into an organization's technology management practices and evolve in time to bring system abuse in line with other organizational control objectives.

D'Arcy et al., (2009), referring to the general deterrence theory, argue that certain controls can function as deterrent mechanisms by increasing the threat of punishment for information

security misuse. Their study reveals that the three ingredients – user awareness of security policies, security education, training and awareness (SETA) programs, and computer monitoring – are significant in deterring computer abuse. Deterrence strategies such as signalling superiority levels of protection could discourage potential attackers (Cremonini & Nizovtsev, 2009). Using a game-theoretic setting, Cremonini and Nizovtsev (2009) argue that financially motivated attackers have the propensity to attack less-protected sites. Therefore, it can be inferred that high levels of protection can be a deterrent factor.

Two important aspects that need to be considered by information security managers are discovery of abuse incidents and discipline of perpetrators (Straub & Nance, 1990). In this regard, Straub and Nance (1990) propose a model designed to manage these two issues. The proposed activities that make up this model are to use internal controls to verify the occurrence of an abuse and identify the perpetrator. The model then stresses that once the perpetrator has been identified, he or she should be disciplined by giving a punishment that fits the crime. This would be the most challenging part as most of the organizations do not report system abuse to enforcement authorities due to the possible law suits or due to negative publicity (Gordon, Loeb, Lucyshyn, & Richardson, 2005; Richardson, 2008). Therefore, a punishment that may create negative publicity is generally avoided but the very basis of the general deterrence theory stands on the disposition that all individuals are rational actors who work by changing the costs and benefits of the situation so that criminal activity becomes an unattractive option (Carlsmith, Darley, & Robinson, 2002). Therefore, when organizations take such inhibitive approaches potential abusers may weigh the cost benefit in committing an abuse in their own favour.

Having a system in place to monitor information security behaviours can be a challenging task (Herath & Rao, 2009a). While proposing a model of the incentive effects of penalties and pressures, the authors claim that severity of punishment has a negative effect on security behaviour intentions. This claim is supported by Liao, Gurung, and Li (2009), K. Guo, Archer, and Connelly (2011), and Princely (2012), whose expectations that users were influenced by severity of punishment and punishment certainty were not supported by the results of their studies. Contrary to their findings on the effects of punishment, D'Arcy et al. (2009) claim that perceived severity of sanctions is more effective in reducing information security misuse. Li et al. (2010) meanwhile suggest that the deterrence effect of formal sanctions is greater when detection probability is higher than sanction severity. Furthermore, personal self-sanctions and workgroup sanctions seem to have a greater deterrence effect on information security violations (Guo & Yuan, 2012).

To sum up the argument on deterrence, it can be concluded that deterrence based research has been generally inconclusive, as observed by D'Arcy et al., (2009). The behavioural aspects studied have been general user behaviour internal to the organization, irrespective of a particular industry or environment. The question is whether the behavioural pattern towards the deterrence strategies discussed will have a different outcome if observed under inter-organizational lenses and specific environments. Figure 6 presents a summary of other relevant information such as the methodologies and theoretical frameworks used in the studies discussed in this subsection.

Findings in Deterrence

- ✓ Administrative and Management procedures are good tools (Straub & Nance, 1990).
- ✓ Perceived behavioural control and subjective norms are significant (Princely, 2012).
- ✓ Influence of punishment severity not a deterrent (Liao et al., 2009).
- ✓ In some cases perceived severity of sanctions is less effective than certainty of sanctions (Herath and Rao, 2009a).
- ✓ In some cases perceived severity of sanctions is more effective than certainty of sanctions (D'Arcy et al., 2009).
- ✓ Pressures exerted by subjective norms and peer behaviour are good deterrents (K. Guo et al., 2011).
- ✓ Certainty of detection is significant (Herath and Rao, 2009a).
- ✓ Personal self-sanctions and work group sanctions have deterrence effects (K. Guo et al., 2011).
- ✓ Signalling of superior level of protection acts as a good deterrence (Cremonini, 2009).
- ✓ Studies of Deterrence on IS research are inconclusive (D'Arcy et al, 2009)

Theoretical Frameworks applied in the findings of Deterrence

- Criminological theory of General Deterrence
- Theory of Planned Behaviour
- Protection Motivation Theory
- General Deterrence Theory
- Theory of Ethics
- Principle Agent Model
- Routines Active Theory

Methodology and Analysis used in the findings of Deterrence

Quantitative Survey (88%) →Analysis: PLS SEM (67%); Game Theory Simulation: (11%)

Figure 6: Literature on information security misuse deterrence

3.3.3 Risk Management and Analysis

Risk management is defined as a proactive process inclined towards expected favourable outcomes by integrating flexible means to respond to any risk related occurrence (Benaroch, Lichtenstein, & Robinson, 2006). On the other hand risk analysis from a conventional perspective is the use of monetary units for measuring the severity of risk (Baskerville & Stage,

1996). Risk analysis can be done with available data; however most of the security breaches are not reported since organizations do not have a formal obligation. Information security is required because the technology applied to information create risks (Blakley, McDermott, & Geer, 2001). Further, Blakely et al., (2001) claim that information security risk analysis methodologies were developed long ago and these methodologies have been included in formal security standards. Security risk management is a continuous process of identifying and prioritizing security risks and implementing and monitoring countermeasures and safeguards (Spears & Barki, 2010). This process of risk management involves the strategies, policies, activities, roles, procedures and people used to manage security risk, while the resulting controls reduce the occurring or the negative effects of a breach (Spears & Barki, 2010). As far as people are concerned, Wang et al (2015) using routine activity theory claim that insider threat are increasingly difficult to prevent and detect and therefore is one of the major challenges of security risk management. They further claim that computer application characteristics (value, inertia, visibility, accessibility) and presence of guardians (data protection measures) significantly affect an application's risk of insider threat. There are several studies on information risk management (Benaroch et al, 2006), however it falls short of demonstrating that it meets practical needs.

Von Solms, van der Haar, von Solms, and Caelli (1994) proposed an information security evaluation tool which can be used by information security managers to put the various facets (information security policy, risk analysis and management, contingency planning, and disaster recovery) into perspective. Fifteen years later, Welinger (2009) revealed that tools used by practitioners to perform their security tasks still seemed to be insufficient in providing them with the required support, especially in the context of the interaction between the security practitioners and other stakeholders.

Lack of awareness by information security managers not only exposes organizations to various threats, but also inhibits them from applying of the full range of available controls to manage risks. Straub and Welke (1998) proposed an effective approach to deal with such a problem. The approach consists of the use of a security risk planning model, education and training in security awareness and a countermeasure matrix. Their work was advanced by Kotulic and Clark (2004), who presented a conceptual model to assist in the study of the security risk management program (SRM) process. Though the model was not successfully tested empirically, they claim that it would prove beneficial in the study of the SRM program process. A similar work in terms of security risk analysis and management is Lili, Srivastava, and Mock

(2006), which proposes an alternative methodology for the risk analysis of information security based on evidential reasoning and a belief function definition of risk. Added to this work on alternative methods is the work of Benaroch et al. (2006), where they argue that in order to effectively address the critical risks, managerial intuition should be supplemented with the use of formal real option models. Real option model based on real options theory are models which conceptualizes and values the importance of risks in terms of IT investments (Benaroch, et al., 2006). Figure 7 presents a summary of the studies discussed in this subsection.

Summary of findings on Risk Management and Analysis

- ✓ Unless performance model is managed by using established measurable goals, security assurances will be based on symbolism than effectiveness (Spears et.al 2013).
- ✓ Tools used for risk analysis are insufficient to provide support for complex and collaborative duties (Benaroch et al., 2006, Werlinger et al., 2009).
- ✓ Security risk planning, awareness, training and countermeasure matrix are the most effective controls in risk management (Straub and Welke, 1998).
- ✓ Evidential reasoning approach is an effective model for risk analysis (Lili et al., 2006).
- ✓ Insider threat is difficult to detect and prevent (Wang, et al., 2015).

Theoretical Frameworks

- Institutional Theory
- Theory of Belief functions
- The capability maturity model

Methods and Sample Sizes

- Qualitative (42%) → Max: 30 interviews; Min: 13 interviews
- Mathematical Models

Figure 7: Summary of findings on risk management and analysis

3.3.4 User Behaviour and Compliance

From the end-users' perspective, Ng, Kankanhalli, and Xu (2009) studies users' computer security behaviour and claim that perceived susceptibility, perceived benefits, and self-efficacy are the determinants of user security behaviour. Adams and Blandford (2005) examined the importance of users' security awareness and control, and found that the understanding of "communities of practice" can help to bridge the gap between organizational and end-user perspectives. A similar concern was addressed by de Paula (2005) who explored how end-users routinely encounter security issues and resolve these issues themselves in collaborative work groups. Dinev and Qing (2007) investigated users' behavioural intention towards the use of protective technologies against viruses, unauthorized access, disruptions, spyware and so on. Anderson and Agarwal (2010) in their study on the precautionary behaviour of the users in the context of these protective technologies call users "cybercitizens".

One potential threat of user behaviour is the disregard of security policies and procedures. Boss et al. (2009) explored this individual information security precaution-taking behaviour in a study and concluded that if the management has a watchful eye on user activities, users will comply. This phenomenon is termed "fear appeal" by Huang, Patrick Rau, Salvendy, Gao, and Zhou (2011). Similar investigations on disregard of security policies are presented by Myyry, Siponen, Pahnila, Vartiainen, and Vance (2009), using moral reasoning on compliance, and by Siponen and Vance (2010), using neutralization theory. To ensure that users comply with the user requirements, persuasive communications with an added element of fear incorporated could prove to be successful (Johnston & Warkentin, 2010). The more recent study by Johnston, Warkentin and Siponen (2015) claim that the effectiveness of fear appeal has been mostly studied using the protection motivation theory and it has been mis-specified and inadequate in describing the information security phenomena. In respect to this, they claim that informal sanction rhetoric effectively enhances conventional fear appeals, thereby providing a significant positive influence on compliance intentions. Informal sanction rhetoric is described as threats to the human asset which adds a dimension of personal relevance (Johnston et al., 2015).

In addition to "fear appealing", Huang et al. (2011) argue that changing perceived knowledge can also achieve compliance. This is in line with studies by Puhakainen and Siponen (2010) and Dodge Jr., Carver, and Ferguson (2007) who note that training is the most commonly suggested information security policy compliance strategy found in the literature and propose empirically validated training programs to support this strategy. A more recent study by Jai-Yeol (2011), using both intrinsic and extrinsic models, showed that employees' security-related rule-following behaviour towards compliance is more significant in the intrinsic motivation model.

Through exploration of the threats posed by employee computer crime ("insider threat"), Robert (2006) offers a theoretical framework to analyse the offender–context relationship. Herath and Rao (2009b), propose a model that shows the adoption of compliance behaviour (adoption of information security practices and policies) by employees is affected by organizational security culture, which includes organizational, environmental, and behavioural factors. This notion is in line with findings of K. Guo et al. (2011) and Bulgurcu, Cavusoglu, and Benbasat (2010), who stress the importance of cultivating a culture of secure behaviour within an organization. In relation to this security culture, Posey, Bennett, and Roberts (2011)

argue that fostering interpersonal and environmental factors leading to the employees' belief in the organization's trust in them leads to a positive attitude towards security.

Behavioural aspects such as attitude, belief, and intention are captured by a model developed to explain employee's adherence to security policies by combining protection motivation theory, the theory of reasoned action, and cognitive evaluation theory (Siponen, et al., 2014). The findings from the application of this model show that the following behaviours have a significant and positive effect on the employees' intention to comply with information security policies: (a) perceived severity of potential information security threats, (b) employees' belief as to whether they can abide by the information security policies, (b) perceived vulnerability to potential security threats, (c) employees' attitude toward complying, and (d) social norms towards complying. Further, the intention to comply with information security policies also had a significant impact on actual compliance with these policies (Siponen, et al., 2014).

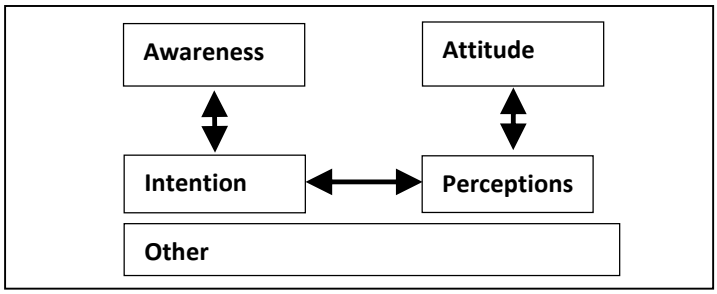

Figure 8: Aspects of user compliance behaviour in the information security literature

Figure **8** shows a simplified linkage diagram of the behavioural aspects discussed in this subsection. Figure 9 present a summary of other relevant information relating to the studies discussed in this subsection, including the theoretical frameworks, methodologies, and analyses used.

Summary of findings

- ✓ **Awareness**: Awareness is significant (Adams & Blandford, 2005; Huang, Patrick Rau, Salvendy, Gao, & Zhou, 2011)
- ✓ **Attitudes**: Attitudes are significant (Bulgurcu, Cavusoglu, & Benbasat, 2010; Ifinedo, 2014).
- ✓ **Intentions**: Intentions play a key role (Anderson & Agarwal, 2010; Herath & Rao, 2009b; Ifinedo, 2014; Johnston & Warkentin, 2010; Li, Zhang, & Sarathy, 2010; Siponen, Adam Mahmood, & Pahnila, 2014; Siponen & Vance, 2010).
- ✓ **Perceptions**: Perceptions play an important role (Boss, Kirsch, Angermeier, Shingler, & Boss, 2009; Li, et al., 2010; Ng, Kankanhalli, & Xu, 2009).
- ✓ **Intentions and Perceptions:** perception is a key determinant of intentions (Guo, Yuan, Archer, & Connelly, 2011).
- ✓ **Awareness and Intention:** Is a strong predictor (Dinev & Qing, 2007) and influences behaviour (Dinev & Qing, 2007).
- ✓ **Attitude and Perceptions:** Perception influences attitude (Guo, Yuan, et al., 2011; Herath & Rao, 2009b; Siponen, et al., 2014).
- ✓ **Other forms of user compliance:** Habitual (Vance, Siponen, & Pahnila, 2012) , past behaviour (Vance, et al., 2012), intrinsic and extrinsic motivation (Jai-Yeol, 2011), specifying policies and evaluating behaviours (Boss, et al., 2009).

Theoretical frameworks

- Theory of planned behaviour
- Social cognitive theory
- Social bond theory
- Protection motivation theory
- Habit theory
- General deterrence theory
- Neutralization theory
- Situational crime prevention
- Health belief model
- Theory of cognitive moral development
- Theory of motivational types values
- Theory of reasoned action
- Theory of planned behaviour
- Theory of technology acceptance
- Theory of rational choice
- The cognitive evaluation theory

Methodology and Analysis methods

				Sample Size	
Methodology	**(%)**	**Analysis**	**(%)**	**Min**	**Max**
Quantitative	70%	PLS-SEM	70%	124	1698
		Regression	30%	132	134
Qualitative	30%			20	64

Figure 9: Summary of findings on user compliance behaviour

3.3.5 Organizational Information Security Behaviour

Studies of organizational information security should go beyond technical considerations and adopt organizationally grounded principles and values (Dhillon & Torkzadeh, 2006). Using stakeholder values as a means to understand socio-organizational aspects, Dhillon and Torkzadeh (2006) presented a list of fundamental objectives. These fundamental objectives are (a) enhance management development practices, (b) provide adequate human resource management practices, (c) develop and sustain an ethical environment, and (d) maximise access control.

One of the main activities performed by organizations to portray their commitment to securing their business practices is the adoption of information security management guidelines. In this regard, Siponen and Willison (2009) give a very detailed explanation of the validity and applicability of various prominent international guidelines. A study conducted by Theoharidou, Kokolakis, Karyda, and Kiountouzis (2005) singled out one of the most dominant standards in information security management (ISO17799) for scrutiny, and concluded that it is aligned with the oldest criminology theory, the general deterrence theory. This theory, based on psychology, explains a behavioural process whereby if individuals perceive legal sanctions as certain, swift and/or severe, they are deterred from committing criminal acts (Williams & Hawkins, 1986). A more recent study has examined the extent to which such standards have been integrated into organizations' internal control (Wallace, 2011). The findings of the study suggest that differences exist in security controls implementation in relation to the status (public and private) and size of the firm, as well as the industry in which the company operates in. Studying the power relations during the adoption of an information security standard mandated by a head of government indicate that the adoption of these standards within organizations is not an easy task (Backhouse, et al., 2006). Furthermore, a study of alternative information security policies show facilitating end-user precautions is more effective than enforcement against attackers when the cost of precautions and the cost of attacks are lower (Png & Wang, 2009).

From an organizational perspective, the focus is still on prevention towards information security threats when there should be a strategic balance between prevention and response (Baskerville, et al., 2014). However, this also depends on the environment of the organization; in a more stable environment prevention may take precedence over response and vice versa (Baskerville, et al., 2014). Figure 10 presents a summary of the theoretical frameworks and methodologies applied in the studies discussed in this subsection.

Categories and summary of findings of literature on Organizational information security compliance behaviour.

1. **Security Strategies**
   - ✓ Information security strategies employ prevention and response paradigms. (Baskerville, Spagnoletti, & Kim, 2014)
   - ✓ Organizations choose to balance between prevention and response as ground for its current information security posture. (Baskerville, et al., 2014)
   - ✓ As a strategy for both mass and targeted attacks, facilitating end-user precautions reduces the expected loss of end users. (Png & Wang, 2009)

2. **International Security Standards**
   - ✓ International standards are generic or universal in scope. (Siponen & Willison, 2009)
   - ✓ In the formulation of the international standards enough attention is not paid to the differences between organizations and their varying security requirements. (Siponen & Willison, 2009)
   - ✓ International standards are validated by appeal to common practice and authority. (Siponen & Willison, 2009)

3. **Adoption of Security Standards**
   - ✓ Factors contributing to resistance to adopt standards can be group norms and cultural biases. (Backhouse, Hsu, & Silva, 2006)
   - ✓ In addition to institutional forces there are other economic base considerations that influences on the degree of the adoption and assimilation of information security management(Hsu, Lee, & Straub, 2012)
   - ✓ Implementation of suggestive controls from international standards depends on a company's status as public, private, the size of the company and in the industry which it operates. (Wallace, 2011)
   - ✓ Maintaining IS Security in organizations, it is necessary to go beyond technical considerations and adopt organizationally grounded principles and values. (Dhillon & Torkzadeh, 2006)
   - ✓ Mandated standards can be inhibited by insufficient resource allocation, lack of senior management input and commitment(Backhouse, et al., 2006)

Theoretical Frameworks

- ✓ Incident Centered Security Framework
- ✓ Institutional Theory on Innovation Diffusion

Methodologies and Analysis methods

Methodology	No of studies (%)	Sample size Min	Max
Quantitative	14	140	636
Qualitative	58	10	103
Content analysis	14	-	-
Mixed method	14	-	-

Figure 10: Summary of organizational compliance behaviour studies

3.3.6 Inter-Organizational Information Security Behaviour

An exhaustive search for journal articles on information security compliance behaviour (ISCB) in an inter-organizational context returned no hits. However, there were studies that discussed issues such as trust and privacy in inter-organizational information exchange between health organizations (van der Linden, Kalra, Hasman, & Talmon, 2009), and technology trust in B2B in online transactions in e-commerce relationships (Ratnasingam, 2005). In the context of supply chains, the inter-organization studies explored information and knowledge sharing for competitive advantage (Warkentin, Bapna, & Sugumaran, 2001), quality of shared information (Li & Lin, 2006), and the type of information shared (Li, Sikora, Shaw, & Woo Tan, 2006). One study that roughly fits into this category is D'Aubeterre, Singh, and Iyer (2008), which investigates the process of securing and cultivating the information supply chain while focusing on information exchange for production, purchasing, inventory and demand forecasting.

3.3.7 Summary of Information Security Literature

The literature review of information security studies revealed technical and behavioural aspects as the two main areas of focus. Table 1 summarizes the technical aspects. The findings on behavioural aspects fall into five main categories: perceived importance of information security (Appendix F: Table 30), deterring threats (Appendix F: Table 31), risk management and analysis (Appendix F: Table 32), user behaviour and compliance (Appendix F: Table 33), and organizational information security behaviour (Appendix F: Table 34). Most of these studies have borrowed from social and criminology theories such as protection motivation theory, general deterrence theory, and the theory of reasoned behaviour, to name a few, in explaining information security behaviour. These behavioural aspects have been mostly studied at user or employee levels internal to organizations. There are very few studies that consider information security aspects within an inter-organizational context.

3.4 Supply Chain Security

SCS is an emerging field of research within SCM and is a subcomponent of the overall risk management strategy of the supply chain (Closs & McGarrell, 2004; Toosi, et al., 2014). Significant elements of SCS include information sharing (Closs & McGarrell, 2004), information security (Lee & Wolfe, 2003), and gathering information for intelligence (Flynn, 2000). With the need to protect national borders against terrorists using conveyances or containers to ship WMD or harmful bio-weapons, SCS has become a key concern for many

countries today (Closs & McGarrell, 2004; Lee & Whang, 2005; Urciuoli, 2010). Security is an important aspect for SCM because of its complexity, dependence on several stakeholders, and need for extensive trust and commitment between supply chain partners (Sarathy, 2006). SCS is a combination of traditional practices of SCM and security requirements. However, little empirical literature supports policy or practice in this emerging field (Williams, Jason, & Stephen, 2008). Furthermore, most studies in this area examine the physical supply chain which addresses the transporting of cargo (Molm, 1991), not informational aspects.

Following Closs and McGarrell (2004), SCS is usually defined as:

> the application of policies, procedures, and technology to protect supply again assets (products, facilities, equipment, information and personnel) from theft, damage, or terrorism, and to prevent the introduction of unauthorized contraband, people or weapons of mass destruction into the supply chain. (p. 8)

Voss, Whipple, and Closs (2012) reviewed a comprehensive list of SCS studies published up to 2009, of which 45% were conceptual studies. Of the reviewed articles, more than 50% mention the September 11, 2001, terrorist attacks on the United States and therefore it can be inferred that the academic interest in this area has increased since this event. Based on the authors' locations, many studies originate from the United States. Half of the studies focus on defining supply chain risks or outlining risk mitigation strategies (Vespignani, 2012). These risk mitigation strategies are very much based on Customs-Trade Partnership Against Terrorism (C-TPAT) security initiative advocated by the United States (Maurer, 2010).

Some of the most cited works in SCS such as Sheffi (2001), Closs and McGarrell (2004), and Lee and Whang (2005) are conceptual. However, the literature also reveals many insights relating to industry and the environment and linked to empirically grounded and well-established academic areas and theories. For instance, Sheffi (2001) links SCS to concepts of inventory management such as Just In Time (JIT) delivery, information sharing, shipment visibility, supplier relationships, and risk pooling, all of which are importance fields in their own right. Although the well-cited article by Closs and McGarrell (2004) was published in a trade journal for practitioners, it has proven to be a guiding source in defining the scope of SCS for academics. It covers areas which have caught academic interest in recent times such as the dimensions of security within the supply chain (Maurer, 2010), integration of security into supply chain (Toosi, et al., 2014), requirements and roles of SCS, and assessment of SCS

(Vespignani, 2012). Finally, Lee and Whang (2005) explore the principles of total quality management in relation to assuring the security of the supply chain.

Martens (2011) reports four major elements that influence the effectiveness of SCS: (1) motivational considerations, (2) resource constraints, (3) internal and external integration, and (4) training measurement. The focus of this thesis is on the first element, motivational considerations, as global security initiatives promise preferential treatments for trading partners to motivate them towards compliance. These motivational considerations include security certification through public-private partnerships (PPPs) enforced by security initiatives such as C-TPAT and the Container Security Initiative (CSI). Certified firms outperform non-certified firms in security performance, firm performance, and resilience (Mizruchi & Fein, 1999). However, critics suggest that current procedures involving cargo in regard to SCS need to be harmonized and more emphasis should be put on a collaborative industry-driven SCS (Domingues et al., 2014). Harmonization would guarantee compatibility between security initiatives and establish mutual recognition (Gutierrez & Hintsa, 2006), while collaboration would result in more sustainable compliance opposed to reaction from coercion (Marucheck, Greis, Mena, & Cai, 2011). Similarly, a critical analysis is needed on the impact of the compliance certification and PPP on inventory management. The results from dynamic modelling of SCS operations suggest that increasing security measures at international borders can increase inventory levels up to as much as 600% compared to normal operating conditions (Scott, 1995).

Most of the GSCS initiatives are voluntary. However, some have become part of the law in various countries (Ke & Wei, 2008; Sarathy, 2006; Wagner, et al., 2011). This has forced companies to adopt new technologies to meet the requirements of the GSCS initiatives (Banomyong, 2005; Osarenkhoe, 2010) and to look for GSCS-compliant partners (Osarenkhoe, 2010; Sheu, et al., 2006; Wagner, et al., 2011). Companies face the threat of being cut off from the supply chain if they do not comply (Banomyong, 2005; Sheu, et al., 2006). While the authorities promise benefits in terms of rewards and fair treatment for the compliance efforts of traders, they also threaten to delay shipments at the border with lengthy physical inspections for all non-complying traders (Banomyong, 2005; Sheu, et al., 2006). The GSCS initiatives will be the norms of operation in the future and the stakeholders need greater awareness and understanding of security issues to shift their beliefs, attitudes and intentions towards compliance (Banomyong, 2005; Sheu, et al., 2006; Wagner, et al., 2011).

Information management and information sharing are key factors in the overall security of the supply chain (Gutierrez & Hintsa, 2006). Information sharing, in the context of SCS, focuses on the degree to which supply chains share accurate information in a timely manner to address security-related incidents (Wu, et al., 2014). While information security is a critical component of global supply chains, and there are many threats to the integrity, confidentiality and availability of information (Workman, Bommer, & Straub, 2008), there is no specific study on information security in the context of SCS (Smith, Watson, Baker, & Pokorski, 2007). The few studies that have been done on international SCS have overlooked the critical role of information technology (IT) in SCS (Lee, Palekar, et al., 2011). This may be due to the fact that academic research on SCS is still in its infancy (Sheu, et al., 2006). Moreover, information security research has traditionally focused on security in e-commerce in business organizations (Smith, Winchester, Bunker, & Jamieson, 2010). The SCS literature clearly lacks specific focus on information security. However, most of the SCS literature refers to and accepts information security as a key concern while addressing SCS. For instance, Harland, Brenchley and Walker (2003) argues that information security vulnerability may occur at different management levels, while Tang (1990) notes that securing information through technology is important to establish SCS. Further, Banomyong (2005) highlights secure information flow as a key factor in the process of establishing SCS. As all security initiatives heavily depend on the capture of accurate information for the effective targeting of security threats, if the information is falsified through a breach of security, these initiatives become ineffective (Sarathy, 2006).

A review of the top 52 journals in the fields of SCM and information systems by Gunasekaran and Ngai (2004) revealed that the literature can be classified into six main categories: (1) strategic planning for IT, (2) virtual enterprise, (3) e-commerce, (4) infrastructure for IT, (5) knowledge and IT management, and (6) implementation of IT. This shows the absence of information security as an area of research within the supply chain context. However, Chang, Xu and Song (2014) reveal that though security damage and the risks associated with physical flow are as a whole more likely to have serious impacts than the risks associated with information flow, the most serious of the risk factors associated with information flow, in terms of seriousness of impact, was shippers hiding cargo information. Accordingly, information management partnership/relationships have significant positive effects on safety performance (Haughton & Isotupa, 2013)

3.4.1 Summary of SCS Literature

The literature on SCS contains more conceptual than empirical studies and the subject has yet not assumed a prominent position in mainstream academic journals. It can be inferred that mainstream journals still treat SCS as a component of overall risk management which does not need to be studied in isolation. Hence, leading journals see SCS as a terminology to be used when discussing supply chain disruptions and other forms of risks. For supporting evidence of this claim, the reader is referred to the tabulated summary of literature review on SCS by Voss et al. (2009) in Appendix E, Table 27, where most of the literature classified as SCS is not centrally focused on SCS. While the studies mention SCS they in fact address disruptions and risk management within SCM. Whenever there is a specific focus on SCS in publications, it appears mostly in trade journals rather than scholarly journals. To substantiate this argument, the reader is referred to the tabulated summary of SCS literature by Williams et al. (2009) in Appendix E, Table 28. An updated literature review summary table is also included in Appendix E, Table 29. Figure 11 categorizes the concepts found in the studies discussed in this subsection and Figure 12 categorizes their findings and methodologies. Figure 13 summarizes the findings from the studies using the identified categories.

The limited literature on SCS identifies information security as crucial to SCS. This link between SCS and information security has generated research interest in SCS. This is evident from recent studies such as Lu et al. (2013) that identify the significance of "big data" in ensuring SCS from an ICT supply chain perspective. While big data is currently a popular academic research topic, except for this conceptual work of Lu et al. (2013) there is little or no evidence of conceptual or empirically researched studies specific to information security within the context of SCS. This is evident from Williams et al. (2009), which expresses this concern by calling for future research on information security in the overall management of SCS.

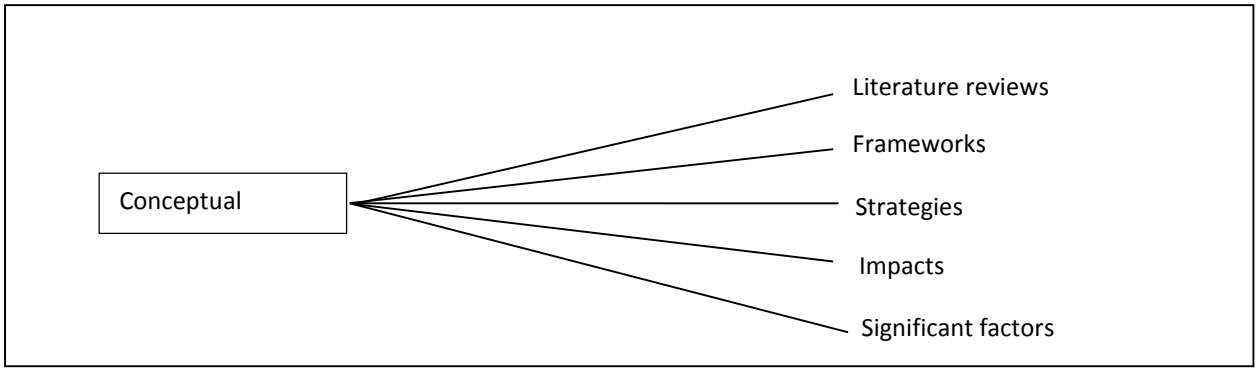

Figure 11: Categories of concepts discussed in the SCS literature

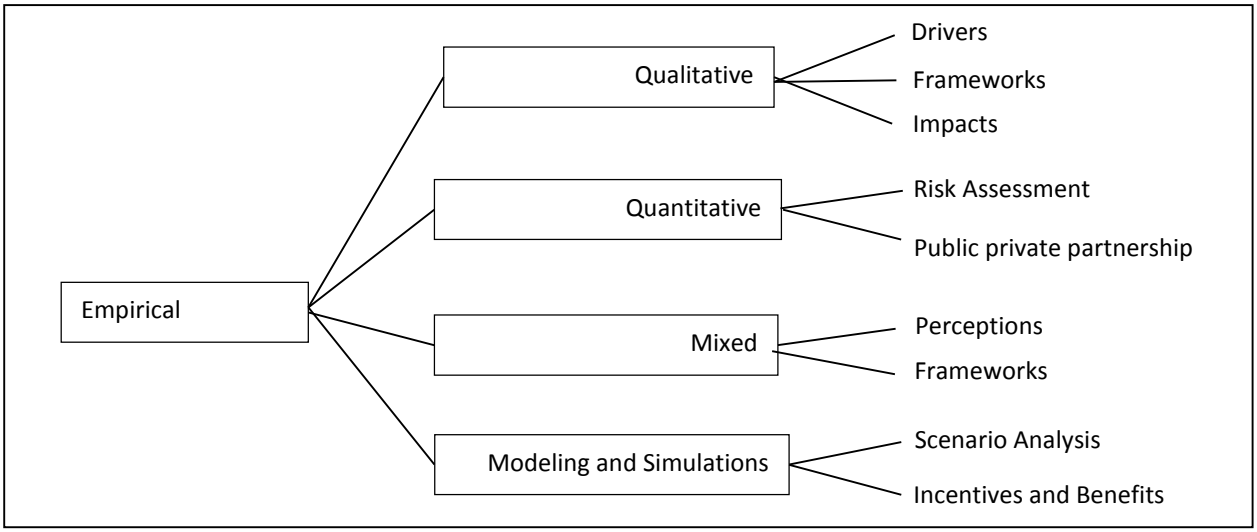

Figure 12: Categories of findings and methodologies in the SCS literature

Empirical Findings Summary

1. **Impacts of GSCS initiatives**
   - ✓ GSCS initiatives such as C-TPAT have significant impacts on the international trade (Sheu, Lee, & Niehoff, 2006).
2. **Drivers of SCS**
   - ✓ Four primary drivers of SCS are government, customers, competitors and society (Osarenkhoe, 2010).
3. **Frameworks**
   - ✓ To examine the threat of potential disruptions (Wu, Chuang, & Hsu, 2014)
   - ✓ Analysis of design and SCS standards for the benefit of government policy makers, supply chain and security experts (Hintsa, 2010).
4. **Incentives and Benefits**
   - ✓ When security concerns are not strong enough to dominate efficiency concerns, stakeholders may not have a sufficient incentive to invest; therefore, at least one stakeholder under invests (Lee, Palekar, & Qualls, 2011).
   - ✓ When security concerns are strong enough to dominate efficiency concerns, stakeholders may not invest at all because of the uncertainty of other stakeholders' behaviour, rather than the lack of an incentive to invest in the technology (Lee, Palekar, et al., 2011).
5. **Perceptions**
   - ✓ International firm's perception of security is higher and is more likely to assess the security procedures of their partners (Whipple, Voss, & Closs, 2009).
   - ✓ International firms perceive they perform better in terms of the ability to detect and recover from security incidents (Whipple, et al., 2009).
   - ✓ Internal and external integration efforts, a nodal planning focus, and proactive motivations related to security measures were found to be positively related to security effectiveness (Yang, 2010).
6. **Risk assessment and mitigation strategies**
   - ✓ Balance between the efficiency of maritime logistics and SCS is of vital importance to trading countries dealing with security risk issues (Banomyong, 2005)
   - ✓ Security initiatives depend on top management mindfulness, operational complexity, product risk, and coupling (Wu, et al., 2014).
   - ✓ Areas to be improved for SCS are government initiatives, management strategies, operative routines and technical system (Kostova & Roth, 2002).
7. **Partnerships**
   - ✓ Certified firms outperform noncertified firms in security performance, firm performance, and resilience (Mizruchi & Fein, 1999).
   - ✓ Security certification costs are justified in terms of achieving internal targets in performance (Mizruchi & Fein, 1999).

Figure 13: Summary of findings in the SCS literature

3.5 The Research Gap

Although the literature identifies several significant issues of compliance behaviour, most of these are related to individual behaviour leading to implications internal to the organization. It can be argued that a focus on inter-organizational compliance behaviour is lacking. It can also

be argued that ISCB is discussed irrespective of the industry or environment. In can therefore be concluded that similar to the lack of studies on ISCB in the SCS literature, the information security literature lacks a focus on compliance behaviour among the stakeholders of supply chain in the SCS context.

Thus, there is a research gap concerning ISCB in the context of SCS. The global cross-border supply chain is operating at a heightened security status, and border control authorities are demanding advance information of consignments and conveyances through electronic means. This information is used to gather intelligence to identify potentially dangerous cargo so that it can be targeted and selected well before it reaches the destination port. It is critical that the information transmitted by the market stakeholders possesses all the qualities and characteristics of information security so that it fully achieves the intended purpose. Therefore, knowledge of ISCB on the part of market stakeholders with respect to SCS is crucial. This knowledge would help to broaden understanding of how and why the market stakeholders are responding to the GSCS initiatives in terms of information security. Such knowledge would also further assist the stakeholders of the global supply chain to better plan and secure the supply chain in order to achieve the goals of the GSCS initiatives. Accordingly, a study with an inter-organizational focus is needed because SCS is increasingly governed by the GSCS initiatives (Huibin & Yuan, 2014).

3.6 Chapter Summary

An extensive review of the literature on SCS revealed that SCS is an emerging field of academic enquiry with limited literature. Compared to the SCS literature, the information security literature on socio-technical behavioural aspects is quite extensive and can be classified into six main categories: (1) perceived importance, (2) deterrence, (3) risk management and analysis, (4) user behaviour and compliance, (5) organizational information security behaviour, and (6) inter-organizational information security behaviour. However, the review also showed that ISCB in the SCS context is lacking in the academic literature. Hence, this is identified as a research gap. The next chapter will present the research questions that will assist in closing this research gap. In addition, the relevant theoretical frameworks and a conceptual model designed to answer the research questions will also be presented.

CHAPTER 4: RELEVANT THEORETICAL FRAMEWORKS AND CONCEPTUAL MODEL

4.1 Chapter Overview

The literature review conducted in the previous chapter identified information security compliance behaviour (ISCB) in the SCS context under the influence of the GSCS initiatives as a research gap. This chapter presents the two research questions posed by this study to assist in addressing this gap. In addition, relevant theoretical frameworks are discussed and a conceptual model formulated. Figure 14 summarizes this process.

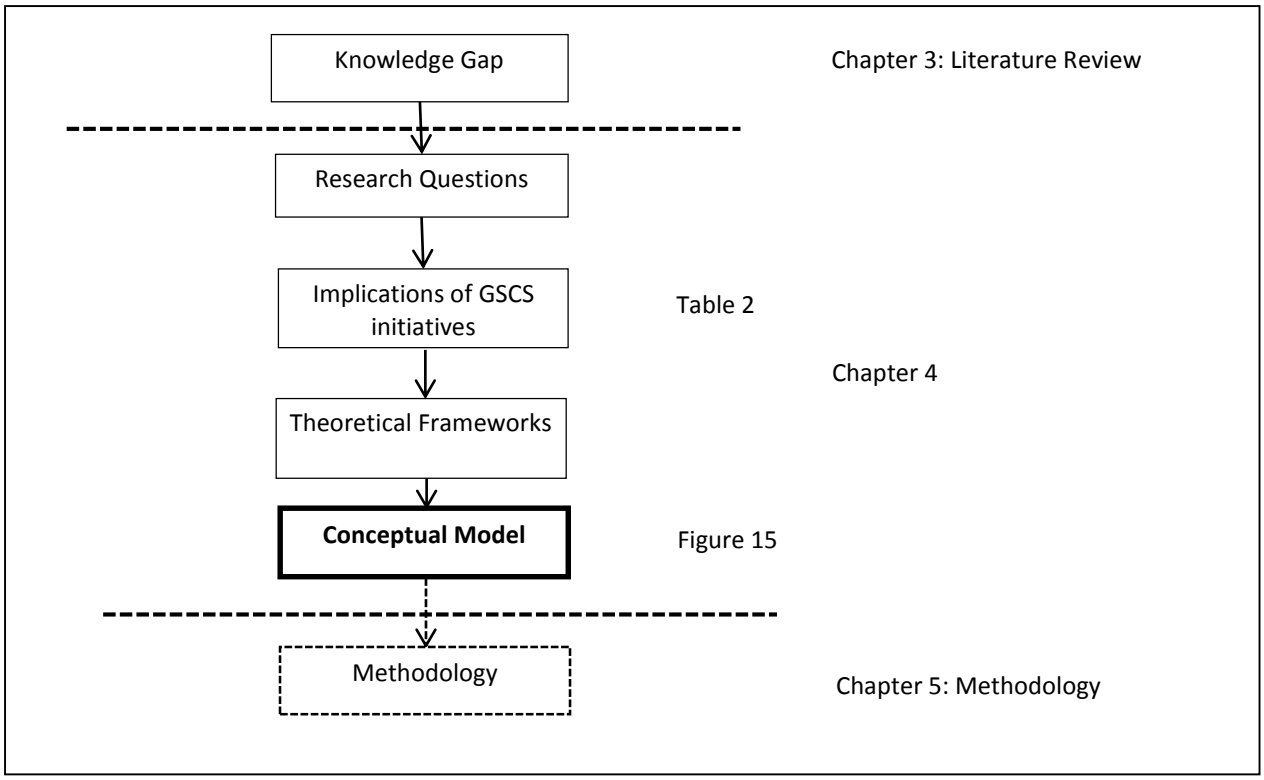

Figure 14: Steps taken to identify relevant theoretical frameworks and develop a conceptual model

4.2 Research Questions

In order to best fill the identified research gap, the following research questions were posed:

The overarching research question:

How do the supply chain security stakeholders comply with information security requirements mandated by the GSCS initiatives?

Sub research questions:

[RQ1] What are the drivers of ISCB and how do they impact the compliance behaviour exhibited by the stakeholders?

[RQ2] What factors influence inter-organizational ISCB in the context of the GSCS initiatives?

The first question addresses the current behaviour in the prevailing environment. The second question explores the impact of the influencing factors on the existing drivers which lead to this current behaviour. As mentioned earlier, the first step in trying to understand the current behaviour is to understand the implications that have occurred since the introduction or the implementation of the GSCS initiatives. In order to achieve this, the next section reviews the relevant literature on these implications.

4.3 Implications of the GSCS initiatives

In order to understand the prevailing environment of SCS against the backdrop of the GSCS initiatives, the implications of GSCS initiatives were identified from the literature. These implications were then classified into groups according to the type of influence imposed. This classification led to the identification of three main groups, which for the purposes of this research will be considered the categories that influence compliance behaviour in the given context. The three categories identified were (1) external inter-organizational influences, (2) rules and norms of social exchange, and (3) organizational perceptions. Table 2 presents these implications and the behavioural categories within the identified implications.

Table 2: Implications of the GSCS initiatives gathered from the literature

Implications of GSCS initiatives	Categories/Elements
Have become part of law in various countries (Ke & Wei, 2008; Sarathy, 2006; Wagner, et al., 2011)	- External inter-organizational influences Regulatory demands
Suppliers looking for GSCS initiatives compliant partners (Osarenkhoe, 2010; Sheu, et al., 2006; Wagner, et al., 2011)	- External inter-organizational influences Market influence
Peer companies adopting new technologies and specializations in their professions to meet the requirements of the GSCS initiatives. (Banomyong, 2005; Osarenkhoe, 2010)	- External inter-organizational influences Peer pressure
Promises benefits if complied with (Banomyong, 2005; Sarathy, 2006; Sheu, et al., 2006)	-Rules and norms of social exchange (reciprocity and fair treatment)

	-Organizational perceptions → Benefits
Threatens to cut off from supply chain if not complied with; Threatens to delay the shipment at the border for lengthy physical inspections (Banomyong, 2005; Sheu, et al., 2006)	-Organizational perceptions → Threats
Claims GSCS initiatives will be the norms of operation of the future (Banomyong, 2005; Sheu, et al., 2006)	-Organizational perceptions → Norms

4.4 Review of the Relevant Theoretical Frameworks

In order to study the effect of the behavioural categories in Table 2 in the given context, the theories that best explain these categories were identified from the literature. The outcome of this exercise revealed that the most relevant theoretical frameworks were institutional theory and social exchange theory (SET), the key themes of which are listed in Table 3. The following subsections give a brief overview of these two theories and their relevance to this research.

Table 3: Key themes and relevant theoretical frameworks

Implications from GSCS (see Table 2)	Identified constructs	Proposed theoretical framework	Relevance
External inter-organizational influences	Regulatory demands (coercive pressure)	Institutional theory	The more power an organization has the more influence it has to determine the nature of inter-organizational exchange and is the fundamental process in an exchange relationship (Cook, 1977).
	Market influence (Normative)	Institutional theory	Normative pressure is "the collective struggle of members of an occupation to define the conditions and methods of their work, to control the production of the future member professionals, and to establish a cognitive base and legitimization for their occupational autonomy" (DiMaggio & Powell, 1983).
	Competitive (Peer pressure)	Institutional theory	While technology is poorly understood and what could be achieved is ambiguous, organizations respond to uncertainty by mimicking actions of other organizations (DiMaggio & Powell, 1983; Lim & Palvia, 2001).
Organizational perceptions	Perception of benefits	SET and institutional theory	The reciprocal actions such as fairness and reward by the authorities can be perceived as beneficial by the organizations (Rodríguez & Wilson, 2002). Organizations do not change its ways just for efficiency but to reap the benefits of being a legitimate institute (DiMaggio & Powell, 1983). Institutional theory is complimentary to economic theory (Carpenter & Feroz, 2001), as such Institutional theory views organizations functioning within a social framework portraying economic behaviour (Oliver, 1997).
	Perception of threats (coercive)	Institutional theory	The power exerted by the state on organizations which refers to threat or actual use of force to gain compliance (DiMaggio & Powell, 1983; Lawrence, Winn, & Jennings, 2001; Liang, Saraf, Hu, & Xue, 2007).

Implications from GSCS (see Table 2)	Identified constructs	Proposed theoretical framework	Relevance
Rules and norms of social exchange	Perception of norms	Institutional Theory	According to institutional theory, for a given group of organizations deviation from group norms can result in inferior performance (DiMaggio & Powell, 1983). Research evidence suggests that firms competitive behaviour should match the perceived industry norm (Li, Li, & Cai, 2014) Norm is a standard behaviour practiced and those who follow these norms should have an obligation to behave reciprocally (Fan, Zhang, & Yen, 2014).
	Power and Dependence (Fairness)	SET	Fairness mediate satisfaction with a relation within the framework of exchange theory (Molm, 1991)
	Reciprocation (Reward)	SET	When benefits are greatly bestowed beyond the formal contracts of the exchange relationships, the benefitting member may feel obligated and willing to contribute (reciprocate) (Settoon, Bennett, & Liden, 1996).

4.4.1 Institutional Theory

Institutional theory was first developed by DiMaggio and Powell (1983) for examining the pace and stability of institutionalization. According to this theory, an organization changes its behaviour not necessarily to gain efficiency or in the face of competition, but more due to the need to legitimize its existence in its business environment. This effect is termed institutional isomorphism, and the authors propose coercive, mimetic and normative as the three facets that describe the three distinct processes of institutionalization (DiMaggio & Powell, 1983).

Coercive pressure often results from the actual use of force by the state or other powerful authorities in order to gain compliance (Kostova & Roth, 2002; Lawrence, et al., 2001). Eventually, these coercive pressures become regulative processes (Scott, 1995). Normative pressure is a result of the expectations of the peer group of a professional environment (Kostova & Roth, 2002; Zucker, 1987). The peer group must all belong to the same profession and interact through their professional network such as the trade associations (Mizruchi & Fein, 1999). Economic activities, such as supply chain activities, are embedded in the institutional context of the societal norms and expectations that define socially acceptable economic behaviour (Zukin & DiMaggio, 1990). Mimetic pressure arises as response to uncertainty when there is ambiguity and lack of a clear direction (Mizruchi & Fein, 1999). It stems from the perception that by following the more successful actors, they themselves become more effective and efficient (Lawrence, et al., 2001). Organizations seek guidance from the experiences of other organizations in comparable situations when facing uncertainty (DiMaggio & Powell, 1983) and are under mimetic pressure to keep up with others' standards of practice.

Numerous works related to information systems have utilized this theoretical lens. One specific work related to this study is the work of Hu, Hart and Cook (2007), who investigated the external and internal influences on information security systems. In a similar context, Cai, Liu, Xia, and Liu (2009) studied the implementation of integration of information in the supply chain. Other areas in which this theory has been applied include studies on the role of green information security in environment stability (Butler, 2010) and changes in accounting and financial information systems (Tsamenyi, Cullen, & González, 2006), to name just a few.

One area of application of institutional theory in the literature is to the institutional environment (Zucker, 1987) because the rules that governs these organizations are formed at the state or even at the global level, which are external and hierarchically superior to the organization

(Thomas & Meyer 1984, Meyer & Hannan 1979). While referring to DiMaggio and Powell (1983), Zucker (1987) states that the institutional environment known as the "organization field" is defined in terms of increased density of interaction, information flows, and membership identification. These arguments when considered closely reflect similar characteristics of a supply chain environment. For instance, GSCS initiatives are enforced as global security requirements at an international level and also at a state level by local laws and regulations. Further, one of the main components of these security initiatives is information flow within identified members of the institutional environment.

Institutional theory has relevance to this study because generally compliance requirements demanded by the authorities (in this case both the local customs and the customs of the importing country) are met under institutional pressure. It is therefore of academic interest to investigate the impacts on the compliance behaviour aspect of information security in terms of the facets of institutional pressure, especially in terms of substantive or symbolic compliance. Symbolic compliance is when the attributes of compliance are not implemented in a meaningful way (Westphal & Zajac, 1995). Referring to symbolic compliance as "ceremonial adoption", Kostova and Roth (2002) state that it involves a relatively high level of implementation with a low level of internalization. This implies that though the market stakeholder formally complies with the authorities requirements, the market stakeholder does not view the practice as valuable and does not have a positive attitude towards it.

The implications identified in Table 2 specify broad categories such as external inter-organizational influences, organizational perceptions, and rules and norms of social exchange. These categories are in turn broken down to specific elements. In this respect, external inter-organizational influences are defined by (a) regulatory demands, (b) market influence, and (c) peer pressure. These elements portray similar behavioural aspects as those outlined in institutional theory.

Institutional theory can also be used to explain organizational perceptions. For instance, Whitford (2002) discusses how institutional theory helps to explain decision making under the perception of threats and uncertainty. Institutional theory is complementary to economic theory (Carpenter & Feroz, 2001) and as such institutional theory views organizations functioning within a social framework as portraying economic behaviour (Oliver, 1997). This inference suggests institutional theory can explain the behaviour of an organization when it perceives benefits from its operating environment. The benefits come in the form of rewards for being

similar to the legitimate organizations in the same environment (DiMaggio & Powell, 1983). In the given context, legitimate organizations maybe referred to as other supply chain stakeholders which are recognized by the authorities as complying with SCS requirements.

4.4.2 Social Exchange Theory

According to SET, the fundamental processes in an exchange relation are the processes of power, dependence (Stevens, Kevin Steensma, Harrison, & Cochran, 2005), and reciprocity (Fan, et al., 2014). The foundational ideas of SET's explanatory power are: (a) rules and norms of exchange, (b) resources exchanged, and (c) relationships that emerge (Fan, et al., 2014) and the theory is used in this study to help explain the compliance behaviour aspect of information security within an inter-organizational context. The concepts of power and dependence in the context of SET are explained by Cook (1977), who states that the more power an organization has, the more influence it has to determine the nature of the inter-organizational exchange. He also argues that an organization is less dependent on exchange relations with other organizations in its local environment to the extent that it has accessibility to elements it needs from other sources. However, in the context under investigation, the authorities (customs and ports) only depend on the set of organizations that have a need to trade with the outside world. At the other end, the traders and associated stakeholders such as the brokers and logistics providers depend on these authorities for smooth and timely operations. There is no alternative source performing the same function. When there are no alternatives, organizations may be dependent on a single authority for their survival (Jacobs, 1974); in the research context, the authorities have greater opportunity to exert power on the rest of the stakeholders. This creates a fear of uncertainty among the traders. To overcome this uncertainty the market stakeholders will fully comply with the requests of the authorities in order to avoid any delays of their cargo at the border, as the cost of delayed cargo may prove to be more costly than the cost of compliance. However, Cook (1977) argues that in such a situation, in addition to the creation of a negotiated environment between the authorities and the rest of the stakeholders, there might be a formation of a coalition in the form of alliances or mergers within the exchange network to increase their bargaining power. Further, when there is increased cooperation among organizations this creates the opportunity to exert power on the single most powerful organization (customs or port authorities in this context) (Provan, Beyer, & Kruytbosch, 1980).

The other important construct of SET is reciprocity. The use of SET in models of organizational behaviour is formulated on the basis of exchange rule, which focuses on expectations of

reciprocity (Fan, et al., 2014). Cropanzano and Mitchell (2005) identified three types of reciprocity as (a) interdependent exchanges: an action of one party leads to a response by another, (b) cultural: expectation that people get what they deserve, and (c) moral norm: a standard that describes how one should behave and those who follow these norms are obligated to behave reciprocally. As seen in Table 2, several themes that emerge from the existing literature on compliance behaviour seem to have behavioural characteristics which correspond to these types of reciprocity. In this respect, SET portrays interactions similar to economic exchange where people take part in an activity only if the outcomes involve a reward (Gefen, Karahanna, & Straub, 2003).

Fairness is a contribution that enhances quality and desirability of an ongoing relationship and in turn obligates one to reciprocate in ways that preserve the social exchange relationship through voluntary behaviours that benefit the party who treated one fairly (Masterson, Lewis, Goldman, & Taylor, 2000). Such actions by non-market stakeholders within the social exchange framework are perceived as beneficial by the market stakeholders.

The use of SET in inter-organizational behaviour has been reported in many studies, especially in buyer–supplier relations (Anderson & Narus, 1990; Griffith, Harvey, & Lusch, 2006). In this respect, Griffith et al. (2006) analyse the significance of fairness in buyer–supplier relationships and Wagner et al. (2011), referring to Thorelli (1986), evaluate reward as a preconceived expectation in a collaboration exchange relation between two firms. The literature on SET clearly identifies that when exchange of sensitive information occurs in an inter-organizational context, reciprocity through fairness and rewards plays an important role in compliance behaviour, as the benefit that one party obtains from cooperation should have an obvious positive effect on the exchange partner (Rodríguez & Wilson, 2002). This explains the perception of benefits through reciprocity. Hence, these three concepts of fairness, reciprocity (reward) and perceptions of benefits from SET will be used to understand compliance behaviour in the context of this study.

As Chapter 3 established, there is no focus on ISCB in the SCS context in the extant literature. However, there are several implications for this context that can be inferred from the literature, which were presented in Table 2. Further, as shown in Table 3, focusing on these implications led to the identification of two relevant theoretical frameworks. Referring back to the literature review, institutional theory and SET are two of the least used theories in studying ISCB in any given context, while the most commonly applied theoretical frameworks are protection

motivation theory and the theory of planned behaviour. This can be observed by referring to the relevant tables presented in the literature review in Chapter 3. Since protection motivation theory and BP are mainly used to study individual behaviour, and Institutional theory is used to study behaviour at an organizational level, it can be inferred that there is a lack of academic literature on information security at an organization level.

4.4.3 Integration of the Two Theories

Information security compliance requirements are demanded by enforcement authorities such as the customs from market stakeholders of the supply chain, such as customs brokers, traders and freight forwarders (Sarathy, 2006). This is a dyadic relationship between two asymmetrically dependent organizations (Dahl, 1957). The dominant organization, customs, has the power to influence target firms to act as the dominant firm desires. This is what is known as coercive pressure which is one of the main facets of institutional theory (DiMaggio & Powell, 1983) and can be defined as the dominant firm's ability to mediate punishment if a target firm is not cooperative (Ke, et al., 2009). Further, in this type of relation the dominant organization has the "reward power" to reciprocate through rewards for the cooperation of the target firm (Ireland & Webb, 2007; Ke, et al., 2009). The dominant organization also has the power to enforce regulations in a manner that could be perceived as fair or unfair by the target organizations. In terms of getting cooperation through reward and fair justice, both are explained by SET (Blau, 1968). Therefore, in the given relation between the customs and the market stakeholders in the context of SCS, there is a concurrent play of institutional forces within the framework of social exchange. Hence, the aggregation of these two theories has the potential to provide a convincing explanation of the balance between coercive pressures through regulatory demands and the compliance behaviour portrayed by the target organizations within the norms of reward power and fairness (Ireland & Webb, 2007).

Similar aggregation of these two theories can be found in the literature in various contexts. The study of electronic supply chain management system adoption by Ke et al. (2009) is one such example, and the study of trust and power in strategic supply chains by (Ireland & Webb, 2007) discusses extensively the combined effects of institutional theory and SET.

4.5 The Conceptual Model

The conceptual model developed to explain ISCB in the context of this research is presented in Figure 15 below.

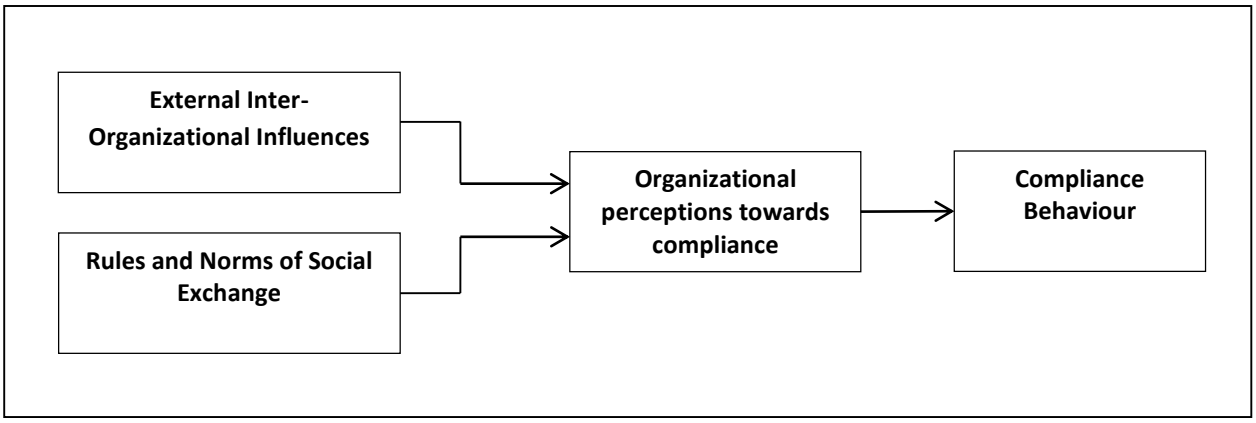

Figure 15: The conceptual model

The argument behind the model is that the compliance behaviour practised by the organizations in the selected supply chain context is influenced by the organizational perceptions towards compliance. Organizational perceptions towards compliance are in turn influenced by external inter-organizational influences as well as by the rules and norms of social exchange between the organizations.

The findings presented in Table 2 provide evidence from the literature that stakeholders of the supply chain are susceptible to regulatory requirements, market influence, and peer pressure, the three facets of institutional pressure (DiMaggio & Powell, 1983). For the purposes of explaining the conceptual model, these three facets are categorized as external inter-organizational influences, which can emanate from two main categories of organizations in the external environment of the selected context for this research. The first category includes organizations in the market environment such as traders, logistic operators and customs brokers. The second category consists of organizations from the authoritative or enforcement environment, including customs, port authorities and other enforcement agencies which operate across supply chains. The literature suggests that when organizations are under institutional pressure to comply with external requirements, most organizations comply only symbolically (Edelman, 1992) as behavioural changes due to institutional pressure in organizations are driven less by desire for efficiency than the need for legitimacy (Liang, et al., 2007).

Organizational perceptions towards compliance are analysed in this research by utilizing the themes derived from the literature on why organizations comply with information security requirements, as well as the concepts from institutional theory and SET. In the literature these aspects are explored solely from intra-organizational and individual behaviour perspectives. While these aspects will still influence compliance behaviour at the organizational level, this research proposes that when subjected to the institutional pressures, the perception of these aspects are likely to be affected and thus impact on compliance behaviour.

The rules and norms of social exchange, derived from SET, are proposed as an element which can also influence organizational perceptions towards compliance. The argument is that the rules and norms of the exchange relationship between the target organization, which has to comply with external requirements, and the authoritative organization exerting institutional pressure for compliance, could change the perceptions of the target organization, leading to more substantive compliance behaviour as opposed to the symbolic compliance suggested in the institutional theory literature.

Hence, the aspects leading to compliance behaviour as identified from the literature and used to formulate the conceptual model are (a) organizational perceptions towards compliance, (b) external inter-organizational influences, and (c) rules and norms of social exchange. The following subsections discuss these aspects in turn.

4.5.1 Compliance Behaviour

A major threat to information security relates to compliance behaviour (Boss, et al., 2009; Siponen & Vance, 2010). For instance, not abiding by information security policies or guidelines set out to maintain integrity, availability and confidentiality is negative compliance behaviour (Herath & Rao, 2009b). Vice versa, when people carefully follow guidelines with the intention of sustaining information security, they are showing positive compliance behaviour.

There are two aspects of compliance behaviour reported in literature: substantive compliance and symbolic compliance. Substantive compliance refers to material changes to maintain acceptability and symbolic compliance behaviour is the performing of activities in a superfluous manner to gain approval (Christmann & Taylor, 2006; Levina & Vaast, 2005). Substantive assurance is needed to ensure effective security, while symbolic assurance is needed to gain the trust and acceptance of the stakeholders (Christmann & Taylor, 2006;

Spears, Barki, & Barton, 2013). Hence, for the purposes of this research ISCB is classified as either substantive or symbolic.

4.5.2 Organizational Perceptions of Compliance

The conceptual model shown in Figure 15 identifies organization perceptions towards compliance as a driver of ISCB in the given context. As presented in Table 2, organizational perceptions towards compliance include perception of threats, perception of benefits, and perception of norms.

4.5.2.1 Perception of Threats

In the literature on managerial decision making, a threat implies a negative situation in which loss is likely and which one has relatively little control over. Therefore, the best course of action is a strategic response – adaptation. Senior management need to change the internal organizational processes in order to adapt as internal activities are easier to access and manipulate (Fornell & Bookstein, 1982). Perception of threats is increased when an organization's actions are guided through coercion or threat of legal sanctions (Hoffman, 1999) by the exertion of power by the state to gain compliance (DiMaggio & Powell, 1983; Lawrence, et al., 2001; Liang, et al., 2007). Moreover, when the perceived threat is severe or imminent, people's compliance towards security polices and guidelines is suggested to be higher (Carlsmith, et al., 2002). Hence, it can be inferred that perception of threats plays a key role in compliance behaviour.

4.5.2.2 Perception of Benefits

If employees, such as boundary-spanning personnel, perceive that being compliant benefits the organization, they are more likely to have a more positive attitude towards security policies (Bulgurcu, et al., 2010; Herath & Rao, 2009b). Further, the benefit that one party obtains from cooperation should have an obvious positive effect on the exchange partner (Rodríguez & Wilson, 2002). One of the factors that shape the benefits of compliance is rewards (Bulgurcu, et al., 2010). This is in line with the discussion on rewarding compliance, as encouragement towards desirable behaviours (Boss & Kirsch, 2007; Pahnila, Siponen, & Mahmood, 2007). Furthermore, according to institutional theory, an organization changes its behaviour not necessarily to gain efficiency but in the face of competition (DiMaggio & Powell, 1983), and the need to legitimize its existence in its business environment (Zhu & Sarkis, 2007). This can be seen as benefit-seeking behaviour. Therefore, if organizations perceive benefits from

compliance, they will be more positive towards complying with the requirements posed by the non-market stakeholders.

4.5.2.3 Perception of Norms

Perception of norms arises from standard behaviour being practised and those who follow these norms perceive that they have an obligation to behave reciprocally (Fan, et al., 2014). This can be identified as normative influence, where people or a group of people conform so that they fit in, obtain approval for others, or avoid punishment and social isolation (Hair, 2010). This conformity to norms signifies inclusion in the group, which makes members feel good about their group membership and is a way to express their loyalty and commitment (Bagozzi, 1981; Bagozzi & Yi, 1988). This normative behaviour towards conformity is so strong in motivation that once identified within a group, their conformity would not be deterred even when such conformity clashes with their own interests (Fehr & Gächter, 2000). Hence, if compliance is perceived as the norm of the market stakeholders this would positively impact on the compliance behaviour exhibited.

4.5.3 External Inter-organizational Influences

Inter-organizational groups fall into many categories, one of which includes those restricted by external influences in performing their task structures (Schopler, 1987). Schopler (1987) showed that with these external influences, the costs and benefits of compliance are specified. This is what is observed in Table 2 – the market stakeholders of the supply chain environment must be restricted by external compliance requirements if they are to operate as inter-organizational entities within the environment.

Implementation requirements of information security are politically motivated and governed by perverse incentives from regulators and foreign governments (Anderson, 2001). As a result, regulatory requirements have become the number one reason for information security investments (Johnson, 2009). They have gradually shifted from a mere cost of doing business to a highly integrated mandatory activity necessitated to enhance regulatory compliance (Khansa & Liginlal, 2012). Ashenden and Sasse (2013) showed that senior managers' drive to align security compliance with their business strategies is due to legal and regulatory requirements.

Regulatory requirements are written broadly to govern industry-wide business practices and are mostly non-functional as more emphasis is given to actions of stakeholders rather than

describing the structure in support of these actions (Breaux & Antón, 2008). This creates many problems such as keeping up with the ever-growing regulatory demands and translating these demands into IT actions (Pinder, 2006). These mandatory information security requirements have arisen because of the ease of access to information (Posthumus & Von Solms, 2004), as easy access leads to carelessness with information. Failure to take available precautions contributes to significant civil losses and even to crimes (Workman, et al., 2008). Modern technology provides means for users to easily access sensitive information in public settings, thereby creating situations where such information can be seen and captured by others (Tarasewich, Gong, & Conlan, 2006).

Regulatory forces are powerful drivers for change but other institutional influences play a significant role in organizational change for improving information security (Hu, et al., 2007). According to Bjork (2004), these external influences lead to differing behaviours between formal security structures and actual security behaviour can be studied using institutional theory (DiMaggio & Powell, 1983). Furthermore, Bjork (2004) claims that institutional theory can help explain why organizations often create and maintain formal organizational security structures and policies without actually implementing them. Backhouse (2006) strengthened this claim by stating that the institutional forces of different interests and objectives influence the creation of information security management standards.

Normative pressure is defined as the collective struggle of the actors of an environment in achieving legitimacy (DiMaggio & Powell, 1983). Typically, normative pressure is exerted by external stakeholders with a vested interest in the organization (Zhu & Sarkis, 2007). In the given context this normative pressure maybe defined as the market influence emanating from the market stakeholders of the supply chain on the prevailing information security compliance practices. This market influence motivates organizations to incorporate the features relevant to these concerns and respond with in-kind performance improvements (Kagan, Gunningham, & Thornton, 2003). In the absence of the market influence, there might be reluctance in implementing innovate practices which might bring economic benefits (Zhu & Sarkis, 2007).

The same institutional environment is responsible for influencing mimetic behaviour which DiMaggio and Powell (1983) define as an organization's response due to uncertainty. Several studies refer to peer pressure as competitive pressure and report that it is more strongly influential than any other institutional force (Carter & Carter, 1998; Hui, Li, & Lau, 2003). In the given context, peer pressure maybe the mimetic pressure arising from the competitors of

the market stakeholders that compel them to comply with the information security requirements of the authoritative organizations.

Hence, there is sufficient evidence supporting the importance of the role of external inter-organizational influences in information security compliance. As shown in the conceptual model in Figure 15, these external influences modify the organizational perceptions which finally drive the ISCB. However, the literature on external influences in an inter-organizational context lacks empirical evidence and is mostly anecdotal or limited to professional opinions.

4.5.4 Rules and Norms of Social Exchange

The interactions within social exchange are usually interdependent (Blau, 1964) and SET gives importance to the potential of these interdependent interactions to provide high quality relationships (Cropanzano & Mitchell, 2005). Cropanzano and Mitchell (2005) further argue that reciprocity is the best known exchange rule. According to the formal theory of reciprocity proposed by Falk and Fischbacher (2006), people reward kind actions and punish unkind actions. In the case of the given context of SCS, actions considered good, such as complying with the information security compliance requirements, are rewarded with expedited clearance procedures (Banomyong, 2005; Sarathy, 2006; Sheu, et al., 2006). Therefore, in the given context, reciprocity could be identified as the reward mechanism infused into the GSCS initiatives as incentives.

Procedural fairness in social exchange leads to a considerable level of certainty which brings about a variety of positive outcomes for an organization and its enhancement (Lind & Van den Bos, 2002). The lack of procedural fairness may result in arousal of negative emotions towards security compliance (Bulgurcu, et al., 2010). In addition, how organizational justice is perceived (in terms of fairness) can assist to set high moral and ethical standards (Komodromos, 2014). In their discussion on the motives of disgruntlement due to injustice which lead to abusive information security behaviour, Willison and Warkentin (2013) point to reward and fairness as possible causes of this abusive behaviour which need to be investigated. Reward (expectations of future returns) and fairness are crucial to social exchange relationships (Higgs & Titchen, 1995), and Cropanzano and Mitchell (2005) argue that fairness and reciprocity through reward are basic tenets of social exchange theory. Fairness and reward are both expected to lead to the perception of benefits.

4.6 Summary

In addition to revealing the research gap, conducting a literature review also helped to identify the implications of SCS under the backdrop of the GSCS initiatives. These implications were then classified as aspects that may influence the compliance behaviour in the given context. This led to the formulation of two research questions that will assist in addressing the identified research gap. Relevant theoretical frameworks were identified and a conceptual model developed. The next chapter describes the research paradigm and methodology in order to best answer the research questions.

CHAPTER 5: METHODOLOGY

5.1 Chapter Overview

The previous chapter presented the theoretical framework and conceptual model applied in this research. This chapter describes the research methodology, its purpose, and how the study was designed and implemented. Figure 16 below outlines the stages that were followed in adopting the most suitable research methodology.

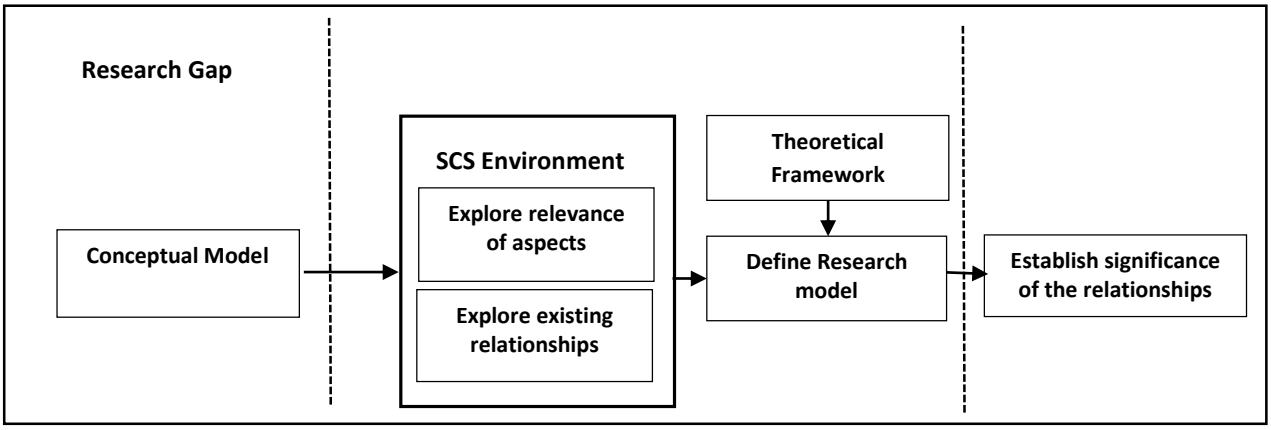

Figure 16: The stages followed in choosing a suitable methodology

Figure 17 outlines the steps that were followed to achieve the goals of the chosen methodology.

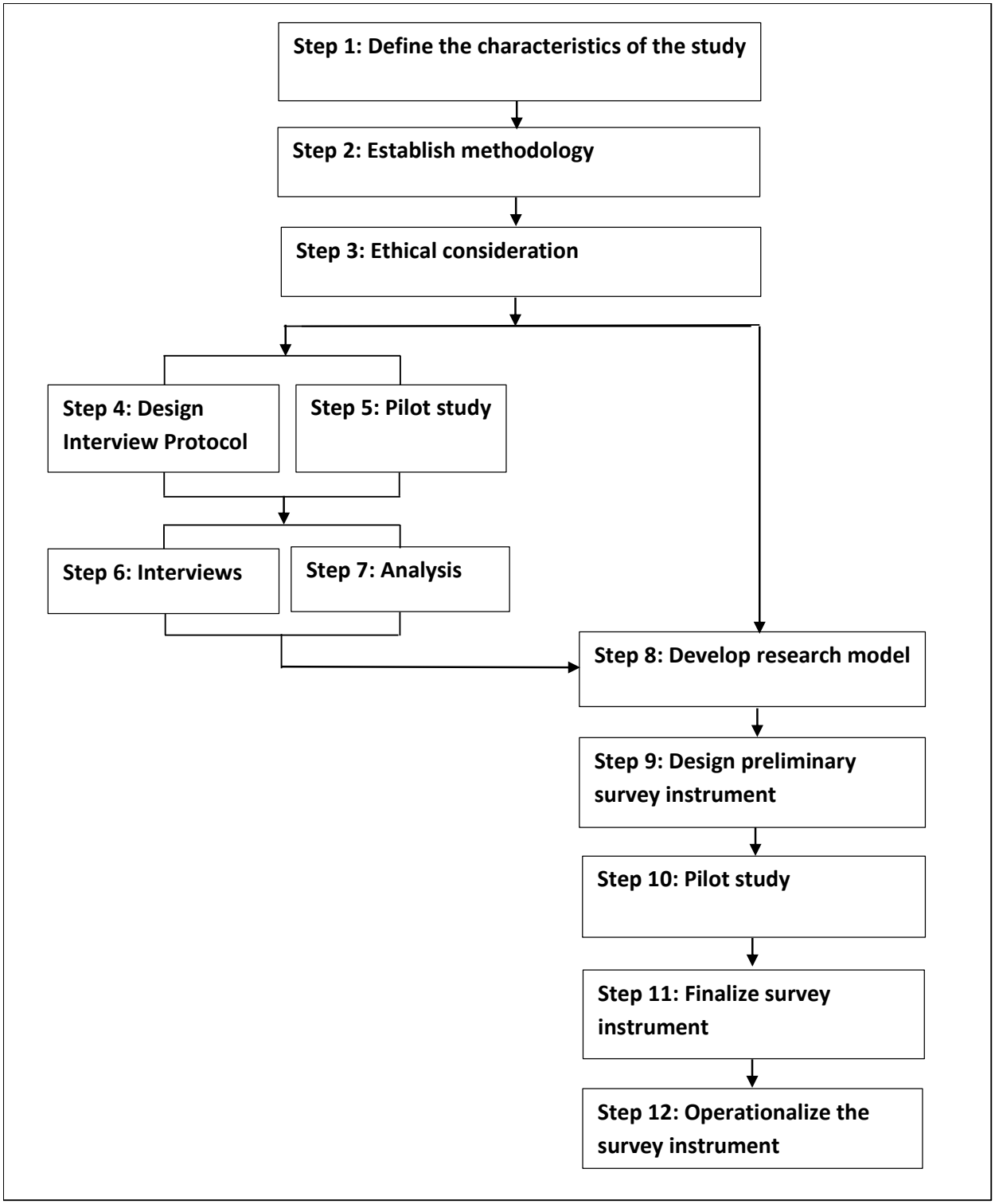

Figure 17: The steps in the execution of the chosen methodology (adapted from Gable, 1994).

5.2 Research Objectives

The aim of this research is to study information security compliance behaviour (ISCB) within a supply chain environment in relation to security of the supply chain. As an area of research, information security is a prominent field of study with extensive academic literature. The security aspect of supply chain, referred to as SCS, is still an emerging area of study with limited academic literature. The literature review conducted in Chapter 3 led to the identification of the understanding of ISCB in the context of SCS as a research gap, one which this study is designed to address.

As discussed in Chapter 3, studies linking information security and SCS are almost non-existent. From this limited literature, aspects that influence compliance behaviour have been established. However, an exploration of the research context is needed to verify the relevance of the identified aspects and to identify any new emerging themes from the research context. This would help in the identification of the constructs and the development of the survey instrument.

5.2.1 Characteristics of the Study

Table 4 presents the characteristics of the study relevant to the research questions and research context. The purpose of this table is to highlight the hurdles and restrictions that were anticipated in conducting this research.

Table 4: Characteristics of the study

Scenario	Inferred from	Leading to	What the literature suggests
Literature is suggestive of the intrusive nature of studies on information security	(Kotulic & Clark, 2004; Smith, et al., 2010)	Less participation resulting in poor sampling number The participating members maybe uncomfortable or unwilling to answer	Snowballing through interviews (Atkinson & Flint, 2001)
SCS is an emerging area of study	(Marucheck, et al., 2011)	Insufficient data	Need exploration (Bjorck, 2004; Johnson & Onwuegbuzie, 2004)
The supply chain is a complex socio-technical system	(Nissen, 2001; Wu, 2001)	Managerial and organization aspects are often entangled	Need multiple methods of inquiry (Dumas, Recker, & Weske, 2012)

Scenario	Inferred from	Leading to	What the literature suggests
Researcher is not familiar with the supply chain environment of New Zealand		Recruiting participants	Snowballing through interviews (Atkinson & Flint, 2001)
Lack of literature on SCS in the New Zealand context		Relevance of the aspects reported in the literature to New Zealand context	Need exploration through interviews (Bjorck, 2004; Johnson & Onwuegbuzie, 2004)
Research model based on theories that need empirical verification		Statistical Analysis	Quantitative survey

5.3 Research Paradigm

Research paradigm refers to a system of ideas, or world view, used by the research community to generate knowledge (Fossey, Harvey, McDermott, & Davidson, 2002). There are three principle research paradigms and they are empirico-analytical, interpretive and critical research paradigms (Higgs & Titchen, 1995). Empirico-analytical paradigm is referred to as positivism which is logical deduction, while interpretive refers to study of the meaning of human experiences and finally critical research is the advocacy where we become aware of how thinking is socially and historically constructed and how this limits our actions (Fossey, et al., 2002).

It may be assumed with reasonable confidence that the reality of the phenomenon under question exists within the chosen context. This would be the ontological perspective of the line of inquiry, which could be argued as the assumption of the existence of the reality, which is driven by immutable natural laws and mechanisms (Guba & Lincoln, 1994, p. 109). The challenge in seeking out the said reality would be to ensure that the researcher and the phenomenon under investigation be kept independent. This would be the epistemological perspective where the researcher be capable of studying the object without influencing it or being influenced by it (Guba & Lincoln, 1994, p. 110). This epistemology would be true from the viewpoint of positivist paradigm. However, this research was conducted under the post-positivist paradigm.

Post-positivism from an ontological perspective, relates to the nature of study being as close to the reality as possible, through widest possible criticism, which exists only among flawed human intellectual mechanism and fundamentally intractable nature of phenomenon (Guba &

Lincoln, 1994, p. 110). In this post-positivist paradigm, the epistemology that defines the dualist and objectivist nature is modified by abandoning the dualist nature as not possible to maintain (Guba & Lincoln, 1994, p. 111). Special emphasis is placed on objectivity such as ascertaining whether the findings fit the pre-existing knowledge , (Guba & Lincoln, 1994, p. 111) in this case the existing knowledge is embedded in the conceptual model formulated from the literature. The choice of this paradigm is further justified by the alignment of the philosophical elements of post-positivism as defined by Creswell and Clark (2007, p. 22) with the characteristics of this study. These elements include determination (cause and effect through forming theories), reductionism (narrowing and focusing on selected variables gathered from the literature), empirical measurement (statistical analysis), and theory verification (through hypotheses).

Some researchers have argued that a post-positive philosophical paradigm should be combined only with quantitative methods (Creswell & Miller, 2000). In this case, the question arises whether two worldviews or paradigms can coexist in a single study. According to Creswell and Clark (2007, p. 22), multiple paradigms can exist in a single study as long as each of the paradigms is honoured. Other features of this study can be related to other philosophical elements defined by Creswell and Clark (2007, p. 22), which include consequences of actions (actions leading to either substantive or symbolic compliance behaviour), problem-centred (disruption of supply chain), pluralistic (multiple data through systematic inquiry), and practical oriented (supply chain operations). The characteristics of this study were presented in Table 4 and very closely reflect the arguments made above. Guba and Lincoln (1994) suggest that the methodology for a post-positivist paradigm include falsification of hypotheses and may include qualitative methods. Hence this study adapts a mixed method.

SCS is an emerging field (Marucheck, et al., 2011) and lacks empirical studies (Concha, 2014). As noted above, Chapter 3 identified ISCB in the SCS context as a research gap. A conceptual model was formulated in Chapter 4 using the limited literature on SCS and information security in the SCS context. This model will be used to conceptualize the aspects that influence ISCB in SCS as a consequence of the GSCS initiatives. A qualitative method helps in the exploration to identify the relationships and their respective variables/constructs that may be measured subsequently through the use of existing instruments or the development of new ones (Hanson, Creswell, Clark, Petska, & Creswell, 2005). Therefore, a qualitative method would be a good choice to verify the relevance of the identified influence in the given context. The nature of

verification using a qualitative study is the process of checking, confirming, making sure and being certain (Morse, Barrett, Mayan, Olson, & Spiers, 2008). The research questions call for the identification of the drivers of compliance behaviour and other factors that influence these drivers. Hypotheses concerning the relationships between the drivers and influencing factors will be developed from the research questions and tested as to their significance. The suitability of a quantitative survey as a method to empirically test the significance of hypotheses has been widely established, and therefore a quantitative survey was chosen to test this study's hypotheses. This approach, where a qualitative method is followed by a quantitative method, is called sequential mixed methods research in which the researcher seeks to elaborate on or expand the findings of one method with another method (Johnson & Onwuegbuzie, 2004)

The supply chain is considered a complex socio-technical system which integrates technology, people and organizations (Nissen, 2001; Wu, 2001). As indicated in the objectives of this research, this study aims to investigate the behaviour of such complex socio-technical integration among IT and organizations. When studying such a complex socio-technical system in which managerial and organization aspects are often entangled, a multi-method approach is more appropriate (Dumas, et al., 2012). A multi-method approach, also referred to as a mixed methods design (Wetzels, Odekerken-Schroder, & Van Oppen, 2009), consists of both qualitative and quantitative methods. Venkatesh, Speier, and Morris (2009) argue that although these two terms are used interchangeably, they have significant differences and the correct term should be mixed methods when qualitative and quantitative methods are used in combination. A mixed methods design can be defined as a research design (or methodology) in which the researcher collects, analyses and mixes (integrates or connects) both quantitative and qualitative data in a single study or multiphase program of inquiry (Johanson & Mattsson, 1987). Given the strengths and weaknesses of the mixed methods design , using mixed methods is important in examining the design of SCS research because it is an emerging area of study (Wu, et al., 2014). In this respect, multiple perspectives and a complete understanding of the problem can only be achieved by following up a qualitative study with a quantitative study on the identified constructs and relationships (Clark, 2010). This is in addition to providing further insights to refine the hypotheses and instrument development (Morris & Venkatesh, 2000). Such a combination of methods to answer a research question is called a sequential mixed methods design (Narasimhan, Nair, Griffith, Arlbjørn, & Bendoly, 2009).

The use of a qualitative approach to verify or identify variables/constructs of the research model ensures instrument fidelity and is one of the rationales for conducting mixed methods research (Collins, Onwuegbuzie, & Sutton, 2006). Further when the context of the research is significantly different it is a good enough reason to use mixed method (Venkatesh, Brown, & Bala, 2013). For instance, the study of information security compliance behaviour in the supply chain security context is significantly different to the context of similar studies reported in literature. The strengths of a mixed methods design are that it can lead to increased generalizability of the results and both methods (qualitative and quantitative) used together produce more complete knowledge necessary to inform theory and practice (Johnson & Onwuegbuzie, 2004). Information security studies are considered intrusive in nature (Smith, et al., 2010) and can lead to over cautionary behaviour by the participants due to mistrust of outsiders to the organization (Kotulic & Clark, 2004). Given this nature of the study, an added concern is the unfamiliarity of the researcher with New Zealand's supply chain environment. Hence, establishing contacts to participate in the research was a substantive concern. Fortunately, the qualitative approach can involve the technique of snowballing (Atkinson & Flint, 2001). The snowballing or chain referral sampling method yields a study sample through referrals made among people who share characteristics that are of interest to the research (Biernacki & Waldorf, 1981). Snowballing is relevant especially when the issue under investigation is sensitive and requires insiders to locate people for study (Biernacki & Waldorf, 1981). These factors also support the inclusion of a qualitative component through a mixed methods design.

This study uses a sequential mixed methods design with a qualitative method to explore the constructs of the conceptual model before the dominant quantitative study. This method has been successfully applied in information system studies. The reader is referred to Zakaria and Janom (2011), who use a prior qualitative enquiry to establish the content validity, accuracy and clearing the uncertainty of each construct of their conceptual model formulated from the findings of literature, and to a study on information security risk management by Spears and Barki (2010). The literature on SCS and information security reveals considerable debate about research paradigms and the possible biases of positivism and anti-positivism. Hence choosing a method that is acceptable to these two varying audiences becomes important in order to increase the validity of the study. Creswell and Clark (2007) state that it is vital to apply the most suitable methodology to ensure acceptability among the audience when there are possible biases towards positivism and anti-positivism.

Since this research uses a mixed methods design, it consists of two phases of data collection and analysis. Phase 1 is a qualitative study conducted to identify a conceptual model formulated from the findings of the literature review and relevant existing theories. The objective of such an exploration was to establish the relationships and conceptualize hypotheses, and to ensure a foundational understanding of the area under investigation in relevance to the theoretical aspects informed by the literature and past experience (Creswell & Clark, 2007). The outcome of this first phase will be the transformation of the conceptual model into a research model, the formulation of hypotheses, and the development of the quantitative survey instrument used in Phase 2. Greene, Caracelli, and Graham (1989), after much examination of mixed methods research publications, called this stage of the mixed methods design "development", while Collins et al. (2006) call it instrument fidelity; that is, assessing the appropriateness and/or utility of the chosen instrument.

Phase 2 is the quantitative survey and the objective of this phase was to assess the significance of the relationships in the research model and validate it. Hence, this is a quantitative dominant mixed methods study, which according to Johnson, Onwuegbuzie and Turner is where one relies on a quantitative post-positivist view of the research process while concurrently adding qualitative data.

5.3.1 Mixed Methods Research in Supply Chain Studies

While discussing the findings from an extensive literature review on supply chain research, Burgess et al. (2006) expressed the concern on the relative lack of mixed methods research. To substantiate this concern, a survey was conducted of the articles published in one of the A grade listed journals, the Supply Chain Management: An *International Journal* from 2006 to the time of writing. This resulted in the identification of not a single study that specifically claimed to be using the mixed methods design. However, a wider journal search did return studies by Voss et al. (2012), Whipple et al. (1997) and Speier et al. (2014). This is by no means an exhaustive list, more an indication that the mixed methods design has been successfully applied in supply chain studies and interestingly all of these studies are in the context of SCS. Voss et al. (2012) do not provide either an explanation or a justification for the application of the sequential mixed methods design with a dominating quantitative survey. However, similar to the methodology applied in this study, Voss et al. applied a qualitative method at the beginning to assess respondents' perception of firms' security initiatives and resulting performance, which led to

survey development and administration. These studies from the literature were therefore used as a guide in applying the chosen methodology.

5.3.2 Mixed Methods Approach in Information Security Research and Information Security in the Context of the Supply Chain

The mixed methods approach has been applied in various information security studies. Spears and Barki (2010) applied this approach in a study on user participation in information security risk management and Hsu, Lee and Straub (2012) used it in a study on institutional influences on information security innovations. To ascertain this approach's validity in the chosen context of the supply chain, a literature survey was performed on two prestigious information security journals. This resulted in the identification of studies by Trkman et al, (2010) and Lavastre, Gunasekaran and Spalanzani (2012), both of which used a literature review to develop a conceptual model and semi-structured and open-ended interviews. The results of the interviews were then used to formulate the quantitative survey instrument. Following the approach of these studies, a preliminary survey instrument for the quantitative survey (Phase 2) was developed from the findings of the qualitative survey in this research. The data collected from the interviews were analysed to operationalize key constructs and ground the findings of this study.

5.4 Operationalizing the Research

In this study the inter-organizational context proposed is SCM. However, the organizations selected were not all from the same supply chain. They were organizations of any given supply chain which are mandated to comply with a set of requirements from a focal enforcement organization such as customs or port authorities. Organizations were selected by approaching the Customs Brokers and Freight Forwarders Federation (CBAFF) of New Zealand, a trade association. In all organizations, boundary-spanning personnel performed a liaison function with other organizations (Chen, Lin, & Yen, 2014). In the context of SCM, this would be frontline managers or executives who frequently confer with officials of the focal organization. It was hypothesized that systematic inquiry into the role-sets of these boundary-spanning personnel would shed light on inter-organizational relations (Chen, et al., 2014). This form of selective sampling is important to meet the aims of the study (Schatzman & Strauss, 1973).

5.5 Ethical Considerations

Prior to conducting the study, as per the requirements of the Auckland University of Technology (AUT), an ethics application was submitted to the AUT Ethics Committee. The ethics application (13/144) was approved on September 17, 2013.

The Ethics Committee required the researcher to send an invitation letter to each interview participant outlining the following:

1. purpose of the research
2. how the participant was identified and why the participant was being invited
3. what will happen during research
4. what are the discomforts and risks
5. how these discomforts and risks will be alleviated
6. the benefits
7. how will the participants privacy will be protected
8. the costs of participating in the research
9. how the feedback will be received
10. how to react to any concerns regarding the participation
11. contact details if further information is required

The approval letter is included in Appendix A.

5.6 Phase 1: Qualitative Study

As discussed, the conceptual model was formulated from the themes arising from the literature review and the identification of relevant theories. Qualitative methods, which involve interviewing, provide a rich understanding of participants' activities, behaviours, and assignments (Spears & Barki, 2010), thereby helping to supplement the findings from the literature, explore the research model, and aid the development of the quantitative instrument (Amaratunga, Baldry, Sarshar, & Newton, 2002). In addition, qualitative methods allow the researcher to avoid prior commitments to theoretical constructs and the formulation of hypotheses before gathering data (Yin, 2012).

5.6.1 Interview Protocol Design

Open-ended interviews are the most popular form of interviewing technique as they allow the participants to fully engage in expressing their perceptions and experiences (Rimal & Real,

2003). In order to get open-ended responses, the questions have to be worded as such (Bendor & Swistak, 2001). However, the questions also need to be semi-structured so as to give the interviewee some general insight into what is being sought. This involves the combination of topic initiating questions and follow-up questions (Rapley, 2001) In this study, the semi-structured questions formulated using themes from the literature were evaluated by the researcher's two supervisors and a qualitative research expert from a different faculty of AUT. The supervisors evaluated the relevance of the questions to the objective of the study and also their relevance to the literature surveyed for this study. The questions were again vetted by a linguistic expert from Massey University to ensure that the questions were asked in clear and natural English. The questions were further tested with two PhD candidates to ensure that there were no expressions or hints of the actual relationships under investigation. The interview protocol is shown in Table 5.

Table 5: Interview questionnaire

	Subject	**Question**
1	Regulatory demands	What is your perception on the local regulatory authority's demands in relation to information security in the exchange of information between the supply chain stakeholders and the authorities?
2	Market influence	What is your perception on the authority's promotion of information security in the information exchange standards and the adoption of these standards by other stakeholders within the supply chain?
3	Peer pressure	What is your perception of your competitor's behaviour towards the information exchange requirements within the supply chain?
4	Perceived norm	What is your belief on the expectation of people who influence you and who are important to you think how you should behave towards the information exchange requirements?
5	Perceived threat	What is your perception of the negative outcomes if you do not follow the authority's requirements?
6	Perceived benefits	What is your perception of the benefits to you and to your peers, if you follow the authority's requirements?
7	Fairness	What is your perception on impartiality, refutability, explanation, familiarity and courtesy towards you from the authority?
8	Reciprocity (Reward)	What is your perception on the reciprocity (incentives and rewards) when you comply?
9	Symbolic and substantive compliance	How does your organization conduct itself in fulfilling the information security compliance requirements?

5.6.2 Sample Selection

The participants selected for interviews are boundary personnel of target organizations such as shipping companies, freight forwarders and customs brokers. It can be inferred from Yang (2011) that professionals from these areas provides significant participation in SCS. The list of the target organizations were obtained from the website of the CBAFF. Verbal consent was sought from the federation before the members were contacted over the phone and email. Table 6 shows the types of organizations chosen and their business descriptions. The boundary personnel were identified by communicating the intent to the head or senior management of the selected organization. One participant from each of the 35 target organizations was selected for the interview, so as to get as many different perspectives as possible. A number not more than 25 is sufficient for a phenomenological study Creswell (2012), however 35 was selected in case any of the respondents changed their mind and declined to give an interview.

Table 6: Participating organizations and their businesses

Participant area	Description	Number of participants
Brokers and Freight Forwarders	In addition to dealing with the authorities with the export or import documents on behalf of their customers, they also provide freight forwarding services.	12
Customs Brokers	Prepares documents for import and export and deals with the authorities on the customer's behalf	15
Shippers	Consolidates cargoes and ships across to international destinations.	3
Major Exporter	An exporter who has in house customs brokers and freight forwarding arm. (a member of the NZ Customs Secure Export program)	5

5.6.3 Pilot Study

A pilot study is the trying out or pre-testing of a research instrument (interview schedule) to check the wording, the order of the questions, and also get an advance warning of where the research protocol may fail (Blau, 1964). A pilot study was therefore conducted to test the semi-structured questions formulated from the findings of the literature. The pilot study provides the researcher with a clear definition of the focus of the study (Christensen, Rothgerber, Wood, & Matz, 2004). The main purpose of a pilot study is generally to refine data collection rather than to formulate an analytic scheme or develop theory (Bandura, 1986). In other words, it is a preliminary test of the instrument to implore comments and suggestions about the instrument

from the respondents (Arvey & Ivancevich, 1980). In this respect, the objective of the pilot study was to:

1. Ensure that the semi-structured questions uses the industry accepted terms, thereby ensuring that the participants are aware what is being asked and how it fits into their daily operations.
2. Ensure that the questions are broad enough to the extent that the respondents can give a lengthy account of their experience and its relevance to the research context.
3. Finally, test the researcher's ability to carry out interviews by engaging a senior and experienced professional to carry forward a meaningful discussion on the research questions, before embarking on the actual interviews for the study.

Four participants were selected from the CBAFF list for the pilot study interviews.

5.6.4 Data Analysis Methods

The strategy applied to analyse the interviews was that outlined by Saba and Shearer (1994), where the transcribed text is read to identify surface-level details and reveal themes and defining categories from the data as a whole which indicate relationships and generalizations. In this study however, the categories were defined beforehand, and instead of redefining the categories, the pre-existing categories were matched with the findings from the data. The main aim of this analysis was to "put on trial" within a real empirical context for contextual re-specification, refinement or elimination (Onwuegbuzie & Collins, 2007) the dimensions or themes of the proposed model. This form of qualitative data analysis that sets out to test whether data are consistent with prior assumptions or with theories identified or constructed by an investigator is called deductive analysis (Thomas, 2006). As discussed earlier, the whole purpose of the qualitative phase was to supplement the findings from the literature, verify the conceptual model, and aid the development of the research model and instrumentation for the quantitative study.

5.6.5 Validity and Reliability

It was necessary to ensure that the qualitative analysis had enough rigour to ensure that the outcome of the process was valid and reliable. The literature on validity and reliability of qualitative studies is not clear on what verification aspects constitute validity and what aspects constitute reliability. However, according to Morse et al. (2002) verification strategies that ensure both reliability and validity of data are activities such as ensuring methodological

coherence, sampling sufficiency, developing a dynamic relationship between sampling, data collection and analysis, and thinking theoretically. The application of these activities in this research is described in the Table 7.

Table 7: Validity and reliability measures for the qualitative study

Strategy	**Explanation by Morse et al. (2002)**	**How it was achieved**
Methodological coherence	The interdependence of qualitative research which demands that the question match the method, which matches the data and the analytic procedures.	The qualitative method chosen was interviewing and the questions were semi structured to ensure that the respondents had ample opportunity to add information beyond the question. The interview responses were then transcribed in order to identify and group the emerging themes.
Sampling sufficiency	Sufficient data to account for all aspects of the phenomena have been obtained	While the interviews were being conducted, gradually common themes started emerging. By the time 15 participants were interviewed, saturation was reached, meaning no new information were being generated and further interviewing was stopped
Collecting and analysing data concurrently	Mutual interaction between what is known and what one needs to know.	The main surface level themes that emerged from previous interviews were asked with the next participant as a probing question and the difference or commonality in the response was observed.
Thinking theoretically	Ideas emerging from data are reconfirmed in new data; this gives rise to new ideas that, in turn, must be verified in data already collected.	Findings from the literature were grouped in broad based headings. The ideas emerging from each interview were fitted into these groups. By doing this common themes were being grouped as the interviews were being conducted.

5.7 Phase 2: Quantitative Study

Quantitative methods were then employed to validate the theoretical model that had been explored and enhanced by the findings of the qualitative study in Phase 1. A sample set, that excluded respondents of the qualitative interviews, was selected among the boundary-spanning personnel of the target organizations. The purpose for such a selection is to ensure that separate and dissimilar datasets collected on the same phenomenon provide a richer scenario (Babu, Gunasekaran, & Krishna, 2014). Quantitative methods also enable the discovery of relationships that are common across the stakeholders (Gable, 1994) and some of the features inherent to specific organizations within the entities under study.

5.7.1 Preliminary Survey Instrument

The quantitative survey was conducted using a self-administered questionnaire as a survey instrument. The preliminary survey instrument was formulated using pre-existing scales that have been operationalized and peer-reviewed. The items were reworded to fit the research context. Further refinement was done based on the outcome of the qualitative study. The items were measured using a 7-point Likert-type scale (Strongly Agree, Agree somewhat, Undecided, Disagree somewhat, Disagree, Strongly disagree).

5.7.2 Sample Selection

In order to choose a sampling technique, the researcher needs to consider carefully the characteristics of behaviour and social interactions that are relevant to the study population and the research question at hand (Altmann, 1974). The process of sample selection was based on the process followed by Benton and Maloni (2005). In their study a list of buyers was obtained from a major supplier and the buyers were requested to nominate an individual who was at the decision-making level to participate in the survey. These individuals are the boundary-spanning personnel who play a strategic role in the inter-organizational relations among the stakeholders. Benton and Maloni's process (2005) fits the pattern argued by Altman (1974) and is similar to what the current study set out to achieve. The population from which the sample was desired were boundary-spanning individuals from the supply chain environment. Any random person picked from this sample frame is assumed to have sufficient knowledge to inform the research question at hand. This method of selecting random cases from the sampling frame and randomly choosing a desired number of individuals to participate in the study is called random purposeful sampling (Onwuegbuzie & Collins, 2007).

A list of shippers, customs brokers and freight forwarders taken from the CBAFF and other business directories was compiled. Yang (2011) notes that professionals from these areas have significant participation in SCS. The initial list contained 165 companies. These companies were contacted by phone, and the email addresses of the people that could be identified as boundary personnel were sought. This exercise resulted in 320 email addresses of potential participants.

5.7.3 Pilot Study

The process followed by Yang and Wei (2013) to test the viability of the quantitative survey instrument in their study of SCS was utilized to conduct the pilot study for the survey. Ten

supply chain stakeholder companies in Hamilton were chosen for the pilot study and the internet link to a Qualtrics web survey was emailed to them with an explanation of the aim of the pilot test.

5.7.4 Data Analysis

The data collected from the survey was analysed using partial least squares (PLS) regression. PLS is better suited for explaining complex relationships because of its efficiency in avoiding two serious drawbacks: inadmissible solutions (negative variance) and factor indeterminacy (Fornell & Bookstein, 1982). There is a large number of successful applications of PLS regression in information security studies including Bulgurcu, et al., (2010) and Liang et al. (2007), to name a few.

Since information security research is intrusive in nature and requires a lot of trust between the organization and the researcher (Smith, et al., 2010), there was a concern that not enough participants would be recruited to conduct a viable quantitative analysis. It is widely believed that PLS gives more leverage and is more appropriate over statistical estimation methods when the sample size is small (Goodhue, Lewis, & Thompson, 2012). The rule of thumb for an appropriate sample size in PLS is that the sample size should be at least 10 times the number of incoming paths to the construct with the most incoming paths, which is called the "10 times" rule (Hair, Ringle, & Sarstedt, 2011). In the model formulated for this research the most incoming paths for a single construct is four, and if the "10 times" rule is to be followed, a sample size of 40 would suffice. However, there is quite an extensive debate in academia over the insufficiency of this size for correlational analysis. In this sense, it was deemed important to employ statistical reasoning to ensure the correct sample size. As such a statistical power analysis using a software called G*Power was conducted. The details of this analysis are presented in Chapter 8.

PLS analysis to calculate the structural path significance of the outer model and the inner model was done using a software application called SmartPLS. An inbuilt algorithm called Bootstrapping also facilitated this analysis by generating the *t*-statistics to verify the significance of the research hypotheses proposed in this study.

5.7.5 Reliability and Validation

The first reliability test performed was the common method bias (CMB) test. This relates to an error that might arise from data collected through the same questionnaire during the same period having a common rater, a common measurement context, a common item context, or from the characteristics of items themselves (Podsakoff, MacKenzie, Lee, & Podsakoff, 2003). The most widely used test for CMB is Harman's single factor test (Podsakoff, et al., 2003) and this method was used to test for CMB in this study.

The first step in data analysis of the evaluation of theory via structural equation modelling is to determine whether the measures have satisfactory psychometric properties. The properties of interest are reliability (convergent validity), average variance extracted (AVE) and discriminant validity for each unobserved variable (Fornell & Larcker, 1981). Accordingly, the following tests were performed:

a) indicator reliability and internal consistency was tested using Cronbach's alpha method as suggested by Morris and Venkatesh (2010).
b) convergent validity was tested using AVE as suggested by Bagozzi and Yi (1988)
c) discriminant validity was tested using the square root of AVE for each latent variable as suggested by Wong (2013)
d) target endogenous variable variance was tested using the coefficient of determination [R2] for the endogenous latent variables as suggested by Hair et al. (2011)
e) predictive relevance was tested using the Q2 values as suggested by Hair et al. (2011)

5.8 Summary

This chapter provided a detailed explanation of the research design and the methods employed to enable collection and analysis of data. The best-fit research paradigm for this study was identified as post-positivist. A detailed explanation of how the research objective, the research questions, and the research context can be addressed under this paradigm was given. An extensive justification was also provided for the selection of a sequential mixed methods research design. A description of how both the qualitative survey and the quantitative survey were conducted in terms of sample selection, interviews, and quantitative survey and data analysis methods was provided. In addition, the measures taken to ensure the reliability and validity of the methods employed and the maintaining of ethical standards were detailed. The following chapter provides the findings from the qualitative phase of the study.

CHAPTER 6: PHASE 1 – QUALITATIVE ANALYSIS AND RESULTS

6.1 Chapter Overview

Chapter 5 described the research paradigm, the justification of the chosen methodology, and how the methodology is applied for this study. During this discussion, it was specified that the study would follow a sequential mixed methods research design and there would be two phases of data collection and analysis.

This chapter provides the specific details of the qualitative study conducted in Phase 1, which includes the pilot study, selection of research participants, interviews, data analysis, and the findings. The objective of this qualitative survey was to verify the conceptual model and confirm the existence of the identified themes that led to the formulation of the constructs of the conceptual model. Furthermore, this phase was expected to ensure that the foundational understanding informed by the literature is relevant to the research context. One of the strengths of the qualitative research is to illuminate the subjective meaning and context of those being researched (Fossey, et al., 2002). In this sense Creswell (2003) argues that if a concept or phenomenon needs to be understood because little research has been done on it, then qualitative research could help . Further, it can be inferred from Creswell (2003) that qualitative inquiry can help in the identification of the important variables to examine. These claims fit into the characteristics of this study where the literature is scarce and the context is new. Hence, by doing the qualitative inquiry prior to the testing of the model will ascertain the post-positivist ontological paradigm in which this study is positioned philosophically.

To set out an ambitious objective such as exploration for new and emerging themes was considered less likely as the study being intrusive in nature, there was always the fear of the participant's level of response to a face to face interview on information security questions (Myers & Newman, 2007). As such the depth of analysis is considered only to the level of verification and confirmation of the identified themes which represent the conceptual model, so that the testing of the conceptual model could be done using the quantitative survey which is the dominant phase of the chosen mixed method. However, any narratives from the qualitative inquiry that clearly emphasises the significance of a relationship can be used to strengthen the arguments on the relationships tested through the quantitative survey.

Researcher acting as an informed consumer using the literature to conduct an analysis of the concept can be called verification using a scaffold (Morse & Mitcham, 2008). Scaffold is an

education term which refers to learners while they engage in activities that are normally out of reach (Palincsar, 1986). As for some studies, the researcher may have a preliminary model or theory which to base the enquiry on and through these objects an initial list of coding can be generated (Miles & Huberman, 1994), which is in this case are the identified themes. This provides the researcher reasonable confidence about the domain of the concepts such as what is and what is not an example of the concept (Morse & Mitcham, 2008). The verification (validity and reliability) strategy of the qualitative process adapted from Morse et al., (2002) was explained in Table 7 and hence is not repeated in this chapter.

6.2 Pilot Study

6.2.1 Overview and Analysis

A pilot test is the trying out or pre-testing of a research instrument (interview schedule) to check the wording, the order of the questions, and also get an advance warning of where the research protocol may fail (Blau, 1964). Two participants were selected from the CBAFF list for the pilot study interviews. After each interview, a preliminary analysis was conducted to ensure that all the constructs in the model were addressed sufficiently. Any new ideas that emerged were incorporated into the questionnaire and used in the next interview. Sandelowski (2000) notes that constant comparison of the qualitative content can be used to analyse data from the instrument. Once the interviews were completed a final analysis was done to collectively ensure that the questions achieved their targeted purpose and that the inferences from the analysis were acceptably accurate. To ensure accuracy, the participants were met with to discuss the findings. Hence, it was concluded that the interview protocol and the conduct of the interview sessions were acceptable and that it was suitable to proceed with the rest of the interviews. .

6.2.2 Research Method and Process

One organization each from cities Auckland and Hamilton in New Zealand were selected for the pilot study. The two interviews were conducted at the participants' premises during their working hours. The two interviews were recorded and analysed to identify potential problems with the questions. The steps followed for this process were:

1. Each of the organizations selected for study was contacted via phone and a request was made to meet with a senior person liaising with customs and other relevant authorities regarding export of goods across the national borders.

2. Once such a person was identified, the contact details of that person were sought with their consent.
3. The incumbent participant was then contacted directly and explained the reason why he or she was being contacted.
4. Once the incumbent participant agreed to give an interview, further communication was exchanged for a time and day for the interview.
5. The two participants agreed to meet at their work place for the interview.
6. Before the beginning of each interview, each participant was given a copy of the ethical commitments and the details of the supervisor and the contact person from the AUT Ethics Committee.

6.2.3 Participants

The participants were chosen from the list of customs brokers and freight forwarders published on the CBAFF website (www.CBAFF.org.nz) Verbal approval was sought from CBAFF before contacting their members. The interviews lasted 40 minutes each and were recorded with the participants' consent. Table 8 lists the characteristics of the participants.

Table 8: Characteristics of the pilot study participants

Participant	Type	Location	Designation	Duties	Gender	Age	Experience
Company A	International freight forwarder	Hamilton	Senior Manager	Liaise with authorities	M	45	10 years
Company B	Sea food exporter to the United States	Auckland	Business Owner	Liaise with authorities	M	42	8 Years

6.2.4 Data Analysis

The recorded interviews were listened to in the presence of two PhD graduates to ensure that the objectives mentioned in section 6.2.1 were met as per the categories presented in Table 9.

.

Table 9: Observations of the pilot study

No	Category	Observation
1	Terms from the conceptual model: • GSCS initiatives • SCS • Preferential treatment • Security compliance • Peer pressures • Regulatory demands and influences • Market pressure	The two participants showed acceptance and understanding of the terms, without prior definition by the interviewer. Therefore, it was conclusive that the terms were acceptable for the interviews.
2	Did the participants find the questions relevant to the work they do regularly?	Almost all of the questions posed were answered without any hesitation and further qualification, indicating that the questions were relevant to their daily work.
3	Did the participants answer all the questions in length?	The semi-structured and open-ended nature of the questions proved to be effective in encouraging the participants to give a lengthy account of their beliefs and knowledge on the subject of the question.
4	Did the questions lead to other probing questions?	The questions proved to be broad enough to provide opportunities to pose probing questions.
5	Was the researcher able to keep the participant engaged in a meaningful discussion?	The researcher showed confidence and the two interviews led to a relaxed and an informative session. *(To assess the confidence of the interviewer, PhD graduates listened to the recordings)*

6.2.5 Conclusion

The pilot study, in addition to achieving its main objective outlined in section 6.2.1, confirmed the effectiveness of the semi-structured questions. A semi-structured instrument should consist of open-ended questions which have the potential to define and explore the research context while giving ample opportunity for the interviewee to diverge in order to pursue and idea in more detail (Britten, 1995). Hence, there was no significant need to change the content of the questionnaire or the way the interview was conducted before proceeding with the rest of the interviews.

6.3 Interviews

Kotulic and Clark (Kotulic & Clark, 2004) employed the methods listed in Table 10 to increase participation in their information security study and these were used as a guide for this research.

Table 10: Methods used to increase participation

	Methods	Result after applying to the current study
1	Colleague and insider referrals and introductions.	No such privileges exist due to the researcher being a student and new to the environment.
2	Contacting professional organizations that had sponsored supported or published information security surveys.	• Several emails sent and no response. • Left messages, no response.
3	Contacting leading security industry firms.	• Several emails sent and no response. • Left messages, no response
4	Contacting consulting firms with a visible presence in information security	• Several emails sent and no response. • Left messages, no response.
5	Making presentations in security symposiums.	• No such symposiums.
6	Contacting several governmental organizations.	Two relevant government organizations were contacted and there were email communications. The final reply was they could not assist.

Emails were sent to senior managers after getting their contact information from the company websites and calling the respective office. Ten days passed without any response from any of the 35 contacts. Further contacts were made by placing phone calls to these companies to get an appointment with the senior managers. Each appointment was registered with the person answering the public number. There were five inquiries about the purpose of an appointment, which was explained through email once again. Finally, two agreed to an interview; the remaining 33 did not reply. This represented a discouraging 6% response rate.

After discussion with and advice from faculty members, the researcher decided that these two respondents could be a starting point for a snowballing strategy with the aim of producing a pool of possible participants by asking the incumbent interviewee for information on other similar candidates who may have the same knowledge and be willing to participate in the study at hand (Polkinghorne, 2005) .

In total, 10 semi-structured face-to-face interviews were conducted at the participants' respective workplaces. The questions, though semi structured, were presented in an open-ended form as to give the maximum opportunity for participants to express their views. This allowed flexibility regarding the direction of the interviews and provided unrestricted flow of knowledge, lessening the possibility of missing key areas and predefinition of possible answers. Except for one face to face interview, all were conducted at the participant's work desk. This provided a comfortable environment where the participants did not feel restricted or

uncomfortable about sharing information (Rimal & Real, 2003). Each of these interviews lasted 45 minutes to an hour.

During these interviews, some of the interviewees shared their internal documents such as email communications between their customers across the borders. Some of the participants shared their work terminals and demonstrated how they used their document-processing applications. In addition, some of the participants discussed with their colleagues over the intercom or invited them to their desk before responding to some questions. It is worth mentioning that all of the participants performed very professionally and participated with great enthusiasm. Seven participants agreed to their interview being recorded.

Five further interviews were conducted over the phone. The phone interview participants did not agree to their interview being recorded, however each of the participants spent close to 30 minutes on the phone. Three of them sent extra information by email. Similar to the pilot study, after each interview a preliminary analysis was conducted by reading the transcribed notes from the interview and tabulating the arguments according to the constructs.

The participants were senior managers responsible for the communications between the customs regarding the transport of cargo across the borders. During the interviews, the participants were requested to assist in recruiting their colleagues or peers for the study. At the end of each interview, the participants provided a list of their colleagues from different companies performing the same functions as them and drafted an introductory email requesting them to participate in the study. The email was copied to the researcher, the content of which advocated their participation on the grounds of corporate responsibility and to contribute to research in the field, ending with encouragement to help a student complete his PhD thesis. Figure 18 below shows the sequence of participant recruitment for the interviews through snowballing with each letter representing a participant.

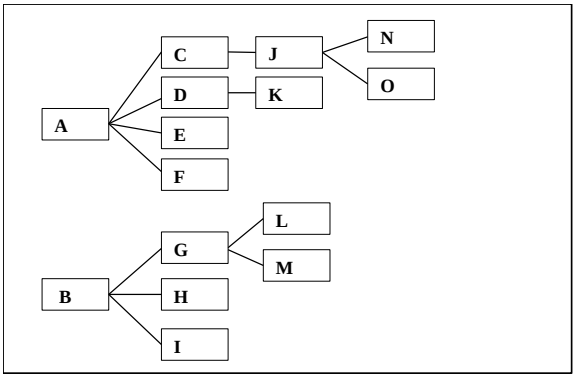

Figure 18: The results of snowball sampling (letters represent participating firms)

By the time 15 interviews were conducted it was clear that saturation had been reached as no new information was being generated (Gordon, et al., 2005). Further, a number between 5 and 25 interviews is sufficient for a phenomenal study (Creswell, 2012). The remaining five potential participants were contacted over the phone and told that enough data has been collected for now and that they would be contacted later if more data were required.

Of the 15 interviews, five were conducted over the phone and 10 were conducted at the participant's workplace during office hours. As noted above, none of the interviews conducted over the phone were recorded. Of the face-to-face interviewees, seven gave their consent for the interview to be recorded; the remaining three, though did not object, showed hesitance and discomfort when recording of the interviews was suggested. The responses of the participants who objected were recorded on paper. Finally all the recorded interviews were transcribed and analysed along with the textually recorded responses. The roles of the interviewees are given in Table 11.

Table 11: Interviewee characteristics

	Organization Type	Position	Experience	Interview type
1	Customs Broker	Senior Broker	10	Face-to-face
2	International Trader	Head of Exports	7	Face-to-face
3	Customs Broker	Broker	12	Phone
4	Shipping and Freight Forwarder	Senior Manager	11	Face-to-face
5	Freight Forwarder	Manager	7	Phone
6	Cargo Clearance	Customs Broker	10	Face-to-face

	Organization Type	Position	Experience	Interview type
7	Cargo Clearance	Customs Broker	10	Face-to-face
8	Freight Forwarder	Freight Agent	9	Phone
9	Shipping and Freight Forwarder	Freight Agent	6	Face-to-face
10	Cargo Clearance	Manager	8	Phone
11	Cargo Clearance	Manager	13	Face-to-face
12	Logistics Operator	Customs Broker	11	Phone
13	International Trader	Customs liaison	7	Face-to-face
14	Cargo Clearance	Manager	9	Face-to-face
15	Exporter	Manager	9	Face-to-face

6.4 Qualitative Analysis

As noted in Chapter 5, the strategy applied to analyse the interviews was as outlined by Saba and Shearer (1994) and the guidelines from Thomas (2006) were followed. These included reading the text to identify surface level details, identifying themes and defining categories by assertions from the data as a whole which indicate relationships and generalizations (Maloni & Benton, 2000) in order to achieve reliability and validity. The process of identifying themes and categorizing the themes was carried out with the assistance of two independent PhD graduates. Assistance was sought from these two students to ensure that the researcher is non-biased in understanding and classifying the expressions of the participants. The researcher and these two assistants recorded their own set of themes in accordance with what was identified from the literature. Once each of the three lists was completed, each of the identified themes was discussed one by one and put into the identified categories. Words, phrases or events that appear to be similar can be grouped into the same category and may be gradually modified or replaced during the subsequent stages that follow (Hoepfl, 1997) . This exercise resulted in creating a general phrase or sentence which captured the essence of each respondent. The main objective of this exercise was to verify that the participants express in their own words the themes identified from the literature. The outcome of this exercise is summarised in the following

Table **12**. According to Onwuegbuzie and Teddlie (2003), qualitative data can be quantified by enumerating the frequency of themes associated with a given category of respondent, or the percentage of people selecting specific themes. This exercise resulted in Table 13.

Table 12 : Grouping of similar phrases that captured the essence of the identified themes

	Theme from Literature (Code)	**Question and the keywords and phrases extracted from the responses which portray or express the identified themes.**
1	Regulatory demands	What is your perception on the local regulatory authority's demands in relation to information security in the exchange of information between the supply chain stakeholders and the authorities? **Responses** 1. Cumbersome; form is denied (burdensome, stringent) 2. Never easy; strict and demanding (burdensome, stringent) 3. Financial implications; time consuming (burdensome, costly) 4. Heavy workload due to strict time constrains; (burdensome) 5. Should be completed and submitted in a given time frame; strict (burdensome, stringent) 6. Not very sympathetic; gets what they want (stringent) 7. Strict demands; lose business (stringent, costly) 8. Tough and strict; Costly (burdensome, stringent , costly) 9. Too much work; difficult to deal with (burdensome, stringent) 10. Very demanding and strict; costly training and software ((burdensome, stringent , costly)
2	Market influence	What is your perception on the authority's promotion of information security in the information exchange standards and the adoption of these standards by other stakeholders within the supply chain? **Responses** 1. Every broker I know is aware; Customs website, flyers; customers check our knowledge (compliant, customer confidence) 2. All the brokers are aware of the consequences through Customs bulletins, website; Customers are concerned so are we; (customer confidence) 3. We need to be registered as a broker to submit customs docs; that sends a message to the customers. (compliant, customer confidence) 4. Brokers are registered with the customs; no one will approach a non-registered broker (compliant, customer confidence)
3	Peer pressure	What is your perception of your competitor's behaviour towards the information exchange requirements within the supply chain? **Responses**

		1. Avoid penalties from customs as other brokers manage to avoid it (bad image) 2. Delayed cargo leads to loss of customers to competition; other agents spread the word (competition) 3. Follow big companies; their ways work (identification) 4. Monitor what the successful agents do; how are they getting all the privileges (successful agents)
4	Perceived norm	What is your belief on the expectation of people who influence you and who are important to you think how you should behave towards the information exchange requirements? **Responses** 1. It is well understood non-compliant parties are delayed (understood) 2. Our customers choose us because we are compliant (choose) 3. Our stakeholders (believe) that compliance is a (regular practice) 4. Our stakeholders (continuously monitor) that we comply
5	Perceived threat	What is your perception of the negative outcomes if you do not follow the authority's requirements? **Responses** 1. Any error in the form, cargo is delayed and penalty incurred (penalty) 2. You want to avoid penalties, it is an added cost (cost) 3. Frequent delayed cargo may lead to losing customers (lose) 4. Customers have directly threatened to switch to our competitors if there are compliant issues (switch) 5. Privileges suspended or warned of suspension if too many errors (warning)
6	Perceived benefits	What is your perception of the benefits to you and to your peers, if you follow the authority's requirements? **Responses** 1. It is beneficial when cargo is released without delayed inspections 2. Bigger firms set the standard and we learn from them (lowers cost of training and research) 3. Good relations by complying helps, ignores minor errors 4. Increases customer confidence 5. Bigger firms recommend us to smaller clients; good reputation 6. Authorities sometimes make non-formal recommendations to new customers
7	Fairness	What is your perception on impartiality, refutability, explanation, familiarity and courtesy towards you from the authority?

		Reponses 1. Some officers are stringent, irrespective of our compliance status (irrespective) 2. Some officers are clear on the next step to take, while others may choose to penalise (choice) 3. There have been instances where cargo have been delayed without prior notice or explanation (prior notice) 4. Most of the time adequate opportunities are given to explain the situation, during an erroneous application. (adequate) 5. Do not know which parties have been fined or penalised. Clients must know; do not know who are slacking. (know) 6. Most of them are courteous most of the time (most)
8	Reciprocity (Reward)	<u>What is your perception on the reciprocity (incentives and rewards) when you comply?</u> **Responses** 1. Everybody seems to be getting the privileges; therefore do not feel special or rewarded (customers are not aware) 2. Quick clearances makes our customers happy (reward) 3. We expect the authorities to reciprocate us for our compliant behaviour (reciprocate) 4. We were explained of the rewards if we went along with the compliant programs (rewards expectation)
9	Symbolic and substantive compliance	How does your organization conduct itself in fulfilling the information security compliance requirements? **Responses** 1. We believe following international security standards are beneficial; however unnecessary to this environment (unnecessary) 2. We share our passwords with non-registered brokers; they know the rules and regulations (sharing passwords) 3. Our brokers do not share their passwords with anyone. (we are very strict on that) 4. We know each other and trust each other, therefore no need of a security policy (no need of security) 5. We have not been audited, but would fail if audited on security issues 6. We do not have a secure file system. All the staff have access to the files (they are not treated as trade secrets) 7. Have been infected with viruses. Do not have firewalls or antivirus software 8. Our company policy demands firewall and anti-virus software 9. We have processes in place that includes security standards demanded by the authorities. (staff are penalised if not complied)

The findings are analysed and discussed in this section under the main categories identified in the conceptual model illustrated in Figure 15 (Chapter 4). These categories are: (1) organizational perceptions towards compliance (threat, benefits and norms), (2) inter-organizational influences (regulatory, market and peer), and (3) norms and rules of social exchange (fairness and reward). Direct quotes from the participants are presented to support the arguments made. A summary of the key findings is presented in Table 13.

6.5 Findings and Discussion

6.5.1 Compliance Behaviour

Almost all organizations gave unrestricted access of all employees to customer and shipment records and used common passwords and sharing of user terminals. Though there was also common agreement in standards and policies to protect information and information systems, they believed they operated in a very trusting and peaceful environment as far as SCS was concerned. They also believed that if they were audited on the basis of CSI, CT-PAT or other global SCS initiatives, they would be likely to fail. Hence, it can be inferred that there was symbolic compliance behaviour in play.

> "We are a small community and we know each other very well, so mostly it is trust based rather than following policies and international standards." [6]

> "If we are audited under the standards of CT-PAT or CSI, we will definitely fail." [2]

6.5.2 Organizational Perceptions towards Compliance

6.5.2.1 Perception of Threats

Fear appeals are persuasive messages designed to inform that terrible things will happen if compliance is not forthcoming (Witte, 1992). When a fear appeal is successful in eliciting a significant perception of a threat, cognitive processes employ strategic responses to avert the threat (Johnston & Warkentin, 2010). The interviewees understood there were threats for non-compliance, such as delayed shipments due to lengthy physical inspections and penalties leading to financial implications, both leading to reduced customer confidence. This reduced customer confidence can lead to the customer threatening to switch service providers. From the following comment, it is evident that strong and threatening communication occurs between the freight forwarders and their customers on compliance issues.

> "The more complicated our involvement (with the authority) gets, the more unpopular we become with our customers, and as you can see from the emails they sent us, threatening to switch shippers if we fail to comply." [5]

Hence it can be inferred that there is the perception of threats among the respondents, proving the relevance of the threat perception in the given context.

6.5.2.2 Perceived Benefits

The health belief model posits that healthy behaviour is a product of an implicit and subjective assessment of the relative costs and benefits of compliance in relation to personal goals and the constraints of everyday life (Gassenheimer, Houston, & Davis, 1998). Drawing parallels with this theoretical perception, the interviewees stated that when the authorities are led to believe that information provided is accurate and complete, the organizations receive quick clearance times which is both beneficial to the organizations in terms of cost and also to the customers in terms of quick delivery. The interviewees perceived that being compliant was beneficial, as illustrated by the following comment:

> "We do what they (authorities) ask and our shipments are untouched, let's say one every ten to fifteen and that is good." [9]

Thus perceived benefits are relevant to this research context.

6.5.2.3 Perceived Norms

Perceived norms refer to one's belief that the prevailing behaviour is the norm and the greater that perceived prevalence of behaviour the greater the likelihood of engaging in the behaviour (Kingsolver & Schemske, 1991). The interviewees believed that customers and authorities have high expectations that they comply with security requirements. As the comment below exemplifies, there was general understanding among the respondents that if there were any shortcomings in compliance, the shipment will not move any further. From the responses it can be inferred that being compliant is an industry norm; thus perceived norms are relevant to this context.

> "Without the proper and accurate paper work submitted to the local authorities and to the authorities across the border, there is no chance of the shipment moving across the border." [15]

6.5.3 Inter-organizational Influences

6.5.3.1 Regulatory Demands

Studies based on institutional theory show that when faced with an apparently hostile legal environment, organizations adopt formal structural changes as symbolic gestures of compliance with the government policies for strategic gains (Tolbert & Zucker, 1999). In this context as regulatory demands over the organizations. A common theme emerging from the data was influence and pressure from the authorities to provide accurate and timely information, which is sometimes not an easy task. The respondents felt there was pressure from the authorities, through threats of fines and time-consuming physical inspections, to ensure that the authorities' requirements are met. This indicates the relevance of regulatory demands in the given context. Senior managers interviewed made the following comments:

> "Correct information according to their (authorities) requirements should be submitted before shipment can be moved. Officers are friendly and helpful, but documentation should be completed before you get their corporation." [4]

> "These security requirements are costly and pressurizing because we have to make sure that we have to have things done before the time frames." [6]

> "If we miss on any information on the manifest on a going out shipment, we will face a penalty, so there are some financial implications if you make a mistake." [3]

6.5.3.2 Peer Pressure (Competitive Influence)

Interviewees agreed that their customers were aware of the security requirements of the authorities. Organizations were also commonly concerned that if a shipment gets delayed or fined due to inaccurate information, it could result in loss of customers to one of their competitors. The interview data reveals that in order to keep their own customers, the organizations ensured that they closely followed their competitors as much as they could within their means. When competitors have pre-tested the structures which are proving successful an organization is more likely to adopt them (Tolbert & Zucker, 1999). Thus, the interview data suggest competitive influence plays a role in their compliance behaviour:

> "We are not aware how compliant our competitors are, but they should be doing something right else their shipments will not go through … we also ensure that our shipments do not get rejected at port." [6]

> "We keep a watchful eye on the larger companies and even talk to their clients ... sometimes." [1]

6.5.3.3 Market Influence

The legitimacy of market influence as an institutional force was established by Scott (1987). Scott and Meyer (1982) define the market as a technical environment where organizations are rewarded for their conformity to the other actors such as the state, professional associations, and competitors. In line with this argument, the interview data show that the organizations collectively believe that their operating environment exerts a strong influence on what they should do and how they should behave as far as security compliance is required. A common theme was that they all wanted to be seen as organizations who meet all compliance requirements in order to build customer confidence. The following comments are evidence that market influence is a relevant factor in this research context:

> "Customers are aware that the authorities are very strict on the information requirements, and they keep a watchful eye on how we conduct our business. If we get their shipment in trouble with the authorities, it affects their (customer) reputation. If that happens, the chances are we might lose that customer. So far we have had no problem with the authorities regarding a shipment." [7]

> "We do what we can to keep up with the requirements of the authorities. We do not want to be seen as an organization that gets their shipments delayed due to lengthy inspections and that is bad for business. So far we have never been stopped for insufficient or inaccurate information." [7]

Analysis led to the inference that to survive in the industry of cross-border cargo movements, the respondents felt they had to be seen as fully complying with security requirements. The way to prove that to their customers was by ensuring that their cargo flows through customs without any glitches. Hence, it can be inferred that market influence impacts on their compliance behaviour

6.5.4 Norms and Rules of Social Exchange

The norms and rules of social exchange are defined by two principles derived from SET: *fairness* derived from power and dependence; and *reward* derived from reciprocity.

6.5.4.1 Power and Dependence (Fairness)

According to Fehr and Gächter (2000), the power to enforce social norms through collective actions is one of the most important consequences of reciprocity. Fehr and Gächter further state that the number of people in a society who show concern for fairness and behave reciprocally in a given situation is relatively high. In the organizational context, the interviewees believed that authorities have a generalized attitude towards complying and non-complying parties. This is to say that because some brokers or shippers do not comply, the rest have to go through the same stringent requirements. This is a judgement of fairness. In the comments below there is evidence that the organizations believed that there should be a continuous auditing system put in place by the authorities to identify non-compliant free riders. This belief is in line with Fehr and Schmidt (1999), who argue that fairness judgements are inevitably based on a kind of neutral reference outcome that is used to evaluate a given situation of a complicated social comparison. Hence, it can be inferred that the respondents consider fairness, or lack of it, as a factor impacting on their behaviour towards compliance.

> "We have to do all the documentation as strictly as the slack companies and there should be a system where the customers know which companies have a good record of compliance in terms of submission of accurate and complete information to the authorities. It is not fair at all" [11]

> "We agree that we get through customs faster if we keep our information accurate, but then again the guy who has a bad record (fined before) also goes through if he checks out." [9]

6.5.4.2 Reciprocity (Reward)

Fehr and Gächter (2000) argue that in order for social policies to be endorsed by the public, they need to be rewarded selectively for their contribution to the society rather than irrespective of their behaviour. In the organizational context, the participants appreciated the preferential arrangement where complying parties are given easy and quick flow of cargo through the borders. They perceived this as a reward as it helps to attract new customers and assure the existing customers of the organization's good relationship with the authorities. Although the following comments appear to contradict each other, the majority of participants felt that reward is a relevant factor to explore in this context.

"For us reward is they (the authorities) trust that the documents from us are solid and will never be held for inspection unless selected randomly, which is like, one out of every 20 to 30 shipments. So we ensure that all the time our documentations are proper." [13]

"We do not think we are being rewarded, we do what is required, and as long as we do that, they (customs) should treat us accordingly." [3]

6.6 Contribution of the Qualitative findings to the next stage of analysis

The objective of this qualitative survey was to verify the conceptual model and confirm the existence of the identified themes that led to the formulation of the constructs of the conceptual model. Furthermore, this phase was expected to ensure that the foundational understanding informed by the literature is relevant to the research context.

As mentioned before, due to the intrusive nature of the interviews, the participants did not engage in lengthy discussions. It can be inferred from Gauzente (2004), that when there is a higher perception of intrusion, the reluctance to provide information will be also high. Therefore, during this exercise there were no discoveries of new themes emerging from the discussions. Hence, there was no evidence that suggests or new information that required any additions to the model.

Verification in qualitative research is the process of checking, confirming, making sure and being certain that fit of data is relevant to the context and the sample appropriately represents participants who best present or have the knowledge of the research topic (Morse, et al., 2008). As such the results of the analysis prove that the context is valid. Further, the actors of the supply chain environment portray an acceptable level of understanding and experience required to establish the relationships among the identified constructs of the conceptual model, through a quantitative study. This is evident from the discussions presented in the above sub-sections, grouped expressions presented in Table 12 and also the statistical quantification presented in Table 13.

For a survey to succeed in clarifying causal relationships or even in providing descriptive statistics, the survey instrument must contain the right questions asked the in the right way (Gable, 1994). In this sense, the expressions and terminologies gathered from the qualitative analysis paved way for framing of the quantitative survey questions which are native to the

supply chain security context of New Zealand. For instance, almost all of the participants had difficulty in accepting that they were being rewarded for their compliance actions but more at home when the term reciprocity was expressed. Hence, all the expressions of the questions of the items adopted for the quantitative phase were changed to reflect the understanding of similar terms in the given context.

The last but not the least contribution of the qualitative phase comes from the recruitment of participants for the quantitative phase. Several studies express the situation where the quantitative survey instrument or the website link sent through email ends up the junk folder or as spam. However, during the interviews the participants were requested to invite their colleagues and professional contacts to participate in this study. This was a major boost in the number of participants in the quantitative survey for such an intrusive study. In some cases they took the initiative to send the web link to their colleagues using their own email. Further, they acted on the researchers behalf to call some of the participants and ensure that they have completed the survey. Hence, the qualitative phase contributed in the successful recruitment of participants, which would have been quite a challenging task considering the intrusive nature of the study.

Hence, the qualitative analysis has provided sufficient confidence in conducting the dominant quantitative phase of the survey by verifying the relevance of the context to the research, revealing the socio-technical complexity of the context and finally how the expressions and phrases used in the literature differ to the actual research context.

6.7 Summary of the Qualitative Analysis

Table 13 summarizes and classifies the themes identified from interviews. The percentages represent the number of participants with the specified view. Figure 19 shows the resulting relationship diagram. The qualitative analysis verifies and confirms the themes and aspects of the conceptual model. As discussed in Chapter 5, the objective of the qualitative survey was to verify and confirm the constructs of the conceptual model formulated from themes identified from the literature and ensure that the foundational understanding informed by the literature is relevant to the research context. Table 13 and Figure 6.1 are tabulated and graphical representations respectively of the relationships among the aspects identified in the conceptual model.

Table 13: Summary of qualitative analysis

	Labels	Emerging themes (with % of interviewees who mentioned them)
1	Regulatory demands	(i) Burdensome and costly information requirements by the authorities (93%) (ii) Stringent in their (authorities) demands (80%)
2	Market influence	(i) Want to be seen as organizations with all the security compliances met (80%) (ii) Ensure customer confidence (93%)
3	Peer pressure	(i) Want to avoid fines (bad for competition and image) (80%) (ii) Want to avoid lengthy inspections (bad for competition and image)(80%) (iii) Build customer confidence and not to lose customers to competition. (93%) (iv) Other successful companies set the standards (73%)
4	Perceived norm	(i) Industry norm is to comply (93%) (ii) Common knowledge that shipment will not precede any further without compliance (80%)
5	Perceived threat	(i) Threats of fines (80%) (ii) Threats of lengthy inspections (80%) (iii) Threats of losing customers (73%)
6	Perceived benefits	(i) Quick clearance times as a result of complying is beneficial (80%) (ii) Industry norm to comply helps small brokers to follow suite (73%)
7	Fairness	(i) Few organizations slack in compliance leading to unfair strictness in the process to all (60%) (ii) No information revealed to the public on organizations being fined due to non- compliance (which is unfair) (60%)
8	Reward	(i) Enjoys quick clearances for being compliant (73%) (ii) Do not perceive quick clearances as a reward (80%)
9	Compliance behaviour	(i) Shares systems passwords (80%) (ii) Documents are accessible to all the staff (93%) (iii) Licensed brokers share their passwords with other non-licensed staff in submission of documents to authorities (73%) (iv) Do not need strict internal security policies (73%) (v) Would fail a security audit (60%) (vi) International security standards are unnecessary (60%)

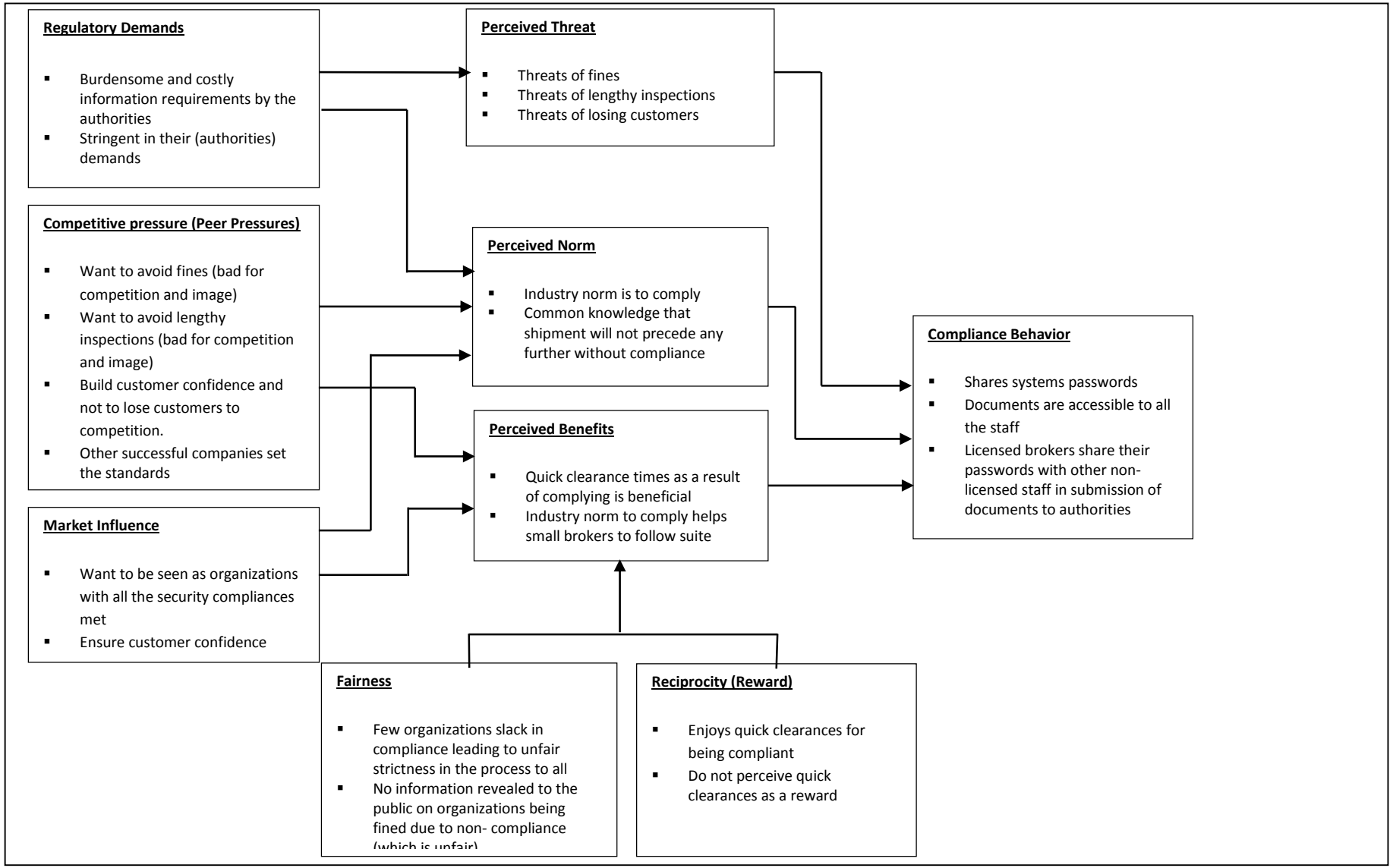

Figure 19: Relationship diagram based on the qualitative findings

As seen in Figure 19, the results of the analysis fit into the identified broad categories of the conceptual model presented in Figure 15 and the implications reported in Table 2. This confirms and verifies the constructs identified from the literature and used to formulate the conceptual model.

However, there were slight differences in the perceptions of the participants compared to the findings of the literature on the prevailing environment. For instance, New Zealand has not been a target of a terrorist activity involving the supply chain. This was a discussion point among a few of the participants but nevertheless all participants were fully aware of the worldwide consequences of the September 11, 2001, terrorist attacks in terms of more stringent security compliance requirements. Since, the objective of the qualitative phase was to verify and confirm the identified constructs and not prepare for triangulation with the findings of the quantitative phase, these findings cannot be generalized. In addition to the verification outcome, one important finding that assisted in Phase 2 was the evident knowledge of the participants on the GSCS initiatives and its implications. This is an indication of the viability of the research in the New Zealand context.

The next chapter describes the development of the research model and hypotheses in order to operationalize the quantitative survey.

CHAPTER 7: THE RESEARCH MODEL AND HYPOTHESES

7.1 Chapter Overview

The research model formulated in this chapter extends the conceptual model proposed in Chapter 4. This extension was made after establishing the relationships that exist among the aspects of the conceptual model through a qualitative inquiry. The relationships found through the qualitative survey are presented in Table 13 and Figure 20 (Chapter 6). This chapter develops the research hypotheses posited to establish the significance of these relationships. Figure 20 outlines the steps leading to the formulation of the research model and hypotheses.

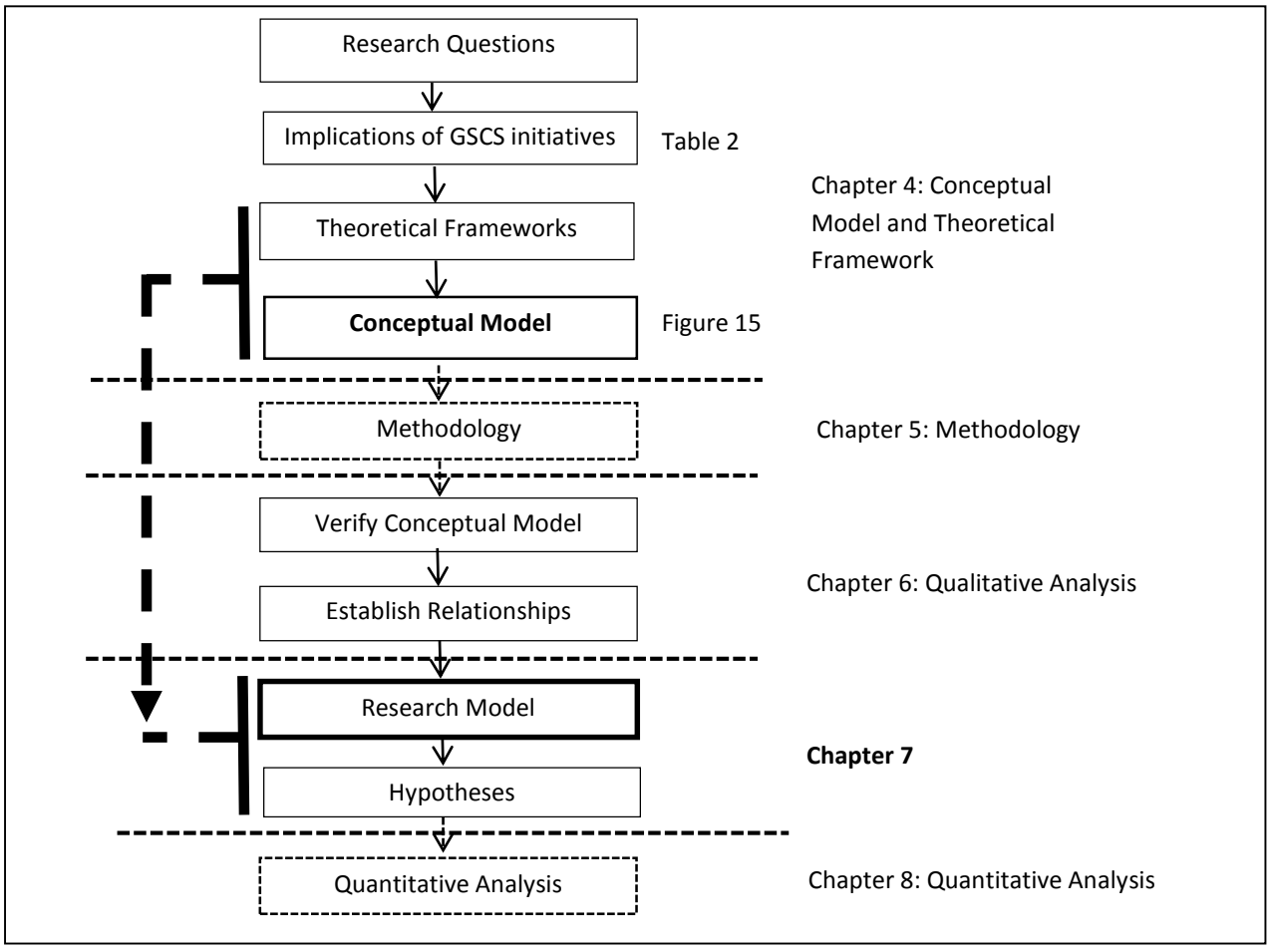

Figure 20: The steps taken to arrive at a research model and the hypotheses

7.2 The Research Model

Chapter 4 described the conceptual model developed from the outcomes of studying the implications of the GSCS initiatives presented in Table 2 (Chapter 4), and linking these with well-established theories. The conceptual model was then verified by interviewing market

stakeholders on the relevance of the aspects included in the model to the research context. The analysis from the interviews that demonstrates the relevance of the model to the research context was discussed in Chapter 6. In this chapter, some of the arguments made by the participants during those interviews are used to further support the arguments regarding the relevance of the research constructs to the prevailing heightened security environment, as well as the relationships between the constructs. This was one of the main reasons for using the sequential mixed methods research design, as the qualitative phase provides reinforcement of the relevance of the chosen constructs of the research model to the actual research context. In this sense, it is important to reiterate the fact that the findings of the qualitative phase will not be triangulated with the findings of the main quantitative phase. However, these findings and the arguments of the participants are used to verify the research model and make the definitions of the research constructs clearer.

The research model presented in Figure 22 has been developed from the conceptual model developed in Chapter 4 to define key constructs within each of the elements and the relationships between the constructs.

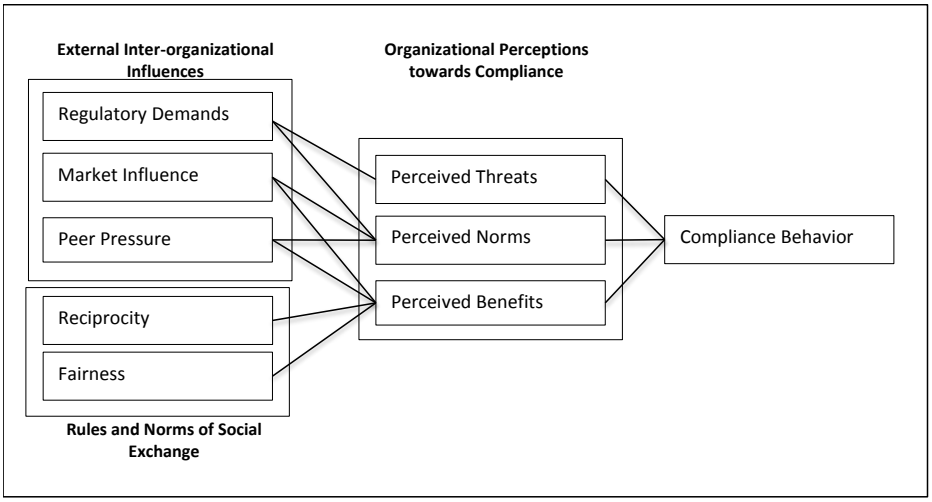

Figure 21: The research model

The constructs that define the organizational perceptions towards compliance are identified as important aspects for an organization because they dictate how the organization complies with information security requirements. These constructs are perceived threats (fear appeal), perceived norms, and perceived benefits. The external inter-organizational influences, based on the core constructs of institutional theory, are formulated as regulatory demands (coercive pressure), market influence (normative pressure), and peer pressure (mimetic pressure). The rules and norms of social exchange are explained through the core constructs of fairness (power

and dependence) and reciprocity, and are taken from SET. These constructs are defined and explained later in the chapter.

By relating external inter-organizational influences and rules and norms of social exchange to organizational perceptions towards compliance, the research model will explain how pressure from external inter-organizational influences, as well as the rules and norms of the exchange relationship, impact organizational perceptions towards compliance and how these organizational perceptions in turn impact the type of compliance behaviour exhibited by organizations.

7.3 Definitions of the Constructs

7.3.1 Compliance Behaviour

For the purposes of this research, compliance behaviour is defined as the response by the market stakeholders to the information security requirements demanded by the authorities in respect to the GSCS initiatives. According to Christmann and Taylor (2006), compliance is not a binary process where an organization is either compliant or non-compliant, but rather a range of implementation behaviour between symbolic and substantive, strategically chosen by organizations to fit their needs. Compliance behaviour will be measured on a scale going from low to high, in line with "lower compliance" (Levinson, 1996) and "greater compliance" (Gray & Deily, 1996) found in the literature. A high level of compliance behaviour implies substantive compliance behaviour, while a low level of compliance behaviour implies symbolic compliance behaviour (Christmann & Taylor, 2006). Substantive compliance behaviour refers to material changes in organizational goals or structures to maintain acceptability, while symbolic compliance behaviour is performing corporate activities in a superfluous manner to gain approval (Day & Woodward, 2004). There is extensive research on symbolic behaviour in terms of adopting policies or codes of conduct without necessarily applying them in practice (Westphal & Zajac, 1994). This symbolic behaviour is an important aspect of organizational behaviour from an institutional theory perspective, as it defines the environment and delimits social reality (Scott, 1987). As such, these forms of symbolic gestures of compliance with government policy through constructing formal organizational structures are strategically performed to elude provocation (Edelman, 1992). The findings from the qualitative survey established the presence of symbolic behaviour as well as substantive behaviour among the participants interviewed.

In the given context of the GSCS initiatives, there is always some form of compliance as the security requirements demanded by the authorities have to be fulfilled before any consignments are authorized for shipping. Therefore, at the very least, market stakeholders would have to exhibit behaviour that portrays some level of compliance to be able to ship their cargo, even though the compliance may not be fully implemented as intended by the authorities. Hence, low compliance behaviour will be considered as symbolic compliance behaviour and high compliance behaviour will be considered as substantive compliance behaviour.

7.3.2 Organizational Perceptions towards Compliance

The constructs described below as organizational perceptions are themes that have been widely discussed in the context of intra-organizational and individual behaviour towards information security compliance. For the purposes of this research it is proposed that these constructs will be impacted when subjected to inter-organizational influences.

7.3.2.1 Perceived Threats

Perceived threats refer to the knowledge of danger being involved that influences people's intention to comply with information security requirements (Huang, et al., 2011). Perception of threats is prevalent when an organization's actions are guided through coercion or threat of legal sanctions (Hoffman, 1999) by the exertion of power by the state to gain compliance (DiMaggio & Powell, 1983; Lawrence, et al., 2001; Liang, et al., 2007). For the purposes of this research, perceived threat is defined as the knowledge of the market stakeholder of the negative consequences that could result due to non-compliance with the information security requirements of authoritative organizations. This was evident in the interviews where respondents expressed the uncertainty of the outcome if the required level of performance was not met with respect to the security requirements. The main concern identified was the threat of being subjected to heavy fines or the lengthy physical cargo examination, which could be quite costly for the market stakeholder.

7.3.2.2 Perceived Norms

Perceived norm refers to one's belief that the prevailing behaviour is the norm and the greater that perceived prevalence of behaviour, the greater the likelihood of engaging in the behaviour (Kingsolver & Schemske, 1991). According to institutional theory, for a given group of organizations, deviation from group norms can result in inferior performance (DiMaggio & Powell, 1983). Bendor and Sistak (2001) argue that norms are meaningful to the extent that it

is perceived that, if violated, some social sanction will result. It was revealed from the analysis of the interview data that the general belief among market stakeholders was that complying with the information security requirements was the only way that they could keep the goods flowing across the border without any delays. For the purposes of this research, perceived norm is the extent of the belief of the market stakeholder that conforming to the information security requirements of the authoritative organization is the prevailing norm of conduct for market stakeholders.

7.3.2.3 Perceived Benefits

Perceived benefits are the overall expected favourable consequences to an organization (Bulgurcu et al., 2010). For the purposes of this research, perceived benefits refer to market stakeholders' belief that by complying with the information security requirements of the authoritative organizations, they will benefit directly from both the authoritative organizations and other market stakeholders. This is inferred from (DiMaggio & Powell, 1983), who state that institutional pressures may in fact lead to benefits when organizations strategically align themselves to other similar organizations by internalizing their structure to the demands of the environment. The analysis of the interview data supported these arguments in suggesting that when the information provided to the authorities is accurate and complete in terms of compliance, market stakeholders receive quick clearance times which are beneficial to the organization in terms of both cost and efficiency. Further, it was revealed that when the target organizations comply with the information security requirements of the authorities, other stakeholders such as their partnering firms within the supply chain are more ready to collaborate with them, thereby strengthening the inter-organizational relationship.

7.3.3 External Inter-organizational Influences

7.3.3.1 Regulatory Demands

Coercive pressure is mainly exerted by the state on organizations and refers to threat or actual use of force to gain compliance (DiMaggio & Powell, 1983; Lawrence, et al., 2001; Liang, et al., 2007). Coercive pressure is more likely to emanate from government authorities (Liang, et al., 2007). Within the supply chain context selected for this research, coercive pressure originates from regulatory authorities such as customs and port authorities, and can be exerted on trading organizations within the supply chain. This was very apparent from the interviews where participants revealed the pressure exerted by the authorities in terms of providing

accurate and timely information in advance. Therefore, for the purposes of this research, regulatory demands are defined as the pressure by authoritative organizations, such as customs and port authorities, on market stakeholders within the supply chain to comply with the information security requirements enforced by the authoritative organizations.

7.3.3.2 Market Influence

When an organization acts in a manner to ensure its membership is legitimate and to be identified among an autonomous occupational environment, then its actions can be defined as being performed under normative pressure (DiMaggio & Powell, 1983)**.** DiMaggio and Powell (1983) also argue that in an occupational environment organizations tend to view problems in a similar fashion, leading to normatively sanctioned structures. Normatively sanctioned structures are structures that respond to problems through defence mechanisms importantly shaped by shared values which are deeply internalized in the members (Abrahamsson, 1993). There is an expectation of shared norms from each legitimate member of the occupational environment (Turker, 2014), which influences stakeholders to uphold these norms. The occupational environment in this study's context can be referred to as the market environment which consists of the traders, logistics operators and the customs brokers, and thus the normative pressure will be referred to as market influence in this research. The findings from the interviews suggest that almost all of the participating organizations want to be seen as organizations who meet all compliance requirements in order to build customer confidence, and that therefore market influence is a relevant factor. In this research, market influence is defined as the normative pressure arising from the market environment, such as customers, on market stakeholders to comply with the information security requirements of authoritative organizations.

7.3.3.3 Peer Pressure

When technology is poorly understood and what could be achieved is ambiguous, organizations respond to uncertainty by mimicking actions of other organizations (DiMaggio & Powell, 1983). Mimetic pressure originating from these successful competitors has a huge influence on other organizations (Turker, 2014). For this research context, mimetic pressure is the pressure on market stakeholders to mimic the compliance behaviour of successful competitors, such as other customs brokers, freight forwarders and traders, with regard to the information security requirements enforced by authoritative organizations. The findings from the interviews indicate that the organizations ensured that they followed their competitors as much as they could within

their means. This is to ensure that they do not lose a customer to one of their competitors, due to a shipment getting delayed or being fined for lack of compliance. Hence, for the purposes of this research, peer pressure is the mimetic pressure arising from the competitors of market stakeholders that compel the market stakeholders to comply with the information security requirements of the authoritative organizations.

7.3.4 Rules and Norms of Social Exchange

The rules and norms of social exchange are defined by two constructs, fairness and reciprocal actions such as reward from the authorities, which are derived from SET and are perceived as beneficial to the organization (Rodríguez & Wilson, 2002). SET has the ability to add depth to the study of inter-organizational relations in ongoing supply chain relations by providing new insights into controlled self-interest (Narasimhan, et al., 2009). In this sense, fairness through social exchange is an important aspect to maintain and sustain an inter-organizational relation (Gassenheimer, et al., 1998).

Power and dependence in a social exchange context are manifested in reward-seeking (and punishment-avoiding) behaviour (Aldrich & Herker, 1977) and as the exchanges proceed, the exchange ratio reaches an equilibrium where one is dependent on the other (Ancona & Caldwell, 1992). In the context of SCS, the authorities depend on market stakeholders for providing accurate information for gathering intelligence and in return the market stakeholders are rewarded with expedited cargo clearances. Market stakeholders depend on these reciprocated privileges accorded through the cooperative relationships to survive in the market (Tokman, Richey, Marino, & Weaver, 2007). This is different to the power exercised in coercion as theorized in institutional theory, where coercion, such as regulatory demands, is exercised with passive dependency. According to Zhuang and Zho (2004), passive dependence is due to lack of choice. However, dependence and power from a social exchange relation perspective as used in the research model is active dependence and reward power, where reward power is defined as the power to reciprocate (Turker, 2014). In the GSCS initiatives context, the Container Security Initiative enforced by the United States provides such reward power by law to the authorities to reciprocate, and the authorities can be selective as to whom they reciprocate with (Romero, 2003). In active dependence, one actually pursues dependence on a powerful member, because such a relation is important for one's future (Edelman, 1992). Furthermore, Zhuang and Zho (2004) argue that a power holder offers dependable support to lesser stakeholders. Active dependence and passive dependence in the research context are both

important for an organization's future. However, regulatory demands to comply puts market stakeholders in uncertainty (Hoffmann & Trautmann, 2006), which leads to passive dependence. Active dependence provides an opportunity to reduce this uncertainty through negotiated social exchange rules such as fairness and reciprocity.

7.3.4.1 Fairness

To develop an inter-organizational relationship, the perceived fairness of contributions an important factor (Gassenheimer, et al., 1998). In this respect several studies have reported the importance of fairness using SET in inter-organizational information exchange, especially in preventing terrorism (Lee & Rao, 2007).

Fairness, concerning the payoffs from an exchange, arises when there is unequal power in a power dependence relation (Iriondo, Albert, & Escudero, 2003) such as the relation between market stakeholder (customs broker) and the more powerful non-market stakeholder (customs). Fairness, according to Leventhal (1976a), is judged in terms of the procedure's consistency and its representativeness of important subgroups, and dictates that persons who contribute more should receive more. This is a social expectation, which demands that those who make the effort to fulfil compliance requirements should be recognized over those who do not. During the interviews with members of the supply chain community, participants commented that fairness need not be formally regulated, but there should be a mechanism whereby the social expectation of fairness could be met. For instance, the way the authorities treat a market stakeholder during a mishap should be differentiated between market stakeholders who comply and those who do not. In other words, compliance efforts should be valued and complimented accordingly. This expectation in social exchange is defined as value in terms of satisfaction with the exchange situation (Deutsch, 1975; Thibaut & Kelley, 1959). In this sense, when there is dissatisfaction regarding the inter-organizational relation, alternative solutions include compromising the interests of both parties, tolerating adverse conditions, or exiting the relationship altogether (Gassenheimer, et al., 1998). However, in the current inter-organizational relation between market stakeholders and non-market stakeholders, there is no way that market stakeholders can exit the relationship if they are to remain as a stakeholder of the cross-border supply chain. Hence, the choice would be either to compromise the interest of both the parties or tolerate adverse conditions.

Fairness, as an aspect to information security, has been studied in various contexts. Culnan and Armstrong (1999), in the context of information privacy, discuss fairness as inseparable to

service quality and note that the perception of fair treatment of customers has been shown to higher levels of satisfaction and fairness is inherent in the consumer's basic need for justice.

For the purposes of this research, fairness is defined as market stakeholders' expectation of authorities to value their efforts towards compliance and treat them accordingly in the application of the procedures formulated by the authorities to comply with the information security requirements.

7.3.4.2 Reciprocity (Reward)

Reciprocity is defined as a method of repayment in kind as a rule of exchange (Cropanzano & Mitchell, 2005). Cropanzano and Mitchell (2005) propose three different types of reciprocity: (1) reciprocity as a transaction pattern of interdependent exchanges, (2) reciprocity as a folk belief, and (3) reciprocity as a moral norm. The GSCS initiatives most closely align with (1), as interdependence involves mutual and complementary arrangements where a bidirectional transaction occurs (Molm, 1994). This can be confirmed by various real-world actions prevailing in cross-border SCS activities. For instance, the Taxation and Customs Union (TCU) of the European Commission has several security cooperation schemes with third countries. These cooperation schemes are governed by mutual recognition and reciprocity of security measures. According to the TCU, under these cooperation schemes the traders who demonstrate compliant efforts to secure their part of the supply chain benefit from increased customs facilitation as reciprocity (Caldwell, 2010; Union, 2014). The interdependence arises when the advance electronic information provided by the market stakeholders is used by the authorities to gather intelligence for securing their borders and in return for this information the stakeholders are rewarded with the said increased facilitation. Therefore, it can be inferred that there is a close-knit inter-organizational dependence between market stakeholders and the authorities. The market stakeholder with increased facilitation will be able to cut costs by delivering the goods more quickly. At the same time, the authorities use the advance information provided by the market stakeholder to target and select potentially harmful cargo well before it arrives at the border.

Reciprocity is a key ingredient of social exchange which could be used to study information sharing and collaborative behaviour in supply chain (Wu, et al., 2014). In the research context, the authorities promise facilitation such as reduced cargo inspection and quick clearances as a reward for compliance behaviour in terms of reciprocity (Banomyong, 2005; Sarathy, 2006; Sheu, et al., 2006). According to Homans (1974), "For all actions taken by persons, the more

often a particular action of a person is rewarded, the more likely the person is to perform that action" (p. 16). In addition, Emerson (1976) states that "if an individual's actions in an exchange process are institutionally required, one might ask how reward/cost analysis can inform us about the process; yet, if valued resources are exchanged through prescribed behaviour, something resembling reward is surely involved" (p. 356).

Reward as a means for reciprocity in the context of inter-organizational relations has been studied before. Maurer (2010), in his study of trust between two organizations, focuses on reward as a facilitator of inter-organizational trust. In a more relevant context, Yang and Maxwell (2011) argue that incentives and reward are believed to positively influence inter-organizational information sharing. Yang and Maxwell (2011) also state that perception of rewards has to be focused on the groups or personnel who control the information. In other words, it is the boundary-spanning personnel who have to perceive if the reward is sufficient to be beneficial to the organization.

For the purposes of this research, reciprocity is the reward that enforcement authorities extend in the form of quick clearance times and minimized physical cargo inspections for organizations that comply with the enforced information security requirements. The reward could also be preferential treatment by giving identification to the organization, which according to Wilson (1974) is a social reward. Zhao, Huo, Flynn, and Yeung (2008) state that identification in this context occurs when the market stakeholder is publicly praised by the powerful organization and wants to establish a relationship with it.

7.4 The Research Hypotheses

This section, while referring to the research model and its constructs, formulates the 11 hypotheses which will be used to validate the model.

Table 14 lists the hypotheses for easy reference.

7.4.1 Perceived Threats under Regulatory Demands

When an organization is under regulatory demands from an authoritative organization to comply with its information security requirements, it can perceive threats that could result from non-compliance and thus is more likely to comply. This type of threat perception due to regulatory demands is quite common in enforcing environment pollution laws (Antweiler, 2003) and is sometimes referred to as regulatory threats. Similarly, the US Customs has the

power by law to stop any cargo from a non-complying importer entering the United States (Bichou, 2004), thereby creating the threat of elimination from the supply chain or the threat of cargo getting delayed indefinitely for cargo processing for non-compliant importers (Banomyong, 2005). In the context of the supply chain, there are several studies that refer to the perception of threats due to regulatory demands, including that by Walker, Di Sisto and McBain (2008) on the perceived threat related to procurement legislation in the green supply chain.

During the interviews with the market stakeholders some of the participants expressed how they felt pressured from the authorities due to the regulatory demands. They revealed that any failure to meet the regulatory demands on compliance is met with heavy fines or lengthy physical inspections. It can be inferred from these comments that there is a strong perception of threats felt by the market stakeholders due to the regulatory demands, and this led to the formulation of the following hypothesis:

Hypothesis 1

The greater the regulatory demands on an organization, the greater the threat perceived by that organization.

7.4.2 Perceived Norms under Regulatory Demands

In the supply chain environment the authorities and companies together create norms and these norms emerge when companies develop implementations, interact with other companies, and agree on industry standards (Burgemeestre, Hulstijn, & Tan, 2014). Informal norms provide a more efficient mechanism than legal rules (Milhaupt, 2001). In some cases the sanction of regulatory demands under local laws may be due to a country's signatory obligation to uphold international public laws (Casey & Scott, 2011). Further, Casey (2011) claims that those regimes which exhibit a degree of tightness in their social organization (e.g. because they are oriented around a particular profession or specialized market) are likely to have greater willingness to abide by norms rather than legal obligations. Such a tighter regime resembles the market stakeholders of the supply chain in this research.

During the interviews, some of the participants voiced their displeasure over the stringent regulatory demands over the security aspects. According to them, New Zealand does not have a history of terrorist activities involving the supply chain and not a single incident of a security threat from a shipment coming out of the New Zealand border. Therefore, they do not believe

that these regulatory requirements exhibit any local norms that prevail in the supply chain environment of New Zealand. The same concern has been raised by the Taiwanese supply chain stakeholders. Yang (2010) reports that changing local laws to secure containers did not particularly address local issues. Therefore, in the given context and in the absence of said terrorist history, whenever the bar of security requirements is raised through regulatory means, the New Zealand supply chain community is under the impression that this may be for strengthening global relations and to be in par with the global protocols, irrespective of its relevance to the prevailing local environment. This led to the formulation of the following hypothesis:

Hypothesis 2

The lower the regulatory demands, the greater the perception that information security is a norm.

7.4.3 Perceived Norms under Market Influence

Under market influence, organizations can have the perception that compliance is a norm of the market environment. In the prevailing heightened security status of the supply chain, it has become a market norm to adhere to information security requirements of authoritative organizations (Sarathy, 2006). This can be inferred as market influence across the stakeholders of the supply chain and DiMaggio and Powell (1983) state that while there is a collective struggle to protect the legitimacy of their identity as supply chain stakeholders, any deviation from these norms would lead to poor performance. As such, there is an expectation of shared norms from each legitimate member of the occupational environment (Turker, 2014), which influences market stakeholders to conform to these norms. This was evident from the analysis of the interviews as participants stated they were under constant pressure to be seen as complying with the authorities' information security requirements because the norm-setting successful organizations are known to be compliant. This led to the formulation of the following hypothesis:

Hypothesis 3

The greater the market influence on an organization, the greater the perception that information security is a norm of that organization.

7.4.4 Perceived Benefits under Market Influence

Market influence is the pressure from other supply chain stakeholders, such as customers, to be compliant with the requirements of the regulatory authorities. The motivation of market stakeholders to comply with the external information security requirements comes from market influence due to the perceived benefits emanating from the market environment and not directly from the authoritative organizations. These benefits may include new customers or more trust from existing customers due to the good reputation attained for good compliance. According to Delmas and Toffel (2004), there are several studies that suggest that an organization's adoption of certain management principles, coerced by regulatory authorities, is motivated by customer concerns. These customer concerns can be inferred as market influence. It can be further inferred that motivation to comply arises from the concern that the market stakeholder could lose its customers to more successful competitors if seen as non-compliant by their customers. As the results of the interviews suggest, market stakeholders are benefited by complying as it increases their clients' confidence in them and helps them to retain business relations. Further, institutional theory is complementary to economic theory (Carpenter & Feroz, 2001) and views organizations as functioning within a social framework portraying economic behaviour (Oliver, 1997). Government authorities grant rewards and recognition to those they think are legitimate institutions in the given market environment (DiMaggio & Powell, 1983). As such, there is pressure on market stakeholders to achieve this status, which they perceive as beneficial. This led to the formulation of the following hypothesis:

Hypothesis 4

The greater the market influence on an organization, the greater the benefits of compliance perceived by that organization.

7.4.5 Perceived Norms under Peer Pressure

Looking at peer pressure in other contexts, a study based in a social context found that fraternity students gave into heavy drinking due to pressure from their peers as they had perceived that it was the norm of the fraternity to have a reputation as a heavy drinker (Evans, Gilpin, Farkas, Shenassa, & Pierce, 1995). In a given social setting, the behaviour of the peers determines the prevailing norm (Lapinski & Rimal, 2005; Rimal & Real, 2005). In the organizational context, DiMaggio and Powell (1983) argue that professional training institutes are important centres for the development of organizational norms. As indicated before, the personnel interviewed

for this study were boundary-spanning personnel who are customs brokers and had been certified as such by training institutes. These institutes emphasise the prevailing heightened security status and the importance of complying with the information security compliance security requirements. Therefore, from the argument made by DiMaggio and Powell (1983) it can be inferred that complying with information security requirements would be the perceived norm among market stakeholders.

When there is continuous direct and indirect persuasion from colleagues and other stakeholders within the industry regarding compliance behaviour, the boundary-spanning personnel may perceive this as the norm of the industry. Almost all of the participants interviewed during the first phase of the study were members of the CBAFF and indicated that all of their peers complied with the information security requirements. As argued before, these boundary-spanning personnel represent their respective organizations and have the power to influence the behaviour of their organizations according to their perceptions in order to survive in their operational environment. This led to the formulation of the following hypothesis:

Hypothesis 5

The greater the peer pressure on an organization, the greater the perception that information security is a norm.

7.4.6 Perceived Benefits under Peer Pressure

Peer pressure may be perceived as beneficial as it reduces research costs (Levitt & March, 1988). Further, in other contexts such as pro-environmental behaviour, the impact of peer pressure seems to create a stronger level of participation (Senbel, Ngo, & Blair, 2014) as it is perceived to be beneficial. Hence, it can be inferred that since information security requirements are enforced for the safety and the protection of the borders and its stakeholders, peer pressure may have the same beneficial effect. The findings from the interviews revealed that the participants kept a watchful eye over their peer competitors and adopted their successful and pre-tested ways of retaining the clients. They also believed that if a disaster occurred due to their negligence over security requirements it would destroy their livelihood through loss of customers. It can be inferred from their responses that mimicking the ever-changing behaviour of the peers towards the escalating security concerns is beneficial for their businesses. This is what DiMaggio and Powell (1983) call the advantageous economic benefits of mimetic behaviour. This led to the formulation of the following hypothesis:

Hypothesis 6

The greater the peer pressure on an organization, the greater the benefits of compliance perceived by that organization.

7.4.7 Perceived Benefits under Rules and Norms of Social Exchange

If the authoritative organization gives assurance of procedural fairness to market stakeholders, or if the market stakeholder is rewarded for compliance, this exchange relationship can be perceived as creating direct benefits for the market stakeholder. For instance, US Customs gives preferential treatment during customs inspection and expedition procedures to organizations that are compliant through the provision of reliable and verifiable security information (Bichou, 2004). This preferential treatment acts as a reward for the organization and the established procedures ensure fairness.

During the interviews, the participants expressed their displeasure over the inconsistent implementation of the security procedures by the authorities. For instance, the correction of an error transmitted to the authorities by the market stakeholder can take from a couple of minutes to several hours. Further, this varied with the officer on duty and depended on their familiarity with the stakeholder in question. However, there are standards set by the authorities on how to respond to complying stakeholders. The market stakeholders perceived inconsistencies and uncertainties in the so-called fair treatment by the authorities. It is therefore important to establish whether the authorities show fairness in their implementation of the procedures and if it is perceived as beneficial by the market stakeholders. Hence, taking guidance from Evan (1965), the inter-organizational relations could be identified from this social exchange viewpoint. While referring to Perrow (1974), DiMaggio and Powell (1983) state that individuals who occupy similar positions across a range of organizations possess a similarity of orientation and disposition that may alter organizational behaviour, as inter-personnel and inter-organizational relations are related although they are theoretically and empirically distinct (Zaheer, McEvily, & Perrone, 1998). This led to the formulation of the following hypothesis:

Hypothesis 7

The more fairly an organization is treated, the greater the benefits of compliance perceived by that organization.

Reciprocity implies actions that are contingent on rewarding reactions from others and can exist among equals (Keohane, 1986), such as between the authorities and market stakeholders. Keohane (1986) states that reciprocity clearly entails at least rough equivalence of benefits and Blau (1964) argues that beneficial treatments are more likely to reciprocated. On the same note, scholars believe that the value of reciprocity lies in the benefits exchanged, and that it is prominent in social exchange (Molm, Schaefer, & Collett, 2007).

During the interviews, there were many participants who questioned quick clearance times and other such procedures as reciprocity for compliance. Their argument was that these are functions of good management which should be forthcoming from the authorities until a party is caught for non-compliance. This could be similar to the deprivation-satiation proposition, which states that that the more often in the recent past a person has received a particular reward, the less valuable any further unit of that reward becomes (Narasimhan, et al., 2009). In this sense, there is uncertainty about whether the authority's implementation of reward scheme for compliance is actually considered as reciprocal and perceived as beneficial by the market stakeholders. The authorities' recognition of organizations through grants or contracts may give organizations legitimacy and visibility, which may be considered as rewards (DiMaggio & Powell, 1983). The findings of the interviews therefore suggest that the participants did not accept the existing reward scheme as reciprocal to the required behaviour. It can be argued that if they have a negative perspective of these reciprocal arrangements then they would not perceive these arrangements as beneficial. This led to the formulation of the following hypothesis:

Hypothesis 8

The greater the reciprocity from the authorities, the greater the benefits of compliance perceived by an organization.

7.4.8 Compliance under Perceived Threat

It is argued that the market stakeholder will do whatever it takes to be seen as compliant in order to avoid the threats of sanctions (Williams, et al., 2009), such as being eliminated from the supply chain (Bichou, 2004) or having their cargo held at customs for an indefinite time for processing (Banomyong, 2005). Edelman (1992) argues that compliance under coercion can be a symbolic gesture made to avoid penalties. This behaviour was clearly identifiable from the analysis of the interviews where some of the participants responded that their compliance

processes, if audited by the authorities, would fail, thereby suggesting symbolic behaviour. Some of the activities mentioned included the sharing of passwords among customs brokers and normal staff. This led to the formulation of the following hypothesis:

Hypothesis 9

The greater the threats perceived by an organization, the lower (or more symbolic) will be the compliance behaviour exhibited by that organization.

7.4.9 Compliance under Perceived Norm

Perceived norm is defined for this study as the extent of the belief of the market stakeholder that conforming to the information security requirements of the authoritative is a prevailing norm of conduct of market stakeholders. In the context of the supply chain, norms emerge when companies develop implementations, interact with other companies, and agree on industry standards (Burgemeestre, et al., 2014). Market stakeholders tend to exhibit a degree of tightness between them and are more oriented to conforming to the market rather than to legal obligations (Casey & Scott, 2011). As mentioned before, almost all of the participants that were interviewed in the qualitative phase were certified customs brokers or had undergone professional training relevant to the supply chain environment. Since the September 11, 2001, terrorist attacks on the United States almost all of the customs-broker training programs have strongly advocated SCS activities as the prevailing norm of the industry. Professional training institutes are important centres that set the norms in a given environment (DiMaggio & Powell, 1983). As such it can be inferred that market stakeholders who conform to the norm of the market environment in relation to security compliance and who have received training that dictates compliance as a norm will have a strong perception of security as a norm of the market and thus for the organization. If this is true, then it can be argued that the higher the perception that compliance is the norm, the more substantive the compliance behaviour exhibited will be. This led to the formulation of the following hypothesis:

Hypothesis 10

The greater the perception that information security is a norm of an organization, the higher (or more substantive) will be the compliance behaviour exhibited by that organization.

7.4.10 Compliance under Perceived Benefits

Perceived benefits are taken into consideration when an organization makes the decision to comply with information security requirements and decides the extent to which they will comply (Casey & Scott, 2011; Westphal & Zajac, 1994). The benefits achieved from complying should have an obvious positive effect (Rodríguez & Wilson, 2002). The perception of benefits is defined for this study as the market stakeholder's belief that by complying with the information security requirements of the authoritative organizations, the market stakeholder will benefit directly from the authoritative organizations through fairness and reward. Further, it is proposed that benefits perceived from institutional pressures such as market pressure (Sarathy, 2006) and peer pressure (Levitt & March, 1988) could prove beneficial for the reasons discussed above, such as customer retention. Bulgurcu et al., (2010) claim that when it is perceived that the compliance behavior is beneficial, the association with compliance behavior is positive. Hence, the study argues that the perception of benefits will lead to substantive compliance behaviour. The findings from the interviews revealed that some participants strongly felt that they would invest without hesitation in whichever activity that would be beneficial to their businesses. In this regard, most of the participants believed that if complying with information security requirements brings them economic benefits, they would most definitely comply by further investing in IT and training staff. This could be inferred as the willingness to comply substantively. This led to the formulation of the following hypothesis:

Hypothesis 11

The greater the benefits of compliance perceived by an organization, the higher (or more substantive) will be the compliance behaviour exhibited by that organization.

Table 14: List of hypotheses

	Perceived Threat under Regulatory Demands
H1	The greater the regulatory demands on an organization, the greater the threat perceived by that organization.
	Perceived Norms under Regulatory Demands
H2	The lower the regulatory demands, the greater the perception that information security is a norm.
	Perceived Norms under Market Influence
H3	The greater the market influence on an organization, the greater the perception that information security is a norm of that organization.
	Perceived Benefits under Market Influence
H4	The greater the market influence on an organization, the greater the benefits of compliance perceived by that organization.

	Perceived Norms under Peer Pressure
H5	The greater the peer pressure on an organization, the greater the perception that information security is a norm.
	Perceived Benefits under Peer Pressure
H6	The greater the peer pressure on an organization, the greater the benefits of compliance perceived by that organization.
	Perceived Benefits under Rules and Norms of Social Exchange
H7	The more fairly an organization is treated, the greater the benefits of compliance perceived by that organization.
H8	The greater the reciprocity from the authorities, the greater the benefits of compliance perceived by an organization.
	Compliance under Perceived Threat
H9	The greater the threats perceived by an organization, the lower (or more symbolic) will be the compliance behaviour exhibited by that organization.
	Compliance under Perceived Norm
H10	The greater the perception that information security is a norm of an organization, the higher (or more substantive) will be the compliance behaviour exhibited by that organization.
	Compliance under Perceived Benefits
H11	The greater the benefits of compliance perceived by an organization, the higher (or more substantive) will be the compliance behaviour exhibited by that organization.

7.5 Summary

Chapter 4 presented a conceptual model formulated from the findings of the literature. Chapter 6 verified that model and its components for relevance and validity. This verification was conducted through a qualitative inquiry. Based on these verifications, this chapter has developed the conceptual model into a research model in order to conduct a quantitative survey. In addition, the constructs used to operationalize the quantitative survey that were obtained from the literature and relevant theories were defined and discussed. Finally, the relationships identified in the research model were developed into the 11 hypotheses presented in Table 14.

.

CHAPTER 8: PHASE 2 – QUANTITATIVE SURVEY AND ANALYSIS

8.1 Chapter Overview

Chapter 5 gave a detailed account of Phase 1 of this research, which was the qualitative study including its analysis and findings. This chapter provides details of Phase 2 of the research, the quantitative phase, including the measures used, the data collection process, the analysis conducted using partial least square structural equation modelling (PLS-SEM), how verifications and validations were achieved, and the findings from the survey.

8.2 Measures

The use of validated and tested questions will improve the reliability of the results (Boudreau, Gefen, & Straub, 2001; Straub, 1989). All of the questions relating to the constructs were adopted from previous studies, as shown in Table 15.

The quantitative survey was conducted using a self-administered questionnaire with pre-existing scales that were operationalized and peer-reviewed. These items were reworded to fit the research context and measured using a 7-point Likert-type scale. As shown in Table 15, after validity testing some of the items had to be dropped before arriving at the final number of items used in the analysis. The survey instrument is appended in Appendix B as Table 26.

Table 15: The number of items for each constructs used in the in survey and analysis

	Construct	**No of items used in the survey**	**No of items used in the analysis (after validation)**	**Adopted from**
1	Regulatory demands (reverse coded)	4	3	(Liang, et al., 2007)
2	Market influence	3	3	(Liang, et al., 2007)
3	Peer pressure	4	4	(Liang, et al., 2007)
4	Fairness	11	3	(Lamertz, 2002)
5	Reciprocity (Reward)	3	3	(Maloni & Benton, 2000)
6	Perceived threats (reverse coded)	2	2	(Scheepers, Gijsberts, & Coenders, 2002)
7	Perceived norms	2	2	(Morris & Venkatesh, 2000)
8	Perceived benefits	3	3	(Lind & Van den Bos, 2002)
9	Compliance behaviour (one item reverse coded)	3	3	(Christmann & Taylor, 2006)

8.3 Sample Selection

A list of 165 companies, including shippers, customs brokers and freight forwarders taken from the CBAFF and other business directories was compiled. These companies were contacted by phone, and email addresses of the people that could be identified as boundary personnel were sought. The 165 phone calls took 14 days. While some companies needed an explanation before they parted with information, others were more than willing. The respondents from some companies needed to consult with their superiors before they parted with information. A few made a return call with the information or emailed it after consultation. A follow-up call was made to the companies that did call back. If the company was willing to give more than one email addresses, they were requested to email a list. This exercise resulted in 320 email addresses of potential participants.

8.4 Sample Size

In order to calculate the sample size needed for the survey, a power analysis calculation was performed (Lerman, 1996). This is what is called a priori power analysis where sample size N is computed as a fraction of the required power level (1-β) with a pre-specified significance level α and the population effect size to be detected with probability (1-β) (Faul, Erdfelder, Lang, & Buchner, 2007). Where (1-β) is the compliment of β the Type II error or beta error probability of falsely retaining an incorrect H0 (Faul, et al., 2007). To estimate an effect size Cohen (1992) suggests 02, 0.5 and 0.8 as small, medium and large effect size respectively. For this study the significance level is set at 95% and the required power is set at 99% with a Cohen's small effect size of 0.2. With these values the analysis results in a sample size of N = 94. The analysis was conducted using a software called G*Power V3.1.9.2.

8.5 Pilot Study

Qualtrics is a free web surveying tool, where the survey instrument can be hosted for public access. The internet link to the quantitative survey hosted on Qualtrics was mailed to 10 supply chain stakeholder companies in Hamilton explaining the aim of the pilot test for improving the questionnaire. The absence of any suggestions or comments on the questionnaire by any of the participants was indicative that the questionnaire was usable and potentially viable for data analysis. Therefore, no changes to the instrument were done as a result of the pilot study. The

same process was followed by Yang and Wei (2013) to test the viability of the quantitative survey instrument in their SCS study SCS.

8.6 The Survey

Potential participants were contacted by email within a period of five days. A link to the Qualtrics web survey with a cover letter vetted by the AUT Ethics Committee was sent to each of the 320 potential participants. By the end of the first week after the emails were dispatched, there were 42 respondents. A second round of phone calls was made 10 days after the email link was sent. In some cases the researcher conversed with a receptionist or the senior managers of the companies, not directly with the potential participants. In these cases, they were requested to remind their colleagues to respond to the request made. Where direct contact was made, they were politely asked if they had responded or if they were willing to respond. All of them showed their willingness to participate, while some already had completed the survey. According to some of them, the email had gone to the junk folder as spam mail. At this point it was decided that making calls would be more effective. Though on occasion there was direct contact with participants, their anonymity was assured as their responses to the survey instrument were recorded online and did not require any specific details which may breach their anonymity. Within three months, 250 calls were made resulting in 163 additional responses.

The exercise resulted in a total of 205 participants from 71 companies from the North Island of New Zealand, which represented a 64% response rate of the sample selected. Wellington and Auckland contributed more than 80% of the participants. Table 16 summarizes the type of companies that participated in the survey. Figure 22 and Figure 23 show the age groups and number of years' experience of the participants. This information is important as GSCS initiatives came into effect after the September 11, 2001, terrorist attacks on the United States and these figures will reflect their awareness and knowledge of the events that followed.

Table 16: Types of companies that participated in the survey

	Type of company	**No of participants**
1	Customs Broker	70
2	International Trader with In-house Customs Broker	6
3	Customs Broker and Logistics Operator	4
4	Freight Forwarder and Logistics Operator	7
5	International Trader	55

	Type of company	No of participants
6	International Trader and Freight Forwarder	22
7	Logistics Operator	41

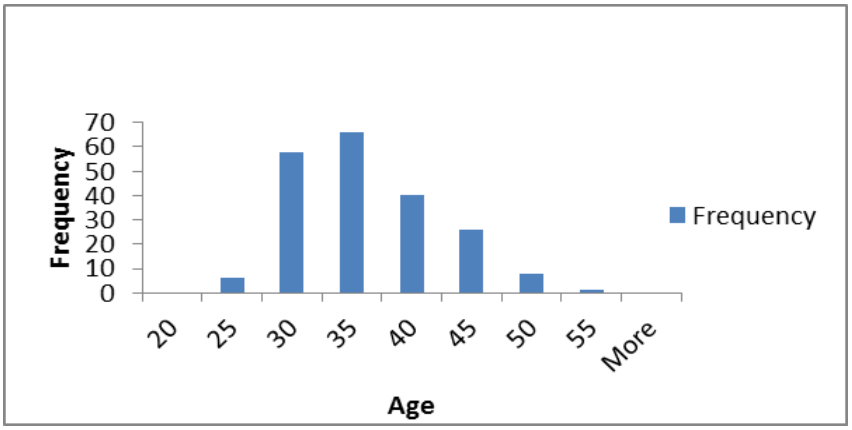

Figure 22: The age group of the survey participants

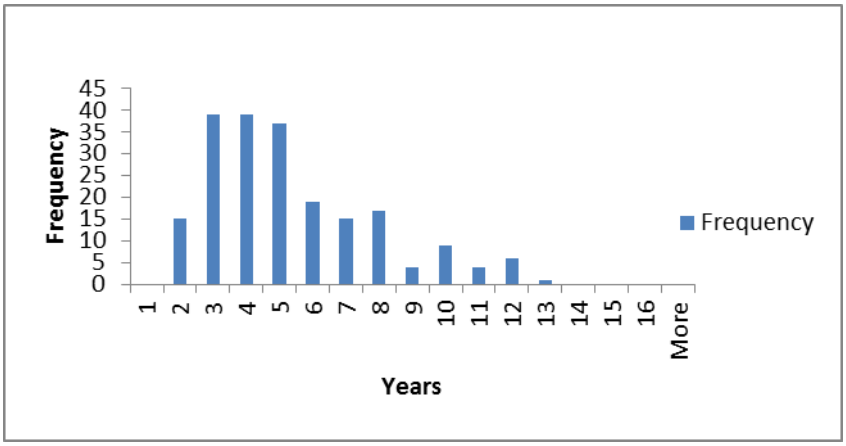

Figure 23: Years of experience of the participants in the field

The average age group of the participants was 35 years and this means when the September 11 attacks occurred most of the participants would have been around the age of 24. Therefore, it can be safely assumed they had knowledge of the extent of this attack and could relate this incident to the prevailing stringent security measures introduced by the GSCS initiatives. This assumption is based on the fact that this was a major event that received global attention and had major consequences on global travel and cargo movements. The chart in Figure 24 indicates that the average experience of the survey participants in the field was four years, with a minimum of two years in the cross-border supply chain environment. This amount of experience is once again assumed sufficient for them to have knowledge of and exposure to the current security environment. Referring to Table 16, it can be observed that more than 40% of the participants were customs brokers. To be a customs broker operating in New Zealand they

would have to be certified by the New Zealand Customs Service and to get this certification they had to undergo a training program concluded by an examination. This again reinforces the fact that the participants would have the relevant knowledge to inform the line of enquiry pursued by this study.

8.7 Quantitative Analysis and Findings

Quantitative data analysis is focused on measurement validation and hypothesis testing. Validation efforts assess the absence of common method bias (CMB) and the reliability and validity of the measures (Straub, 1989), while hypothesis testing analyses the proposed hypotheses. CMB was assessed in this study using Harman's single factor test, which is one of the most widely used techniques to address CMB (Podsakoff, et al., 2003) and the validity tests were done using PLS-SEM.

SEM is a second-generation multivariate data method that can test theoretically supported linear and additive causal models (Haenlein & Kaplan, 2004). There are two sub models in SEM (see Figure 25): the inner model specifies the relationships between the independent and dependent latent variables, whereas the outer model specifies the relationship between the latent variables and their observed indicators (Hsu, Chen, & Hsieh, 2006). In SEM, a variable is either exogenous or endogenous and the technique provides the flexibility to simultaneously construct the relations among multiple endogenous and exogenous latent variables (LVs) and the relations between LVs and manifest variables (MVs) (Hsu, et al., 2006).

There are two types of SEM techniques: covariance-based and component-based (Gefen, Straub, & Boudreau, 2000). PLS path modelling, also known as PLS-SEM, is a component-based technique aimed at maximizing the explained variance of the dependent latent constructs (Hair, et al., 2011). The primary goal is to maximize explained variance in the dependent constructs but additionally to evaluate the data quality on the basis of the measurement model characteristics (Hair, et al., 2011).

SEM excels at prediction and almost all model estimations use the coefficient of determination, R^2 values, to characterize the ability of the model to explain and predict the endogenous latent variables (Ringle, Sarstedt, & Straub, 2012). It is also argued that SEM provides more rigorous testing of construct reliability, convergent validity and discriminant validity (Jarvis, MacKenzie, & Podsakoff, 2003). This is due to the fact that validity and reliability assessment is an integral part of SEM (Hewstone, Rubin, & Willis, 2002). Further, SEM-based approach

provides the researcher with the flexibility to (a) model relationships among multiple predictor and criterion variables, (b) construct unobservable LVs, (c) model errors in measurements for observed variables, and (d) statistically test a priori substantive/theoretical and measurement assumptions against empirical data (i.e. confirmatory analysis) (Chin, 1998a).

Finally, evaluation of SEM using the PLS method demands significantly fewer requirements compared to that of the covariance structure analyses, but nevertheless delivers consistent estimation results (Hoffmann & Trautmann, 2006). SEM lacks the well-identified global optimization criterion, so that there is no global fitting function to assess the goodness of the model, but it is a variance-based model strongly oriented to prediction and focuses on the model's predictive capability rather than the statistical accuracy of the estimates. The statistical significance of the path coefficients can be achieved by a non-parametric goodness of fit (GoF) based validation procedure such as bootstrapping (Hoffmann & Trautmann, 2006). The PLS analysis in this research was conducted using SmartPLS version 2.0.M3.

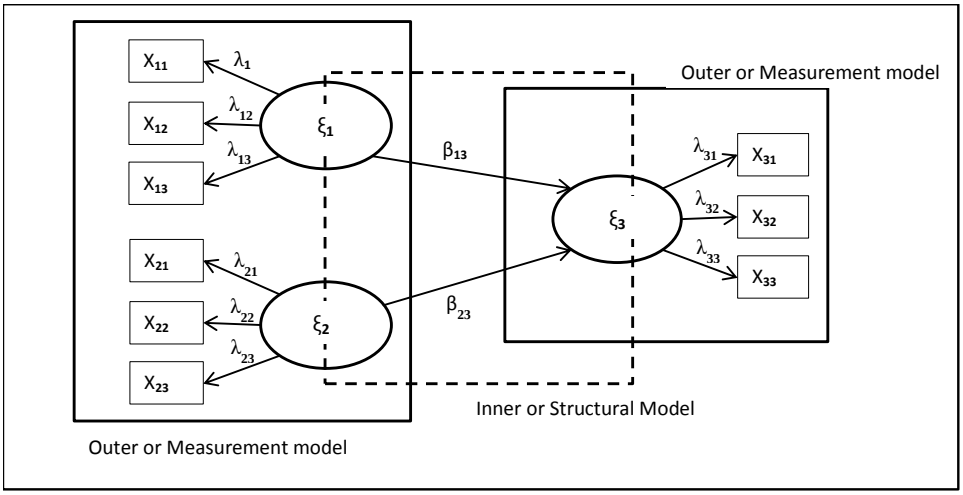

Figure 24: SEM representation

Figure 24 represents a skeleton representation of SEM. The ellipses represent the latent variables ξ (LVs) which are described by observed indicators X usually defined as manifest variables (MV). Arrows show causations among variables (either latent or manifest), and the direction of the arrow defines the direction of the relation. In this respect, the variables receiving the arrow are considered as endogenous variables in the specific relationship. When the variables inside the path model are latent variables whose measure is inferred by a set of observed indicators, the path analysis that follows is termed SEM. Each SEM model involves two levels of relationships: the first one takes into account the relations between the MVs and

the corresponding LV (measurement model); the latter considers the causal relations among the LVs (structural model).

The model used for this study, presented in Figure 25, contains the five exogenous variables and four endogenous variables, with the respective number of MVs describing these variables.

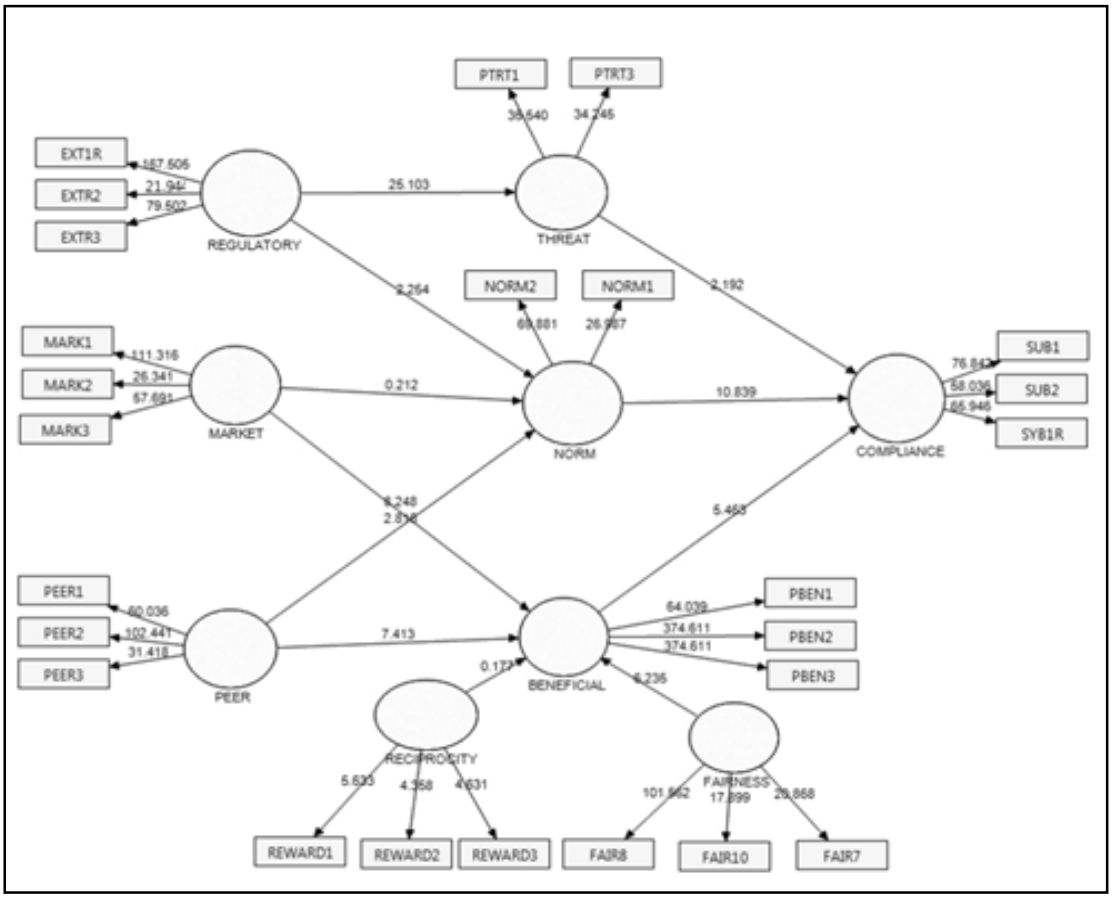

Figure 25: The SEM used for this study

Table 17: List of exogenous and endogenous variables

	Exogenous	No. of MVs	Endogenous	No. of MVs
1	REGULATORY	3	THREAT	2
2	MARKET	3	NORM	2
3	PEER	4	BENEFICIAL	3
4	FAIR	3	COMPLIANCE	3
5	RECIPROCITY	3		

8.7.1 Common Method Bias

CMB may arise from data collected through the same questionnaire during the same period, having a common rater, a common measurement context, a common item context, or from the

characteristics of items themselves (Podsakoff, et al., 2003). One of the most widely used techniques that has been applied by researchers to examine if a survey possesses such bias is the Harman's single factor test (Podsakoff, et al., 2003). This method of CMB detection has been used in many information security studies, such that by Morris and Venkatesh (2010)

The basis of this test is that if a substantial amount of common method variance is present either a) a single factor will emerge from the factor analysis, or b) one general factor will account for the majority of the covariance in the independent and criterion variables (Podsakoff & Organ, 1986). As shown in Table 18, the percentage of variance from the sum of squared loadings is 37.633, which is below 50%, meaning there is no concern about CMB. The full statistical analysis is given in Appendix C.

Table 18: Harman's single factor test results

Extraction sums of squared loadings		
Total	% of Variance	Cumulative %
12.795	37.633	37.633

8.7.2 Reliability and Validity of the Measures

All the items used in this study are adapted from well-cited studies, which have empirically validated these items. This is important as doing so contributes to the cultivation of the tradition of research (Malhotra & Grover, 1998). There are no hard and fast rules that guide the decision to choose the number of items to measure a construct (Hinkin, 1998). However, a single-item measure may cause a problem as it does not allow for an evaluation of internal consistency and reliability (Chen & Sun, 2003). Accordingly, all the constructs in this research are measured using two or more items. Items for perceived norm are adapted from a study by Venkatesh (2000), who uses two items. Items for perception of threat are adapted from a study by Scheepers et al. (2002), in which only two of the items used were relevant to the domain of this study. The literature suggests that when choosing items they should be appropriate to the domain (Malhotra & Grover, 1998). Due to the intrusive nature of this study and the hesitant behaviour of the respondents towards participation in an information security study, one of the decisions during the design of the survey was to keep the number of items to the minimum level, without affecting the statistical significance and outcome. Additional items also demand more time in the administration of a measure (Carmines & Zeller, 1979). Keeping the instrument short is an effective means of minimizing response biases from boredom or fatigue

(Schmitt & Stults, 1985), as well as decreasing the adverse effects of response rate (Chen & Sun, 2003). Although not used in this study, it is also important to note that SEM does permit the use of constructs represented by a single item (Gefen, et al., 2000), but it should have a known reliability and with little or no assumed measurement error (Hair Jr, Anderson, Tatham, & William, 1995).

There is no GoF criterion for PLS path modelling (Henseler, Ringle, & Sinkovics, 2009). Although a global GoF criterion has been proposed for PLS path modelling (Tenenhaus, Vinzi, Chatelin, & Lauro, 2005), it mainly serves a diagnostic purpose and not a formal testing one (Wetzels, et al., 2009). As such, a list of processes outlined by Chin (1998b) caters for the assessment of the partial model structure. These processes are applied systematically in two steps which are (1) assessment of the outer model and (2) assessment of the inner model (Henseler, et al., 2009). The properties of interest that encompass these steps are reliability (convergent validity), average variance extracted (AVE) and discriminant validity for each unobserved variable (Fornell & Larcker, 1981). In this research, the following tests were performed:

1. Indicator reliability and internal consistency
2. Convergent validity
3. Discriminant validity
4. Predictive relevance

8.7.2.1 Indicator Reliability and Internal Consistency

The indicator reliability of the different scales is measured using the Cronbach's alpha method, where alpha values greater than or equal to 0.70 are an indication of internal consistency and the discriminant validity of the scales (Morris & Venkatesh, 2010). Table 19 shows the reliability measures having Cronbach's alphas equal to or greater than 0.70.

Hulland (1999) suggests the use of the square of outer loadings to examine the indicator reliability and generally the value should be 0.7 or higher but if the research is exploratory, 0.4 and higher is acceptable. The results of this test (included in Appendix D) show that all the values are equal to or above 0.7 at one decimal place.

For internal consistency and reliability, researchers recommend the use of composite reliability as a measure of internal consistency and reliability and it is further suggested that the values should be 0.7 or higher but 0.6 and higher could be acceptable if it is an exploratory research

(Bagozzi & Yi, 1988; Hair, et al., 2011). Table 19 shows the composite values were well above 0.7. Hence, it can be concluded the indicators are reliable and internally consistent.

8.7.2.2 Convergent Validity

Construct validity pertains to the degree of correspondence between constructs and their measures and is a necessary condition for theory development and testing (Jarvis, et al., 2003). Hence, convergence measurement should be applied before performing causal analysis as it represents a condition that must be satisfied as a matter of logical necessity (Bagozzi, 1981). To test the convergent validity, AVE numbers are used and according to Bagozzi & Yi (1988), the AVE values should be 0.5 or higher. Table 19 shows that the AVE values were well above 0.5 and thus convergent validity is ensured for the research model measurement.

Table 19: Results showing indicator reliability, internal consistency, and convergent validity (n=205)

	AVE	Composite reliability	R^2	Cronbach's alpha	Communality	Redundancy
REGULATORY	0.8215	0.932	0	0.8901	0.8215	0
MARKET	0.7679	0.9083	0	0.8486	0.7679	0
PEER	0.8486	0.9438	0	0.9105	0.8486	0
FAIR	0.6544	0.8497	0	0.7564	0.6544	0
RECIPROCITY	0.7672	0.9079	0	0.8487	0.7672	0
THREAT	0.7156	0.8342	0.6005	0.6037	0.7156	0.4311
NORM	0.728	0.8424	0.433	0.6893	0.728	0.0315
BENEFICIAL	0.9354	0.9775	0.919	0.9651	0.9354	0.2512
COMPLIANCE	0.833	0.9373	0.7864	0.9008	0.833	0.3617

8.7.2.3 Discriminant Validity

Discriminant validity is defined as the dissimilarity in a measurement of different constructs (Götz, et al., 2010). Götz et al., (2010) further argue that, in addition to considering the indicator and construct reliability, a thorough validation procedure requires the evaluation of a measurement (or structural) model's discriminant validity.

Let R_{xx}, R_{yy} and R_{xy} refer to the correlation matrix of x variables, y variables, and xy variables where x and y are observed variables of different constructs. Then for the observed data to have significant theory, all R_{xy} correlations should be statistically significant (Fornell & Larcker, 1981). The term discriminant validity refers to this relationship of the off-diagonal terms R_{xx}, R_{yy} and R_{xy}, and is exhibited only if all the correlations in R_{xx} and R_{yy} (measurement) are

significant and each of these correlations is larger than all correlations in R_{xy} (Fornell & Larcker, 1981).

In SmartPLS this is done by testing if the square root of AVE for each latent variable is greater than the correlations among the latent variables (Wong, 2013). Table 20 shows all the square roots of each AVE (bold values in diagonal) are greater than the correlations among the latent variables, hence proving discriminant validity.

Table 20: Square root of AVE for each latent variable showing discriminant validity (n=205)

	BENEFICIAL	FAIR	MARKET	NORM	PEER	RECIPROCITY	REGULATORY	COMPLIANCE	THREAT
BENEFICIAL	**0.9672**								
FAIR	0.8206	**0.8089**							
MARKET	0.9223	0.7760	**0.8763**						
NORM	0.7227	0.7724	0.6876	**0.8532**					
PEER	0.9124	0.7433	0.8579	0.6691	**0.9212**				
RECIPROCITY	0.0918	0.1061	0.0938	0.1209	0.0681	**0.8759**			
REGULATORY	0.9463	0.7941	0.9526	0.6827	0.8680	0.0802	**0.9064**		
COMPLIANCE	0.8149	0.6459	0.6783	0.8254	0.7073	0.1288	0.7067	**0.9127**	
THREAT	0.8338	0.6848	0.7547	0.6404	0.7418	0.0642	0.7749	0.7379	**0.8459**

8.7.2.4 Predictive Relevance

The Stone-Geisser test for predictive relevance states than Q^2 values greater than 0 indicate that the exogenous constructs have predictive relevance for the endogenous construct under consideration (Hair, et al., 2011). Q^2 can be tested using a procedure called blindfolding in SmartPLS. The results in Table 21 show that all the Q^2 values were greater than 0, hence all the exogenous constructs under consideration have predictive relevance.

Table 21: Predictive relevance of the endogenous constructs

Total	SSO	SSE	Q^2
BENEFICIAL	84.0288	8.7958	0.8953
NORM	64.9427	20.5685	0.6833
COMPLIANCE	83.1478	13.1705	0.8416
THREAT	61.7443	15.1841	0.7541

$Q^2 = 1 - \frac{SSE}{SSO}$ where SSO is the sum of squares error using the mean for prediction and SSE is the sum of squares of prediction error (Akter, D'Ambra, & Ray, 2011).

8.8 Endogenous Variables and the Outer and Inner Model

PLS path models are defined by two sets of linear equations: the inner model and the outer model (Henseler, et al., 2009). The inner model, which is referred to as the structural model,

specifies the relationships between LVs (Tenenhaus, et al., 2005). As such, the inner model constitutes a causal chain system with uncorrelated residuals and without correlations between the residual term of a certain endogenous latent variable (see Table 17) and its explanatory variables (Henseler, et al., 2009). The outer model, which is referred to as the measurement model, is the sub model in SEM that specifies the indicators for each construct and assesses the reliability of each construct for estimating the causal relationship (Gefen, et al., 2000).

8.8.1 Explanation of Target Endogenous Variable Variance

The coefficient of determination, R^2, presented in Table 19, is defined as the proportion of variance which measures the success of predicting the dependent variable from the independent variables of the model (Nagelkerke, 1991). The R^2 values 0.75, 0.50 and 0.25 for endogenous LVs in structural models respectively explain substantially, moderately and poorly (Hair, et al., 2011). Table 22 explains the significance of the R^2 for the endogenous LVs.

Table 22: The coefficient of determination (R^2) for the endogenous LVs

Endogenous LVs	**R^2**	**Explanation**
THREAT	0.6005	THREAT is explained by REGULATORY demands. Results show that this exogenous variable describes THREAT moderately with 60% of the variance.
BENEFICIAL	0.919	BENEFICIAL is explained by PEER, MARKET, FAIR and RECIPROCITY. Results show that these four exogenous variables describes BENEFICAL substantially with 92% of the variance.
NORM	0.433	NORM is explained by REGULATORY, MARKET, and PEER. Results show that these three exogenous variables moderately describe NORM with 43% of the variance.
COMPLIANCE	0.7864	COMPLIANCE is explained by THREAT, NORM and BENEFICIAL. Results show that these three exogenous variables describe COMPLIANCE substantially with 79% of the variance.

8.8.2 Structural Path Significance of the Outer Model

SmartPLS generates *t*-statistics for significance testing for the outer model and uses a procedure called bootstrapping. This technique, using 5000 simulated samples generated for 205 real samples, was used to assess the significance of the path models. Critical *t*-values for a two-tailed tests are 1.65 (10% confidence interval), 1.96 (5% confidence interval) and 2.58 (1% confidence interval) (Hair, et al., 2011).

The *t*-statistics for the outer model are presented in Table 23 and the results show that all of the outer model loadings were well above 1.96 and therefore significant.

Table 23: Outer loadings

	Original sample (O)	Sample mean (M)	Standard deviation (STDEV)	Standard error (STERR)	t-statistics (|O/STERR|)
EXT1R <- REGULATORY	0.9638	0.9641	0.0058	0.0058	167.3098
EXTR2 <- REGULATORY	0.8652	0.7981	0.0358	0.0358	22.3204
EXTR3 <- REGULATORY	0.9462	0.9463	0.0119	0.0119	79.4983
FAIR10 <- FAIR	0.7495	0.746	0.0427	0.0427	17.5723
FAIR7 <- FAIR	0.7908	0.7885	0.0374	0.0374	21.1542
FAIR8 <- FAIR	0.881	0.8826	0.0087	0.0087	100.9879
MARK1 <- MARKET	0.914	0.9142	0.0082	0.0082	112.0272
MARK2 <- MARKET	0.8602	0.819	0.032	0.032	25.6454
MARK3 <- MARKET	0.892	0.8918	0.0154	0.0154	58.0374
NORM1 <- NORM	0.8224	0.8201	0.0311	0.0311	26.46
NORM2 <- NORM	0.883	0.8836	0.0127	0.0127	69.7339
PBEN1 <- BENEFICIAL	0.9304	0.93	0.0145	0.0145	63.992
PBEN2 <- BENEFICIAL	0.9851	0.9851	0.0026	0.0026	374.7063
PBEN3 <- BENEFICIAL	0.9851	0.9851	0.0026	0.0026	374.7063
PEER1 <- PEER	0.937	0.9378	0.0153	0.0153	61.2612
PEER2 <- PEER	0.9546	0.955	0.0092	0.0092	103.8477
PEER3 <- PEER	0.8698	0.8687	0.0274	0.0274	31.7576
PTRT1 <- THREAT	0.8645	0.8637	0.0247	0.0247	34.9787
PTRT2 <- THREAT	0.8269	0.8268	0.0237	0.0237	34.9212
REWARD1 <- RECIPROCITY	0.9391	0.8741	0.1708	0.1708	5.4975
REWARD2 <- RECIPROCITY	0.8324	0.7806	0.1926	0.1926	4.3225
REWARD3 <- RECIPROCITY	0.8527	0.7994	0.183	0.183	4.6605
SUB1 <- COMPLIANCE	0.9426	0.9417	0.0124	0.0124	76.3161
SUB2 <- COMPLIANCE	0.8785	0.8792	0.0154	0.0154	57.0242
SYB1R <- COMPLIANCE	0.9158	0.9145	0.0141	0.0141	64.9809

8.8.3 Structural Path Significance of the Inner Model

The *t*-statistics of the structural path coefficients with descriptive statistics are given in Table 24 and the results show the significance of the hypotheses of the inner model using the *t*-statistics values. The *t*-statistics show that out of the 11 hypotheses, only two hypotheses (H3 and H11) were insignificant at a 95% confidence interval. This analysis was carried out using the bootstrapping process with 5000 cases and 205 samples.

Table 24: *t*-statistics for the inner model (*p<0.05, **p<0.01, *** p<0.001)

	Hypotheses	Original Sample (O)	Sample Mean (M)	Standard Deviation (STDEV)	Standard Error (STERR)	T Statistics (|O/STERR|)
REGULATORY -> THREAT	H1	0.7749	0.7760	0.0308	0.0308	***25.1836
REGULATORY -> NORM	H2	0.3574	0.3536	0.1635	0.1635	*2.1862
MARKET -> NORM	H3	0.0360	0.0422	0.1768	0.1768	0.2038
MARKET -> BENEFICIAL	H4	0.4315	0.4284	0.0521	0.0521	***8.2777
PEER -> NORM	H5	0.2880	0.2862	0.1056	0.1056	**2.7267
PEER -> BENEFICIAL	H6	0.4049	0.4094	0.0545	0.0545	***7.4258
FAIR -> BENEFICIAL	H7	0.1844	0.1827	0.0293	0.0293	***6.2906
RECIPROCITY -> BENEFICIAL	H8	0.0041	0.0066	0.0228	0.0228	0.1821
THREAT -> COMPLIANCE	H9	0.1315	0.1363	0.0616	0.0616	*2.1342
NORM -> COMPLIANCE	H10	0.4847	0.4810	0.0449	0.0449	***10.7884
BENEFICIAL ->COMPLIANCE	H11	0.3549	0.3536	0.0665	0.0665	***5.3366

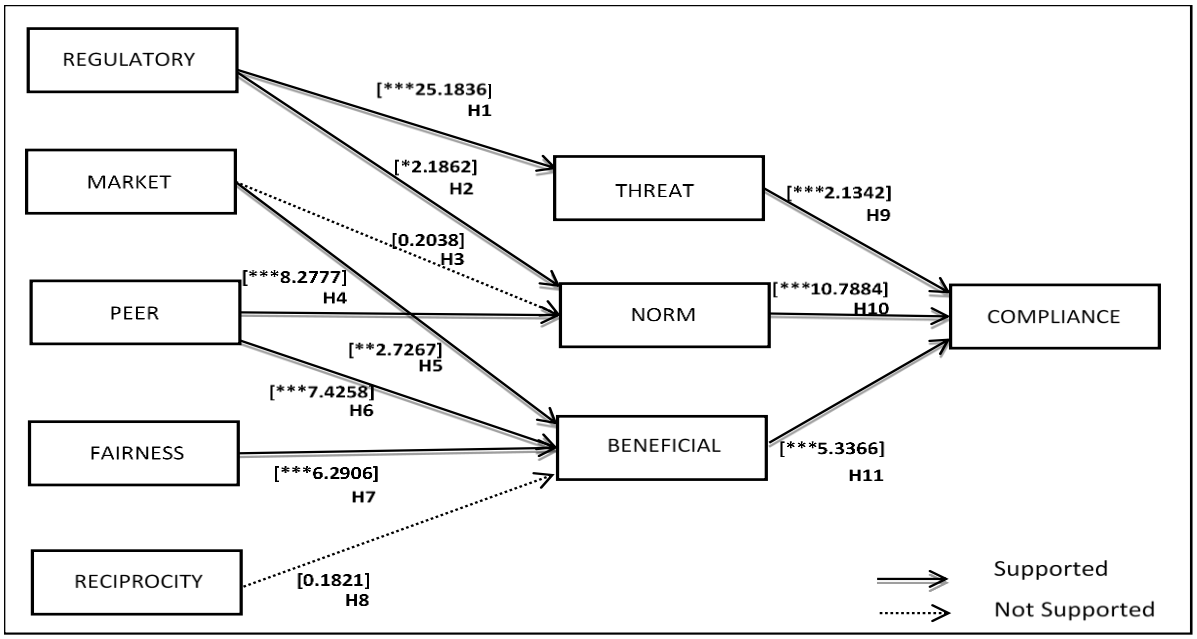

Figure 26: Simulation model with *t*-statistics (*p<0.05, **p<0.01, ***p<0.001)

8.9 Summary

This chapter provided the details of the quantitative study and the results of the data analysis. The analysis was done using PLS-SEM. Harman's single factor test was carried out to see if CMB was a factor Podsakoff, (2003); it was not. This was followed by tests for the reliability and validity of the measures. In this regard, a total of seven tests were performed, the results of which are summarized in Table 25. The next chapter discusses the research findings.

Table 25: Summary of reliability and validity tests

	Test	**Method**	**Result**
1	Indicator reliability and internal consistency	Cronbach's alpha	All variables are > 0.7 proving internal reliability and internal consistency. (Table 18)
2	Convergent validity	AVE	All AVE > 0.5 proving the degree of correspondence between constructs and their measures as acceptable hence proving convergent validity (Table 18)
3	Discriminant validity	Square root of AVE	Square root of AVE for each latent variable is greater than the correlations among the latent variables proving discriminant validity. (Table 19)
4	Predictive relevance	Q^2 test	Q2 test shows all exogenous have Q2 > 0 indicating predictive relevance (Table 20)
5	Target endogenous variable variance	R^2 test	All exogenous variables have reasonable ability to explain the endogenous latent variables (Table 21)
6	Structural path significance of the outer model	Outer model loadings	All outer model loadings are significant at 1.96 (5% confidence interval) (Table 22)
7	Structural path significance of the inner model	Inner model loadings (test hypotheses)	Nine out of 11 hypotheses are significant at 95% confidence interval. (Table 23)

CHAPTER 9: DISCUSSION

9.1 Chapter Overview

This chapter provides a detailed discussion of the key research findings presented in Chapter 8. This discussion is focused on answering the two research questions and is based on the individual predictive and explanatory power of the elements that directly and indirectly influence compliance behaviour. These elements were identified from the literature and then verified for their relevance to the given context through a series of qualitative interviews, as presented in Chapter 6. Chapter 5 argued that this method of verifying the constructs before a quantitative study is becoming quite common in information system studies. In this sense, the whole process of verifying the constructs before the development of the survey instrument makes this study a sequential mixed method with an emphasis on quantitative survey. Therefore, while discussing the findings of the quantitative survey in this chapter, no attempt is made to triangulate the findings of the qualitative phase. However, references are made to the arguments made during the verifications to emphasise the relevance of the findings to the context.

9.2 Research Aim and the Research Questions

As presented in Chapter 4, the aim of this research is to investigate and explain information security compliance behaviour (ISCB) in the context of SCS, emanating from the GSCS initiatives. To achieve this aim, the following research questions were asked:

The overarching research question:

How do the supply chain security stakeholders comply with information security requirements mandated by the GSCS initiatives?

Sub research questions

[RQ1] What are the drivers of ISCB and how do they impact the compliance behaviour exhibited by the stakeholders?

[RQ2] What factors influence inter-organizational ISCB in the context of the GSCS initiatives?

Figure 27 shows the research model used to seek answers to the above research questions and which of the 11 research hypotheses developed were supported. The model shows the β values

and R^2 values from the analysis. The β values represent the coefficient of the structural path that explains the strength of the path, while the R^2 values represent the explanatory power of the endogenous variables. In the following sub-sections, the discussion of the findings is geared towards answering the above two research questions. In the discussion, these β values and R^2 values alongside with t-statistics are used to explain the significance of the endogenous variables or the three drivers in driving compliance behaviour, as well as how the exogenous variables or the influencing elements impact the drivers of compliance behaviour.

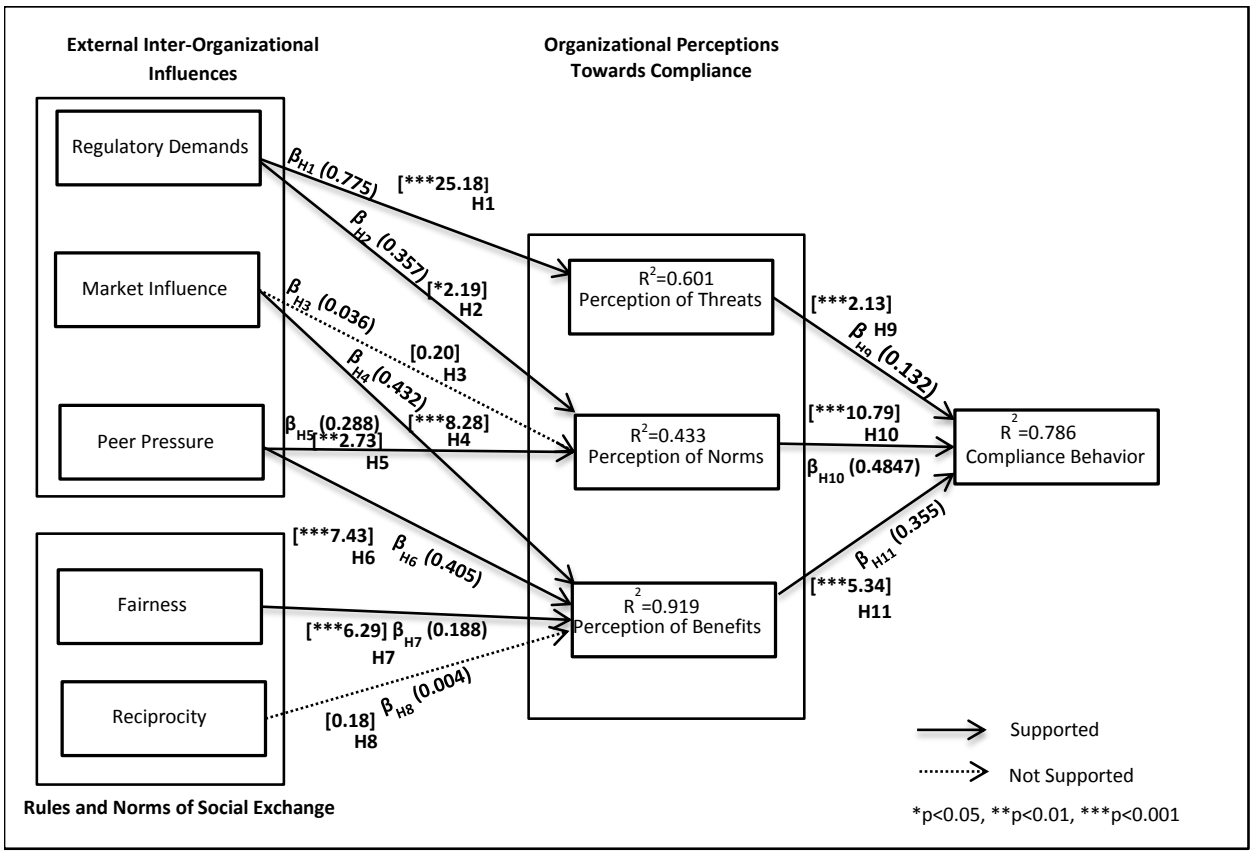

Figure 27: The research model

9.3 Overarching Research Question

How do the supply chain security stakeholders comply with information security requirements mandated by the GSCS initiatives?

The literature identifies two main types of compliance behaviour, namely symbolic compliance behaviour and substantive compliance behaviour (Day & Woodward, 2004). This study shows that ISCB exhibited by the market stakeholders does shift between these two forms of compliance behaviours. Based on the way compliance behaviour is measured for this research, using the operationalization of this construct from Christmann and Taylor (2006), responses showing lower levels of compliance behaviour are indicative of symbolic compliance behaviour and responses showing higher levels of compliance behaviour are indicative of substantive compliance behaviour. The findings show that from the 205 respondents 63% portray substantive compliance behaviour while the other 37% portray symbolic compliance behaviour. In this respect, the findings of this study are in alignment with the literature, where stakeholders' attempts at exhibiting activities in a superfluous manner to gain approval is considered symbolic behaviour, while substantive behaviour is when stakeholders bring about material changes to gain approval (Christmann & Taylor, 2006; Day & Woodward, 2004; Edelman, 1992).

9.4 Research Question 1

[RQ1] What are the drivers of ISCB and how do they impact the compliance behaviour exhibited by the stakeholders?

The findings show that ISCB is driven by three organizational perceptions. They are the perception of threats, perception of norms, and perception of benefits. The high $R^2_{COMPLIANCE}$= 0.786 value of compliance behaviour with high structural path coefficients and significant *t*-values between the paths of these perceptions are indicative that these three organizational perceptions indeed drive compliance behaviour.

The findings of this study also suggest that the three organizational perceptions that drive the type of compliance behaviour exhibited are in turn influenced by factors from the prevailing environment. A discussion of how each of these organizational perceptions impacts compliance behaviour and how factors from the environment influence these organizational perceptions is provided in the next subsections.

9.4.1 Organizational Perceptions

9.4.1.1 Perception of Threats

It was revealed from the literature review that the prevailing heightened security environment poses regulatory threats from non-market stakeholders, such as the customs authorities, for non-compliance, such as delayed cargo clearances and lengthy cargo examinations (Banomyong, 2005; Sheu, et al., 2006). The research model was formulated to confirm if these regulatory threats created a higher level of organizational perception of threats, leading to lower compliance behaviour. The moderately explaining R^2_{THREAT}=0.6005 is indicative of the high explanatory power of the existing perception of high levels of threat in the prevailing supply chain environment. The findings further show that when perception of threats is high, organizations exhibit lower compliance behaviour, which is indicative of symbolic compliance behaviour (Christmann & Taylor, 2006). This is reflected by the significant relation between the perception of threats and compliance behaviour (β_{H9}=0.1315, t_{H9}=2.1342, p<0.001). This finding is supported by Stevens et al. (2005), who found that pressure to comply from non-market stakeholders, such as government agencies, leads to symbolic compliance behaviour. One reason for such behaviour is identified by Herath and Rao (2009), who argue that when the certainty of detection is low, there is a negative impact on compliance. Based on this argument, one plausible explanation could be that when organizations portray symbolic behaviour towards enforcement of compliance requirements from authoritative organizations, they might be under the impression that the chances of detection of their behaviour by the authorities are low. This impression of low detection can be explained by the fact that authorities have to do thorough continuous security audits in order to ascertain the compliance status of individual organizations, which are deemed to incur high costs to the authorities (El Kharbili, Stein, Markovic, & Pulvermüller, 2008). This type of capacity limitation by the state is one of the factors leading to lower levels of compliance (Downs, Rocke, & Barsoom, 1996). In such situations where security concerns are not strong enough, market stakeholders may not have sufficient motivation to invest in security (Lee, Palekar, et al., 2011). This perception of low detection by the market stakeholders is not without reason. Recently, in an exercise, investigators from the US Government Audit Office (GAO) successfully forged documents to import radioactive material through inland borders (Bakshi & Gans, 2010). The exercise was performed to establish the security rigor at US borders and revealed weaknesses in the monitoring process. If examples of symbolic behaviour and the identification of such behaviour by authorities, combined with negative consequences for not complying substantively, are not

publicized or if market stakeholders are not aware of such occurrences, then market stakeholders could continue to comply symbolically.

Certainty of detection is a significant factor (Herath & Rao, 2009a) and merely the threat of punishment is not a deterrent (D'Arcy, et al., 2009). In this regard, compliance is affected by the source's capacity to punish, intent as to the use of force, and the target's capacity to oppose or comply with the source's command (Luckenbill, 1982). If the source is perceived as capable of inflicting threatened punishment and as making punishment contingent on opposition, and if the target perceives itself as incapable of effective opposition and able to comply, the target will comply (Luckenbill, 1982). In fact, a technique based on fear appeals may prove to be ineffective if people view these messages as punishing and show antithetical behaviour in response (Arvey & Ivancevich, 1980), and the threat of sanctions for not complying is not a motivator for compliance behaviour (Pahnila, et al., 2007).

This study shows that in an inter-organizational context, the threat of sanctions from authorities leads to compliance, but the type of compliance behaviour portrayed by market stakeholders under such threat is symbolic compliance. Therefore, the overall effect of perception of threats on compliance behaviour is negative. The more regulatory demands exerted by the authorities, the more symbolic the compliance behaviour portrayed by market stakeholders. The more symbolic behaviour portrayed, the more unreliable the data will be for risk analysis activities such as detecting high risk cargo. It can therefore be concluded that when the regulatory demands are advocated under the local laws with respect to the GSCS initiatives, there is a significant level of perception of threats. This perception of threats arises due to the fact that if the market stakeholders do not fulfil the information security compliance requirements, they will not be able to move their cargo across national borders or have to face lengthy and costly physical cargo inspections. This could result not only in huge financial losses but also in losing existing customers. Hence, market stakeholders fulfil the information security compliance requirements, if albeit symbolically, because they perceive threatening behaviour from the authorities.

9.4.1.2 Perception of Norms

The analysis shows R^2_{NORMS}=0.433, indicating that the perception of norms is moderately described by the exogenous variables. The findings further show that when organizations perceive that the compliance requirements enforced by the authorities are due to the current heightened security environment, which has become the current norm of the industry, they tend

to be inclined towards higher compliance behaviour (β_{H10}=0.4874, t_{H10}=10.7884, p<0.001). Higher compliance is indicative of substantive behaviour (Christmann & Taylor, 2006), which suggests that higher perception of norms leads to substantive compliance behaviour. This is in agreement with the study by Siponen et al. (2014), who found that when there is normative belief towards the organizational security policies, the impact on compliance is positive. This is also in line with findings of Herath and Rao (2009a), who found that social influences such as normative beliefs have a significant impact on security behaviour. Further, the pressure to comply with norms is a good deterrent (Guo, Mu, & Susilo, 2011; Ifinedo, 2014) and can be seen as a deterrent of symbolic behaviour.

In the current study, the market stakeholders accepted the fact that the heightened security environment has become the norm of the industry worldwide. DiMaggio and Powell (1988) state that professional training institutes are important institutions that set environmental norms. Scott (1995) refers to these institutes and professional and trade associations as the organization field where the community of organizations partakes of a common meaning system whose participants interact more frequently, thereby imposing normative influences to the organization these participants belong to. The boundary-spanning personnel who participated in this research are certified customs brokers and would have attended a professional training institution for their certifications. Only registered customs brokers can submit information to the Customs through the electronic system. In order to get registered as a customs broker it is mandatory to do the broker training and pass the broker certification examination These customs-broker training programs highlight the current state of the cargo clearance procedures, identification of high risk cargo, and the use of the electronic information systems to submit information to the customs. Therefore, boundary-spanning personnel are more aware of the prevailing high risk environment and heightened security, and understand and appreciate that these are the GSCS norms of the industry. When it is perceived that information security compliance is the norm to ensure that the business of supply chain environment is conducted smoothly and securely, then compliance behaviour towards the information security compliance requirements is substantial. Hence, the findings show that perception of norms is a driver of substantive compliance behaviour.

9.4.1.3 Perception of Benefits

The findings show that organizations are also inclined towards substantive behaviour when they perceive that the outcome of their responses towards the requirements is beneficial

(β_{H11}=0.3549, t_{H11}=5.3366, p<0.001). This is in agreement with the findings of Bulgurcu et al. (2010), who showed that when the cost of non-compliance is higher and when the benefits for compliance are higher, the rational choice is to comply. The cost of non-compliance could be sanctions from market stakeholders (Christmann et al., 2006). As discussed in Chapter 7, Bulgurcu et al. (2010) define the perceived benefit of compliance as the overall expected favourable consequences to an organization for complying with the security requirements, and claim that when it is perceived that the compliance behaviour is beneficial, their association with compliance behaviour is positive. This positive compliance behaviour can be inferred as substantive compliance behaviour. When the high prevalence of a behaviour is accompanied by beliefs that the behaviour will result in significant benefits, people are more likely to engage in the behaviour (Rimal & Real, 2003). Further, drawing from literature on health, when there is belief that the recommendations would be beneficial and would reduce any perceived threats, then the chances of complying are higher (Fenton, Blyler, & Heinssen, 1997). In respect to these findings and their alignment with the literature, it can be inferred that the perception of benefits is indeed a driver of substantive compliance behaviour.

In light of the above findings, this research demonstrates that an organization can exhibit either symbolic or substantive compliance behaviour when complying with information security requirements demanded by GSCS initiatives, and that it is the perception of threats, perception of norms, and perception of benefits relating to compliance or non-compliance that influence the type of compliance exhibited. When organizations perceive threats due to non-compliance they are more likely to portray symbolic compliance. Conversely, the perception of compliance as a norm of the organisation and the perception of benefits from compliance are both more likely to lead to substantive compliance behaviour.

The findings of this research show that in the given context all of market stakeholders such as the traders, customs brokers and freight forwarders portray some level of compliance behaviour. This means that the market stakeholders all provided the necessary information to the authorities as required and within the required timeframe. However, as discussed, their compliance behaviour can be either symbolic or substantive. In general, and especially in the given context of the GSCS initiatives, symbolic behaviour is undesirable and substantive behaviour is desirable. The information that is demanded from the non-market stakeholders under the GSCS initiatives is used to detect and stop potential terrorist activities. Symbolic behaviour becomes undesirable in the given context because the data provided under such behaviour may not possess the integrity that is required by the authorities to accurately perform

such activities. In this sense, this research has brought to the forefront the behaviour of market stakeholders towards the compliance requirements of the GSCS initiatives and the conditions under which these behaviours are portrayed. This is an important finding that impacts on the achievement of the objectives of the GSCS initiatives and helps to identify keys aspects to drive substantive compliance that would help achieve the objectives of the GSCS initiatives. In this regard the authorities should find ways and means to lower the perception of threats and increase the perception of norms and perception of benefits to achieve the desired goal of substantive compliance behaviour.

9.5 Research Question 2

[RQ2] What factors influence inter-organizational ISCB in the context of the GSCS initiatives?

In answering RQ1 above, it was shown that organizational perceptions drive compliance behaviour. Organizational perceptions are in turn influenced by the factors of external inter-organizational influences and rules and norms of social exchange.

9.5.1 External Inter-Organizational Influences

External inter-organizational influences are made up of regulatory demands, market influence and peer pressure, which are all identified as factors from the prevailing environment that influence the drivers of compliance behaviour.

9.5.1.1 Regulatory Demands

The regulatory demands in this research are the GSCS initiatives compliance requirements that have become part of local laws, which have to be fulfilled in order to conduct cross-border trade. This findings show that these regulatory demands influence the perception of threats (β_{H1}=0.7749, t_{H1}=25.186, p<0.001) and the perception of norms (β_{H2}=0.3574, t_{H2}=2.1862, p<0.05). There is a positive relation between regulatory demands and perception of threats, which indicates that when regulatory demands are high, the organizations perceive greater threat of punishment through fines and delayed shipments, and even the threat of losing customers through non-compliance. This is in agreement with Bichou's (2004) argument that firms will perceive the threat of being eliminated from the supply chain if they did not comply with the regulatory demands made by the United States. This threat is real, as within the supply chain stakeholders seek partnership among organizations which are compliant with the prevailing security requirements and avoid organizations who are not compliant (Sheu, et al.,

2006). Autry and Bobbitt (2008) call these partnerships "security-related partnerships" and failure to form such partnership creates the threat of being eliminated from the supply chain (Sheu, et al., 2006). Hence, regulatory demands and their positive relationship with perception of threats is an important element influencing ISCB.

In the case of the relationship between perception of norms and regulatory demands, the findings show that the higher the regulatory demands, the lower the perception of norms. The structural path coefficient and *t*-statistics are indicative of the strength and the significance of this relation (β_{H2}=0.3574, t_{H2}=2.1862, p<0.05). This significant relationship implies that the market stakeholders were under the impression that the regulatory demands were due to some international obligation by the state and had nothing to do with the prevailing norms of the local supply chain environment (Casey & Scott, 2011; Yang, 2010). When complying with information security requirements is a norm external to the organization, it can lead to negative implications such as pressure (Siponen, 2000). If an organization has a perception that complying with external information security requirements is a norm of the market environment, then the pressure arising from such an external norm can lead to symbolic behaviour (Edelman, 1992). Further, when security requirements become abnormal (i.e. ambiguous and complex), people become stressed leading to security violations and non-compliance (D'Arcy, Herath, & Shoss, 2014), implying symbolic behaviour.

Norms are created by the stakeholders of the supply chain and the authorities together (Burgemeestre, et al., 2014), not just by direct pressure from the authorities. This is further supported by Yang (2010), who showed that changing laws to secure the containers did not particularly address local issues. According to Yang (2010), the port of Taiwan has no history of any terrorist activity however the laws were changed to reflect substantial emphasis on preventing terrorist activities rather than addressing more relevant lo such as the escalating cost of maintaining security. This observation is thoroughly debated in the scholarship on law and society. For example, Meares and Kahan (1998) state that norms are created through social dynamics that are important enough to be worth regulating. In this respect, the findings of this research show that the market stakeholders believed that the existing information security requirements were not regulated based on the prevailing local norms. Hence, higher regulatory demands in the context of information security in SCS created a lower perception of norm.

9.5.1.2 Market Influence

This research shows that market influence affects the perception of benefits (β_{H4}=0.4315, t_{H4}=8.277, p<0.001). There is a positive relationship between these two, indicating that when the market influences are high, the perceived benefits are high. This view is supported by Stevens et al. (2005) who showed that pressure from market stakeholders, such as customers, has a positive effect on organizations' compliance behaviour and thus a direct influence on the economic benefits of the organization. This is in line with Mowery and Rosenberg (1979), who suggest that market influence, such as normative pressure, leads to innovation. In the current research context, customs brokers and freight forwarders are constantly improving their systems with the application of modern software and other logistical support tools to facilitate secure information exchange, in compliance with the GSCS initiatives. This may often be the result of customer concerns over the response of these organization towards certain management principles coerced by the regular authorities (Scott, 1987). However, the findings show that the organizations believed that these influences emanating from the operating environment or the market stakeholders are beneficial for them in terms of leading to efficiency, especially in terms of the adoption of innovative technology and modern management principles. Therefore, this research shows that market influence and its impact on perception of benefits is an important factor influencing compliance behaviour.

This research investigated the effect of market influence on the perception of norms and found that it was not significant (β_{H3}=0.0360, t_{H3}=0.204). One reason for the lack of a significant relationship between pressure from the market stakeholders and the perception of norms could be that complying is already a norm of the industry due to other influences. This finding is explained by Delmas and Toffel (2004), who argue that institutional pressures are exerted at various levels of a firm which may be channelled to different functional subunits. Delmas and Toffel (2004) further state that market influence is not sufficient to change the perception of norms of the targeted group of participants this research has focused on. This finding suggests that boundary-spanning individuals such as the customs brokers, who play a distinctive role in complying with the information security demands, do not perceive market influence as an element that causes them to change or adapt the norm of their organization in terms of ISCB. Additional research is required to better understand this relationship.

9.5.1.3 Peer Pressure

The findings also show that peer pressure, which is the third factor of external inter-organizational influences, is an element that influences both the perception of norms (β_{H5}=0.288, t_{H5}=2.7267, p<0.01) and the perception of benefits (β_{H6}=0.405, t_{H6}=7.3939, p<0.001). The findings suggest that the greater the level of peer pressure on an organization, the greater the level of benefits perceived by that organization. Levitt and March (1988) argue that peer pressure may be perceived as being beneficial as it reduces research costs. This is in addition to the benefits experienced from the existing customers' willingness to continue to do business because of the target organization's conformity to the authorities' demands (Sarathy, 2006). This argument was hinted during the Phase 1 interviews when some of the participants commented on how their peers kept them on their toes and gave reasons to improve themselves if they were to survive in the industry.

In a similar manner, this research found that the greater the level of peer pressure, the greater the level of perception that information security is a norm of the organization. Perceived norms are often conceptualized as the perceived opinions of significant peers (Evans, et al., 1995) and one of the three distinct influences of peer pressure is social norms (Huddy, Feldman, Capelos, & Provost, 2002). In the research context, social norms can be seen as environmental norms; that is, the norms within the supply chain environment. When people perceive that social sanctions exist for non-compliance, they are more likely to conform if they also perceive that the behaviour is widespread among their peers (Lapinski & Rimal, 2005). Hence, peer pressure is an important factor influencing both perception of benefits and perception of norms.

9.5.2 Rules and Norms of Social Exchange

The two components of rules and norms and social exchange are fairness and reciprocity through reward, which were predicted to directly influence the perception of benefits.

9.5.2.1 Fairness

Fairness is described as a professional attitude, non-discriminatory behaviour, and conditional leniency shown in the execution of the procedures by the authorities. When organizations in this research believed that they had been dealt with fairly, they perceived that the actions by the authorities were beneficial (β_{H7}=0.184, t_{H7}=6.2906, p<0.001). The use of fair procedures and the delivery of fair outcomes have a variety of positive effects for an organization and enhance organizational commitment (Lind & Van den Bos, 2002). Lind and Van den Bos

(2002) show that this procedural fairness leads to a higher level of certainty or reduced uncertainty, which is beneficial to the organization. In this respect, the findings of this study are in accordance with the literature, which finds that fairness is perceived as beneficial to the organization. It is worth mentioning that during the interviews all of the participants expressed their satisfaction on the level of fairness portrayed by the relevant personnel of the local authorities. However, most of the respondents believed that it is unfair that the authorities of foreign trading partner countries treat New Zealand as being in the same risk category as the rest of the world. New Zealand does not have a history of any association with international terrorism or even civil disturbances that could lead to such an activity. Goldberg, Dar-El and Rubin (1991) argue that on worker reaction to presumed threats depends on the prevailing technological and demographic circumstances existing in the site. Huddy et al. (2002) meanwhile state that perceptions of terror threats are likely to be at least partly based on actual risk, which is likely to vary across locations. In such a situation where there is uncertainty about actual risk being imminent, the behavioural outcome under such perceptions may be passive dependence on the authoritative organization (Hoffmann & Trautmann, 2006) due to lack of choice (Zhuang & Zhou, 2004). However, fair treatment by the authorities may reduce this uncertainty, leading to a more active partnership (Hoffmann & Trautmann, 2006) as active dependence is deemed to be more beneficial to the organization's future relations with the authorities (Edelman, 1992). Hence, fairness is an important factor influencing the perception of benefits.

9.5.2.2 Reciprocity (Reward)

This research hypothesized reciprocity in the form of reward as a factor influencing the perception of benefits. According to Dekker (2004), reward is an incentive mechanism in an inter-organizational relationship to ensure the partners' motivation to perform adequately. However, the findings suggest that reward does not influence the perception of benefits (β_{H8}=0.004, t_{H8}=0.182). This is contrary to the many studies in literature that report rewards being perceived as beneficial (Stanton, Stam, Mastrangelo, & Jolton, 2005). One possible explanation is that a strong link between performance and reward must be present before a merit system can facilitate productivity (Atkinson, 1964; Porter & Lawler, 1968). This is to say that the reward awarded may not be equitable to the work done by the recipients (Leventhal, 1976b). Further, market stakeholders may be seeking social rewards such as enhanced reputation (Wilson, 1974), and this could be influenced by the social context which may vary geographically and also over time (Delmas & Montes-Sancho, 2010). Market stakeholders

depend on these benefits and reciprocated privileges to survive in the competition (Tokman, et al., 2007). While authoritative organizations have the power to reciprocate through reward to gain active dependence, leading to active partnership (Turker, 2014), the existing reward scheme in this research context seems inadequate to bring about this positive outcome.

9.5.3 Level of Influence of Environmental Factors

This research identifies four important factors influencing the drivers of ISCB in relation to GSCS initiatives. While organizational perceptions are found to have direct influence on compliance behaviour, the following factors were identified as important factors that influenced these organizational perceptions: (1) regulatory demands, (2) market influence, (3) peer pressure, and (4) fairness.

The levels of influence of these factors on the drivers of compliance behaviour can be established by using the structural path coefficient β obtained from the structural path analysis, along with the significant level of the *t*-statistics (Iriondo, et al., 2003). In this regard, SEM is efficient in providing a good estimate of the relative strength of a relationship theorized by a hypothesis (Johnson, Huggins, & DeNoyelles Jr, 1991; Kingsolver & Schemske, 1991). This is made possible by assessing the validity of pre-specified hypotheses, each representing a regression like relationship between factors (Hair, 2010). These results in turn provide a global picture of the affecting factors and clarify the importance of making appropriate management decisions (Iriondo, et al., 2003).

This study shows that the greatest influence is exerted by regulatory demands, which affect the perception of threats. The relationship that defines this path has a structural path coefficient β_{H1}=0.7749 and a t_{H1} =25.184 (p<0.001), thereby indicating a strong and a very significant influencing relationship. This is further confirmed by the high R^2_{THREAT}=0.6005 obtained for the perception of threats which indicates the substantive explanatory power of perception of threats under the influence of regulatory demands, as regulatory demands is the only exogenous variable explaining threat perception. This effect has also been observed by Sarathy (2006) and Bichou (2004). This study shows that the lower the perception of threats, the higher is compliance behaviour, which is indicative of substantial compliance behaviour (Christmann & Taylor, 2006). The structural path coefficient β_{H9}=0.1315 with t_{H9}=2.1342 (p<0.05) indicates the significant relation between the perception of threats and compliance behaviour. Therefore, based on the findings it can be concluded that regulatory demands create perception of threats,

and when the prevailing threat perception is high among the market stakeholders, this leads to symbolic compliance behaviour.

It is also interesting to note that regulatory demands have a considerable level of influence on perception of norms, with a structural path coefficient β_{H2}=0.3574 with t_{H2}=2.1862 (p<0.05), followed by peer pressure, with structural path coefficient β_{H5}=0.2880 with t_{H5}=2.7267 (p<0.01). Perception of norms has moderately high explanatory power, with an R^2_{NORM}=0.433 indicating a 43% of the variance. When regulatory demands are high, the perception of norms is low, leading to symbolic behaviour. Therefore, with the strong explanatory power of regulatory demands linked to both perception of threats and perception of norms, it can be concluded that the most powerful influence is indeed exerted by the regulatory demands, indirectly leading to symbolic compliance behaviour.

The second most influential driver is market influence. This is indicated by the effective structural path coefficient β_{H4}=0.4315 relative to the rest of the influencing factors and the highly significant t_{H4}=8.2777 (p<0.001) describing the positive relation it has on the driver, perception of benefits. According to a study conducted by Poksinska, Dahlgaard and Eklund (2003) on the implementation of the Environmental Management Standard ISO14000 in Sweden, the authors found that market influence played an important role. Market influence was perceived as beneficial as it improved organizations' corporate image among their stakeholders, in addition to the improvement in the relations with the same. Poksinska et al. (2003) call these benefits socio-economic benefits. This behaviour is similar to the ISCB related to the GSCS initiatives reported in this study. For instance, K. Guo et al. (2011) show that pressures exerted by subjective norms and peer behaviour are good deterrents for negative compliance behaviour. In this sense, it can be argued that the resultant behavioural outcome of deterring negative compliance behaviour is substantive compliance behaviour. This is further supported by the Stevens et al. (2005), who found that pressure from market stakeholders such as the customers leads to substantive compliance behaviour.

The third most significant influence is exerted by peer pressure on perception of benefits, with a structural path coefficient of β_{H6}=0.4049 and a highly significant t_{H6}=7.4258 (p<0.001). As noted before, the existing literature supports the strong influence peer pressure has on the perception of benefits, such as the benefits perceived by reduced research cost (Levitt & March, 1988). It is also interesting to note that peer pressure has an acceptable level of influence over

the perception of norms with β_{H5}=0.2880 and t_{H5}=2.7267 (p<0.01), however, as mentioned above its influencing strength is greater on perception of benefits.

The least influencing factor is fairness, portraying a lower structural path coefficient β_{H7}=0.1844 with t_{H7}=6.2906 (p<0.001) with respect to regulatory demands, market influence, and peer pressure. The most obvious reason for this result is the belief of market stakeholders that they were being subjected to rules and regulations that are not consistent with the prevailing local norms, as discussed above.

Therefore, based on the findings from the study it can be concluded that there are four significantly influential factors that affect the drivers of compliance behaviour in the given context. The most significant factor is regulatory demands, which motivates the market stakeholder in terms of pure economic gains in terms of avoiding costs. This motivation significantly affects the perception of threats leading to symbolic compliance behaviour. The second most significant factor is market influence, which motivates the market stakeholders in terms of socio-economic gain. This motivation significantly affects the perception of benefits leading to substantive compliance behaviour. This is an interesting finding in that these two drivers, perception of threats and perception of benefits, lead to two different behaviours of which one is desirable and the other undesirable. This means that the authorities should be wary that the more stringent they are with their regulatory demands, the more symbolic the behaviour will be towards the security requirements. Therefore, if the authorities want to receive accurate and reliable information, they have a better chance of achieving this outcome if they channel their compliance requirements through the market stakeholders, as the present study has proved that peer pressure and market influence are more effective in leading to substantive compliance behaviour through perception of benefits and perception of norms. How this could be achieved is beyond the scope of this study; however it would be a good direction for a future research to take. Through the determination of structural path coefficients and associated *t*-statistics, it has been established that, in decreasing order of significance, regulatory demands, market influence, peer pressure, and fairness all influence affect the drivers of ISCB.

9.5 Summary

This chapter has discussed the research findings in relation to the research questions and provided support for the findings from the literature. The drivers that explain ISCB were identified from the literature as organizational perceptions towards compliance behaviour which are affected by inter-organizational influences and the rules and norms of social

exchange. These drivers and associated factors were then verified for their relevance and validity in the SCS context. The extent of the impact of the drivers and associated factors was established by analysing the predictive relevance of the indirect variables, explanation power of the direct variables, and the significance of the identified relationships. The analysis shows that perception of benefits is strongest in driving substantive compliance behaviour. While perception of benefits is influenced by market influence, peer pressure, and fairness, the first of these is by far the strongest. In contrast, perception of threats strongly influences symbolic behaviour due to the strong influence created by the regulatory demands on the perception of threats. The next chapter concludes this thesis by highlighting the implications of this study, its limitations, and directions for future research.

CHAPTER 10: CONCLUSION

10.1 Chapter Overview

This chapter summarizes the research journey, covering the purpose of the study, the process of identification of the research gap, the research questions, methodology, and the findings of the surveys. The contributions of the study to both academia and industry are also discussed, followed by the limitations of the study and directions for future research.

10.2 The Research Journey

The purpose of this study is to understand and explain the ISCB in SCS under the influence of the GSCS initiatives. A review of existing literature on SCS and information security led to the identification of ISCB within an inter-organizational setting as a research gap. From the literature review several aspects came into focus relating to information security behaviour that seemed to have the potential to explain the compliance behaviour within the identified research gap. Thus, the following research questions were posed:

The overarching research question:

How do the supply chain security stakeholders comply with information security requirements mandated by the GSCS initiatives?

Sub research questions:

[RQ1] What are the drivers of ISCB and how do they impact the compliance behaviour exhibited by the stakeholders?

[RQ2] What factors influence inter-organizational ISCB in the context of the GSCS initiatives?

Using the results of the literature review and integrating two relevant theoretical frameworks (institutional theory and SET), a conceptual model is formulated to assist in seeking answers to the research questions. Since the drivers of compliance behaviour and the factors that influence these drivers were obtained from the information security literature, it was felt important to establish that these aspects are valid and relevant in the SCS context. As SCS is an emerging field, it was decided that validity and relevance would be best achieved through a qualitative survey. After an extensive review of the literature regarding research design and the choice of an appropriate research paradigm, a sequential mixed methods design with emphasis on quantitative survey was deemed the most appropriate methodology.

The qualitative survey was conducted among 15 participants from the supply chain industry of New Zealand recruited using the snowballing technique. The findings from the qualitative analysis showed that the drivers and the associated factors from the literature are indeed relevant to the SCS context. Finally, the conceptual model was developed into a research model and 11 research hypotheses were devised to test the theoretical relationships. This was followed by a quantitative survey conducted using an online self-administered questionnaire. There were 205 responses from 77 organizations which were analysed using PLS-SEM.

This research shows that ISCB is of two types: substantive compliance behaviour, which is the desired behaviour, and symbolic compliance behaviour, which may not lead to the expected outcomes of the compliance requirements. The research revealed that compliance behaviour is driven by three organizational perceptions towards compliance, which are perception of threats, perception of norms, and perception of benefits. Five factors that influenced these drivers were investigated in this research, three of which are collectively referred as inter-organizational influences and the remaining two as rules and norms of social exchange. The three factors of inter-organizational influences are (1) regulatory demands, (2) market influence, and (3) peer pressure, and the two factors of rules and norms of social exchange are fairness and reciprocity. The findings show that symbolic compliance behaviour is driven by perception of threats, which is influenced by regulatory demands. In contrast, substantive compliance behaviour is driven by perception of benefits and perception of norms, with the strongest influence on these perceptions being regulatory demands followed by market influence. These findings conclusively answer the research questions and help to fill the research gap identified at the beginning of this study, thereby fulfilling the objectives of this research.

10.3 Contributions of This Research

SCS is an emerging area of study with limited literature, while information security literature is a prominent strand within academia and is evolving at a considerable pace. However, as discussed in the relevant chapters of this thesis, there is a lack of knowledge in the area of socio-technical behaviour in information security compliance. Against this backdrop, this research makes contributions to both academia and industry.

10.3.1 Academic Contributions

In the literature on ISCB, the findings are mostly reported in terms of compliance or non-compliance. This study contributes by identifying two types of compliance behaviour, namely

symbolic and substantive compliance behaviour in the context of ISCB. This study shows that organizations exhibit both two types of compliance behaviour and that the outcome of the two types of behaviour is entirely different. The desired behaviour is substantive compliance behaviour, the absence of which leads to symbolic behaviour, which can lead to devastating consequences. Therefore, this theoretical contribution in identifying between these two types of compliance behaviour is considered an important academic contribution to the information security literature.

The second contribution this study makes is the identification of the type of compliance behaviour influenced by the existing drivers. The findings show that perception of threats leads to symbolic behaviour while perception of norms and perception of benefits leads to substantive behaviour. This is considered to be an important academic contribution as it brings to the forefront the type of perceptions that motivate the desired compliance behaviour in an inter-organizational context, especially when the power of exchange between two organizations is not equal.

The third contribution of this study is the identification of the impacts of the influencing factors on the drivers of ISCB. By using SCS under the GSCS initiatives as the research context, this study brings to the forefront the impact that external inter-organizational influences and rules and norms of social exchange have on the drivers of compliance behaviour. In this respect, the study highlights that inter-organizational influences such as regulatory demands, market influence, and peer pressure are important elements in influencing the drivers of compliance behaviour. Under rules of norm and social exchange, fairness was found to be a significant element in influencing the drivers. However, this study finds that reciprocity through the existing reward scheme is not significant. This is a critical point, as several references are made in the literature to the effectiveness of reward in general as a means for social exchange, but it is very clear from this study that the reward has to be relevant and worthy to the given context.

The fourth contribution is the aggregation of existing theoretical frameworks to explain ISCB in a heightened security environment, such as under the GSCS initiatives. To the best of the researcher's knowledge, this study is the first to aggregate institutional theory and SET to explain and understand ISCB within the SCS context. The GSCS initiatives context provided a basis to focus the study on compliance behaviour in a situation where there is a disparity in power within the exchange relation between two organizations that exchange sensitive information.

The fifth contribution of this study relates to its identification of critical theoretical perspectives that can contribute to the academic curriculum of supply chain risk management courses. The findings of this research can be used to discuss the possible undesirable outcomes of strong regulatory demands, as this study shows that under strong regulatory demands there is a negative feeling of uncertainty, creating a perception of threats leading to undesirable symbolic compliance behaviour. On the other hand, this study suggests that in order to bring about desirable outcomes through substantive compliance behaviour, it would be more effective to promote the requirements through the market environment rather than through strong regulatory demands. Further, the findings enable discussion of the fact that fair procedures across the stakeholders of a given environment can be more effective in achieving desired outcomes than reciprocating compliance behaviour with reward and privileges.

The sixth contribution is the academic contribution accorded to the complex socio-technical literature by studying the behavioural aspects of complex information technology and complex inter-organizational structures. In this respect, this study has revealed the social behavioural influence of the boundary personnel and their interaction with complex information systems in their efforts to keep up with the compliance requirements. This finding enables to focus on the boundary personnel as a key ingredient of the complex socio-technical composition to ensure the facets information security (confidentiality, integrity, and availability).

The final academic contribution is a methodological one. This study shows that a sequential mixed methods design is a suitable methodology when researching an intrusive and a complex socio-technical topic. There are several forms of mixed method research design proposed in the literature. In this research qualitative inquiry conducted as the first phase of sequential mixed method has been utilised to recruit participants through snowballing, in addition to model verification. A paper regarding this discussion was presented at the KMO 2014 conference in Chile, which is now published in *Lecture Notes in Business Information Processing* by Sage (Shafiu, Wang, & Singh, 2014).

10.3.2 Practical Contributions

International standards are mostly generalized and therefore do not really apply to all cases. This study shows that the international SCS standards, also called the GSCS initiatives, are no exception. This study shows that one of the drivers of compliance behaviour leads to symbolic behaviour. This type of symbolic behaviour could result in negative consequences such as sabotage, terrorist activities, and even theft. Hence, this study provides a set of drivers that can

be used to identify if the proper measures are in place to achieve a more positive outcome, such as substantive compliance. Hence, the first practical contribution is the identification of drivers which would assist the authorities to identify if the organizations are exhibiting substantive or symbolic behaviour. In this sense, public institutions such as border-control authorities should be wary of the fact that pushing sensitive security requirements through strong regulatory demands may not achieve the intended security targets. The market stakeholders or the private organizations could be responding to these requirements only superficially.

Pressure from authorities through regulatory demands to comply with certain rules is accepted positively when these regulations and rules reflect the norms of the environment. This study's findings show that regulations are not perceived as a norm by local stakeholders in the GSCS context if they do not reflect the local norms. The authorities should take into consideration the prevailing norms of the environment before such rules and regulations are formulated. The decision makers of the private stakeholders should be convinced of the implications of the regulations in terms of its relevance to the local environment so that they would incorporate these regulations into their company policies. Once these regulations are incorporated into the company polices it would become part of the company's training programs and finally become a component of the staff appraisal system leading to substantial compliance behaviour.

So far, SCS activities have been locally enforced by regulations and also through voluntary means. However, this study shows that the greater the regulatory demands, the more likely symbolic compliance behaviour will be seen. On the other hand, market influences are more instrumental in leading to substantive compliance behaviour. In this respect this study contributes to industry by showing that authorities could achieve better outcomes if they redesign their policies and strategies to reflect more market-oriented approaches and advocate changes through market stakeholders rather than through regulatory or mandatory approaches alone, in order to achieve substantive compliance.

Finally, this study also contributes by empirically proving that the privileges and rewards accorded for complying do not necessarily lead to substantive compliance behaviour. The authorities advocating reciprocity through rewards as privileges for compliance may be under the impression that their trading partners accept these privileges as beneficial to their organizations. However, this study suggests that this is not the case. Therefore, the provisions included in the GSCS initiatives need to be redesigned and customized to suit the needs of the United States' regional trading partners.

10.4 Limitations of the Research

One of the biggest limitations of this research is in achieving a substantial sample size. As discussed before the nature of the study being intrusive discourages participants, especially when the researcher is a student. Therefore, future research in these areas where it is considered intrusive would be more fruitful if the research is conducted in a collaborated manner through influencing agencies.

New Zealand does not have a history of major supply chain disruptions due to security incidents, nor does it have any associations with major security incidents nationally or globally. Hence, the behavioural aspects of the New Zealand supply chain stakeholders may be very different to that of countries that have gone through major disruptions in terms of terrorist activities, sabotage or theft. Therefore, this study has limitations when it comes to generalizing the findings in relation to the implications of GSCS initiatives on a global basis. A further limitation is generalizing the findings to the international trading community of New Zealand as a whole due to the small sample size of the research. The intrusive nature of the study discourages participants, especially when the researcher is a student. As such, one future research area would be to test the research model in a country with the opposite geopolitical environment to New Zealand. The knowledge would assist in customizing security requirements according to security classifications based on the level of threats and the general perceptions of the trade links within economic regions or among countries. To achieve a substantial sample size, the research could be conducted in collaboration with influential organizations within the research context.

Another limitation of this study stems from the demographics of the participants for this study. As presented in Figure 23 (Chapter 8), the average age of the participants in the quantitative survey was 35 and their average experience in the field was four years, which means the majority of the participating boundary-spanning personnel were not among the first movers towards the compliance requirements dictated by the GSCS initiatives. This is important as the literature suggests that organizations that changed their internal structures to comply with the environmental regulations in its inception stage complied substantively, while late joiners reflected a more symbolic nature of compliance (Delmas & Montes-Sancho, 2010). Therefore, using the age of the company and years of experience of the boundary-spanning personnel as control variables in a future study would eliminate this limitation.

10.5 Directions for Future Research

The study of information security is an intrusive form of study. This is a deterrent factor as far as participation in the study is concerned. On top of this, questions when behavioural aspects such as perception of threats and fairness in relevance to the authorities were touched on in the interviews, there was some level of hesitation from the participants. There were signs of participants attempting to search for politically correct answers or being cautious in their choice of words. Therefore, though the quantitative study has been conducted anonymously, there is the possibility that this cautious behaviour might be reflected in their choice of answers. One future area of research could therefore be to investigate the prevailing levels of trust and confidence between the private sector and the public sector supply chain stakeholders in relation to information security.

The SCS literature suggests, without empirical evidence, that reward is an incentive mechanism which could bring about desired outcomes towards ISCB. This study empirically shows that reward is *not* an influencing factor in the context of SCS. Therefore, it would be fruitful to explore in what circumstances and what types of rewards are perceived as beneficial in bringing about desirable compliance behaviour.

It is argued that training institutions are influential in setting the norm of a given environment and that the customs brokers who have to be certified through training must have attended such a training institute. Therefore, the impact of such training institutions on setting the norms of the supply chain environment would be a good future research area, as this research has already given evidence of the power of perceived norms in leading to substantive compliance behaviour.

This study has focused on the market stakeholders such as customs brokers, traders and freight forwarders of the supply chain. Another potentially fruitful future research area would be to study the information security behavioural aspects of the non-market stakeholders such as the public sector in response to the GSCS initiatives. This knowledge would assist in paving the way for a more collaborative and compatible security process between the public and private sector, leading to a more secure supply chain.

References

Abrahamsson, B. (1993). *The Logic of Organizations*. California: Sage Publications Inc.

Adams, A., & Blandford, A. (2005). Bridging the gap between organizational and user perspectives of security in the clinical domain. *International Journal of Human-Computer Studies, 63*(1-2), 175-202.

Akbulut-Bailey, A. Y. (2011). Information sharing between local and state governments. *The Journal of Computer Information Systems, 51*(4), 53-63.

Akter, S., D'Ambra, J., & Ray, P. (2011). An evaluation of PLS based complex models: the roles of power analysis, predictive relevance and GoF index. *AMCIS 2011 Proceedings-All Submissions*.

Aldrich, H., & Herker, D. (1977). Boundary spanning roles and organization structure. *Academy of Management Review, 2*(2), 217-230.

Altmann, J. (1974). Observational study of behavior: sampling methods. *Behaviour*, 227-267.

Amaratunga, D., Baldry, D., Sarshar, M., & Newton, R. (2002). Quantitative and qualitative research in the built environment: application of "mixed" research approach. *Work study, 51*(1), 17-31.

Ancona, D. G., & Caldwell, D. F. (1992). Bridging the Boundary: External Activity and Performance in Organizational Teams. [Article]. *Administrative Science Quarterly, 37*(4), 634-665.

Anderson, C. L., & Agarwal, R. (2010). Practicing safe computing: A multimethod empirical examination of home computer user security behavioral intentions. [Article]. *MIS Quarterly, 34*(3), 613-A615.

Anderson, J. C., & Narus, J. A. (1990). A model of distributor firm and manufacturer firm working partnerships. *the Journal of Marketing, 54*(1), 42-58.

Anderson, R. (2001). *Why information security is hard-an economic perspective.* Paper presented at the Computer Security Applications Conference, 2001. ACSAC 2001. Proceedings 17th Annual.

Antweiler, W. (2003). How effective is green regulatory threat? *American Economic Review, 93*(2), 436-441.

Arvey, R. D., & Ivancevich, J. M. (1980). Punishment in organizations: A review, propositions, and research suggestions. *Academy of Management Review, 5*(1), 123-132.

Ashenden, D., & Sasse, A. (2013). CISOs and organisational culture: Their own worst enemy? *Computers & Security, 39*, 396-405.

Atkinson, J. W. (1964). *An introduction to motivation*. Oxford, England: Van Nostrand.

Atkinson, R., & Flint, J. (2001). Accessing hidden and hard-to-reach populations: Snowball research strategies. *Social research update, 33*(1), 1-4.

Autry, C. W., & Bobbitt, L. M. (2008). Supply chain security orientation: conceptual development and a proposed framework. *International Journal of Logistics Management, The, 19*(1), 42-64.

Babu, L. D., Gunasekaran, A., & Krishna, P. V. (2014). A decision–based pre–emptive fair scheduling strategy to process cloud computing work–flows for sustainable enterprise management. *International Journal of Business Information Systems, 16*(4), 409-430.

Backhouse, J., Hsu, C. W., & Silva, L. (2006). Circuits of power in creating de jure standards: Shaping an international information systems security standard. [Article]. *MIS Quarterly, 30*(Special Issue on Standard Making), 413-438.

Bagozzi, R. P. (1981). Evaluating structural equation models with unobservable variables and measurement error: a comment. *Journal of Marketing Research, 18*(3), 375-381.

Bagozzi, R. P., & Yi, Y. (1988). On the evaluation of structural equation models. *Journal of the academy of marketing science, 16*(1), 74-94.

Bakshi, N., & Gans, N. (2010). Securing the containerized supply chain: Analysis of government incentives for private investment. *Management Science, 56*(2), 219-233.

Bandura, A. (1986). *Social foundations of thought and action*: Englewood Cliffs, NJ Prentice Hall.

Banomyong, R. (2005). The impact of port and trade security initiatives on maritime supply-chain management. *Maritime Policy and Management, 32*(1), 3-13.

Baskerville, R., Spagnoletti, P., & Kim, J. (2014). Incident-centered information security: Managing a strategic balance between prevention and response. *Information & management, 51*(1), 138-151.

Baskerville, R. L., & Stage, J. (1996). Controlling prototype development through risk analysis. *Mis Quarterly*, 481-504.

Beckles, B., Welch, V., & Basney, J. (2005). Mechanisms for increasing the usability of grid security. *International Journal of Human-Computer Studies, 63*(1-2), 74-101.

Benaroch, M., Lichtenstein, Y., & Robinson, K. (2006). Real options in information technology risk management: an empirical validation of risk-option relationships. *Mis Quarterly*, 827-864.

Bendor, J., & Swistak, P. (2001). The evolution of Norms1. *American Journal of Sociology, 106*(6), 1493-1545.

Benton, W., & Maloni, M. (2005). The influence of power driven buyer/seller relationships on supply chain satisfaction. *Journal of Operations Management, 23*(1), 1-22.

Bertino, E., Jajodia, S., & Samarati, P. (1995). Database security: Research and practice. *Information Systems, 20*(7), 537-556.

Bichou, K. (2004). The ISPS code and the cost of port compliance: An initial logistics and supply chain framework for port security assessment and management. *Maritime Economics and Logistics, 6*(4), 322-348.

Biernacki, P., & Waldorf, D. (1981). Snowball sampling: Problems and techniques of chain referral sampling. *Sociological methods & research, 10*(2), 141-163.

Bjorck, F. (2004). *Institutional Theory: A new perspective for research into IS/IT in organizations.* Paper presented at the Proceedings of the 37th Annual Hawaii International Conference on System Sciences, Hawai.

Blakley, B., McDermott, E., & Geer, D. (2001). *Information security is information risk management.* Paper presented at the Proceedings of the 2001 workshop on New security paradigms.

Blau, P. M. (1964). *Exchange and power in social life*. Wiley, New York: Transaction Publishers, Rutgers.

Blau, P. M. (1968). Social exchange. *International encyclopedia of the social sciences, 7*, 452-457.

Boss, S., & Kirsch, L. (2007). *The last line of defense: motivating employees to follow corporate security guidelines.* Paper presented at the Proceedings of the 28th International Conference on Information Systems.

Boss, S. R., Kirsch, L. J., Angermeier, I., Shingler, R. A., & Boss, R. W. (2009). If someone is watching, I'll do what I'm asked: mandatoriness, control, and information security. *European Journal of Information Systems, 18*(2), 151-164.

Boudreau, M.-C., Gefen, D., & Straub, D. W. (2001). Validation in information systems research: a state-of-the-art assessment. *Mis Quarterly, 25*(1), 1-16.

Breaux, T. D., & Antón, A. I. (2008). Analyzing regulatory rules for privacy and security requirements. *Software Engineering, IEEE Transactions on, 34*(1), 5-20.

Britten, N. (1995). Qualitative interviews in medical research. *BMJ: British Medical Journal, 311*(6999), 251.

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. [Article]. *MIS Quarterly, 34*(3), 523-A527.

Burgemeestre, B., Hulstijn, J., & Tan, Y.-H. (2014). Norm emergence in regulatory compliance *The Complexity of Social Norms* (pp. 123-139): Springer.

Burgess, K., Singh, P. J., & Koroglu, R. (2006). Supply chain management: a structured literature review and implications for future research. *International Journal of Operations & Production Management, 26*(7), 703-729.

Butler, T. (2010). Compliance with institutional imperatives on environmental sustainability: Building theory on the role of Green IS. *The Journal of Strategic Information Systems, 20*(1), 6-26.

Cai, J., Liu, X., Xiao, Z., & Liu, J. (2009). Improving supply chain performance management: A systematic approach to analyzing iterative KPI accomplishment. *Decision Support Systems, 46*(2), 512-521.

Caldwell, S. L. (2010). *Supply Chain Security: Feasibility and Cost-Benefit Analysis Would Assist DHS in Assessing and Implementing the Requirement to Scan 100% of US-Bound Containers*: DIANE Publishing.

Carlsmith, K. M., Darley, J. M., & Robinson, P. H. (2002). Why do we punish?: Deterrence and just deserts as motives for punishment. *Journal of personality and social psychology, 83*(2), 284.

Carmines, E. G., & Zeller, R. A. (1979). *Reliability And Validity Assessment (Quantitative Applications In The Social Sciences) Author: Edward G. Carmines, Richard*: Sage Publications, Inc.

Carpenter, V. L., & Feroz, E. H. (2001). Institutional theory and accounting rule choice: an analysis of four US state governments' decisions to adopt generally accepted accounting principles. *Accounting, organizations and society, 26*(7), 565-596.

Carter, C. R., & Carter, J. R. (1998). Interorganizational determinants of environmental purchasing: initial evidence from the consumer products industries*. *Decision Sciences, 29*(3), 659-684.

Casey, D., & Scott, C. (2011). The crystallization of regulatory norms. *Journal of Law and Society, 38*(1), 76-95.

Chad, W. A., & Bobbitt, L. M. (2008). Supply chain security orientation: conceptual development and a proposed framework. [DOI: 10.1108/09574090810872596]. *International Journal of Logistics Management, The, 19*(1), 42-64.

Chang, C.-C., Hwang, R.-J., & Wu, T.-C. (1992). Cryptographic key assignment scheme for access control in a hierarchy. *Information Systems, 17*(3), 243-247.

Chang, C.-H., Xu, J., & Song, D.-P. (2014). An analysis of safety and security risks in container shipping operations: A case study of Taiwan. *Safety Science, 63*, 168-178.

Chen, C.-J., & Huang, J.-W. (2007). How organizational climate and structure affect knowledge management—The social interaction perspective. *International Journal of Information Management, 27*(2), 104-118.

Chen, P.-y., Kataria, G., & Krishnan, R. (2011). Correlated failures, diversification and information security risk management. [Article]. *MIS Quarterly, 35*(2), 397-A393.

Chen, Y.-H., Lin, T.-P., & Yen, D. C. (2014). How to facilitate inter-organizational knowledge sharing: The impact of trust. *Information & Management, 51*(5), 568-578.

Chen, Y.-K., & Sun, S. Survey Research in Operations Management: Historical Analyses.

Chen, Y.-K., & Sun, S. (2003). Survey Research in Operations Management: Historical Analyses. *Joirnal of Operations Management, 21*(4), 14.

Chin, W. W. (1998a). Issues and Opinion on Structural Equation Modeling. *MIS Quarterly*, pp. 1-1. Retrieved from http://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=345479&site=ehost-live&scope=site

Chin, W. W. (1998b). The partial least squares approach to structural equation modeling. *Modern methods for business research, 295*(2), 295-336.

Christensen, P. N., Rothgerber, H., Wood, W., & Matz, D. C. (2004). Social norms and identity relevance: A motivational approach to normative behavior. *Personality and Social Psychology Bulletin, 30*(10), 1295-1309.

Christmann, P., & Taylor, G. (2006). Firm self-regulation through international certifiable standards: determinants of symbolic versus substantive implementation. *Journal of International Business Studies, 37*(6), 863-878.

Clark, V. L. P. (2010). The adoption and practice of mixed methods: US trends in federally funded health-related research. *Qualitative Inquiry, 16*(6), 428-440.

Closs, D., Speier, C., Whipple, J., & Voss, M. D. (2008). A Framework for Protecting Your Supply Chain. *Supply Chain Management Review, 12*(2), 38-n/a.

Closs, D. J., & McGarrell, E. F. (2004). *Enhancing security throughout the supply chain*. USA: IBM Center for the Business of Government.

Cody, E., Sharman, R., Rao, R. H., & Upadhyaya, S. (2008). Security in grid computing: A review and synthesis. *Decision Support Systems, 44*(4), 749-764.

Cohen, J. (1992). A power primer. *Psychological bulletin, 112*(1), 155.

Cohen, J. F., Mou, J., & Trope, J. (2014). *Adoption of Cloud Computing by South African Firms: The Role of Institutional Forces, Absorptive Capacity, and Top Management.* Paper presented at the Proceedings of the Southern African Institute for Computer Scientist and Information Technologists Annual Conference 2014 on SAICSIT 2014 Empowered by Technology.

Coiera, E. (2007). Putting the technical back into socio-technical systems research. *International Journal of Medical Informatics, 76*, S98-S103.

Collins, K. M., Onwuegbuzie, A. J., & Sutton, I. L. (2006). A model incorporating the rationale and purpose for conducting mixed methods research in special education and beyond. *Learning Disabilities: A Contemporary Journal, 4*(1), 67-100.

Concha, M. (2014). Exploring Collaboration, Its Antecedents, and Perceived Outcomes in Service Partnerships of Community-Based Organizations in South Florida. *International Journal of Public Administration, 37*(1), 44-52.

Cook, K. S. (1977). Exchange and Power in Networks of Interorganizational Relations*. *The Sociological Quarterly, 18*(1), 62-82.

Cremonini, M., & Nizovtsev, D. (2009). Risks and Benefits of Signaling Information System Characteristics to Strategic Attackers. [Article]. *Journal of Management Information Systems, 26*(3), 241-274.

Creswell, J. W. (2003). *Research design: Qualitative, quantitative, and mixed methods approaches*: Sage publications.

Creswell, J. W. (2012). *Qualitative inquiry and research design: Choosing among five approaches*. California, USA: Sage publications.

Creswell, J. W., & Clark, V. L. P. (2007). *Designing and conducting mixed methods research*: Wiley Online Library.

Creswell, J. W., & Miller, D. L. (2000). Determining validity in qualitative inquiry. *Theory into practice, 39*(3), 124-130.

Cropanzano, R., & Mitchell, M. S. (2005). Social exchange theory: An interdisciplinary review. *Journal of Management, 31*(6), 874-900.

Culnan, M. J., & Armstrong, P. K. (1999). Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation. *Organization science, 10*(1), 104-115.

D'Arcy, J., Herath, T., & Shoss, M. K. (2014). Understanding Employee Responses to Stressful Information Security Requirements: A Coping Perspective. *Journal of Management Information Systems, 31*(2), 285-318.

D'Arcy, J., Hovav, A., & Galletta, D. (2009). User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach. *Information Systems Research, 20*(1), 79-98.

D'Aubeterre, F., Singh, R., & Iyer, L. (2008). Secure activity resource coordination: empirical evidence of enhanced security awareness in designing secure business processes. *European Journal of Information Systems, 17*(5), 528.

Dahl, R. A. (1957). The concept of power. *Behavioral science, 2*(3), 201-215.

Dahlman, O., Mackby, J., Sitt, B., Poucet, A., Meerburg, A., Massinon, B., et al. (2005). *Container security: a proposal for a comprehensive code of conduct*: DTIC Document.

Day, R., & Woodward, T. (2004). Disclosure of information about employees in the Directors' report of UK published financial statements: substantive or symbolic? *Accounting Forum, 28*(1), 43-59.

de Paula, R., Ding, X., Dourish, P., Nies, K., Pillet, B., Redmiles, D. F., et al. (2005). In the eye of the beholder: A visualization-based approach to information system security. *International Journal of Human-Computer Studies, 63*(1-2), 5-24.

Dekker, H. C. (2004). Control of inter-organizational relationships: evidence on appropriation concerns and coordination requirements. *Accounting, Organizations and Society, 29*(1), 27-49.

Delmas, M., & Toffel, M. W. (2004). Stakeholders and environmental management practices: an institutional framework. *Business strategy and the Environment, 13*(4), 209-222.

Delmas, M. A., & Montes-Sancho, M. J. (2010). Voluntary agreements to improve environmental quality: Symbolic and substantive cooperation. *Strategic Management Journal, 31*(6), 575-601.

Deutsch, M. (1975). Equity, equality, and need: What determines which value will be used as the basis of distributive justice? *Journal of Social issues, 31*(3), 137-149.

Dhillon, G., & Moores, S. (2001). Computer crimes: theorizing about the enemy within. *Computers & Security, 20*(8), 715-723.

Dhillon, G., & Torkzadeh, G. (2006). Value-focused assessment of information system security in organizations. *Information Systems Journal, 16*(3), 293-314.

DiMaggio, P. J., & Powell, W. W. (1983). The iron cage revisited: Institutional isomorphism and collective rationality in organizational fields. *American sociological review, 48*(2), 147-160.

Dinev, T., & Qing, H. (2007). The Centrality of Awareness in the Formation of User Behavioral Intention toward Protective Information Technologies. [Article]. *Journal of the Association for Information Systems, 8*(7), 386-408.

Dodge Jr, R. C., Carver, C., & Ferguson, A. J. (2007). Phishing for user security awareness. *Computers & Security, 26*(1), 73-80.

Domingues, S., Macário, R., Pauwels, T., Van de Voorde, E., Vanelslander, T., & Vieira, J. (2014). An assessment of the regulation of air cargo security in Europe: A Belgian case study. *Journal of Air Transport Management, 34*, 131-139.

Downs, G. W., Rocke, D. M., & Barsoom, P. N. (1996). Is the good news about compliance good news about cooperation? *International Organization, 50*(03), 379-406.

Dumas, M., Recker, J. C., & Weske, M. (2012). Management and engineering of process aware information systems: introduction to the special issue. *Information Systems, 37*(2), 77-79.

Edelman, L. B. (1992). Legal ambiguity and symbolic structures: Organizational mediation of civil rights law. *American journal of Sociology, 97*(6), 1531-1576.

El-Gayar, O. F., & Fritz, B. D. (2010). A web-based multi-perspective decision support system for information security planning. *Decision Support Systems, 50*(1), 43-54.

El Kharbili, M., Stein, S., Markovic, I., & Pulvermüller, E. (2008). *Towards a framework for semantic business process compliance management.* Paper presented at the Proceedings of the workshop on Governance, Risk and Compliance for Information Systems.

Emerson, R. M. (1976). Social exchange theory. *Annual review of sociology*, 335-362.

Employment, M. o. B. I. a. (2012).

Evan, W. M. (1965). Toward a theory of inter-organizational relations. *Management Science (pre-1986), 11*(10), B217-B217.

Evans, N., Gilpin, E., Farkas, A. J., Shenassa, E., & Pierce, J. P. (1995). Adolescents' perceptions of their peers' health norms. *American Journal of Public Health, 85*(8_Pt_1), 1064-1069.

Falk, A., & Fischbacher, U. (2006). A theory of reciprocity. *Games and Economic Behavior, 54*(2), 293-315.

Fan, J., Zhang, P., & Yen, D. C. (2014). G2G information sharing among government agencies. *Information & Management, 51*(1), 120-128.

Faul, F., Erdfelder, E., Lang, A.-G., & Buchner, A. (2007). G* Power 3: A flexible statistical power analysis program for the social, behavioral, and biomedical sciences. *Behavior research methods, 39*(2), 175-191.

Fehr, E., & Gächter, S. (2000). Fairness and retaliation: The economics of reciprocity. *The journal of economic perspectives, 14*(3), 159-181.

Fehr, E., & Schmidt, K. M. (1999). A theory of fairness, competition, and cooperation. *The quarterly journal of economics, 114*(3), 817-868.

Fenton, W. S., Blyler, C. R., & Heinssen, R. K. (1997). Determinants of medication compliance in schizophrenia: empirical and clinical findings. *Schizophrenia Bulletin, 23*(4), 637.

Fernández-Medina, E., Trujillo, J., & Piattini, M. (2007). Model-driven multidimensional modeling of secure data warehouses. *European Journal of Information Systems, 16*(4), 374.

Flynn, S. E. (2000). Beyond border control. *Foreign Affairs, 79*(6), 57-68.

Fornell, C., & Bookstein, F. L. (1982). Two structural equation models: LISREL and PLS applied to consumer exit-voice theory. *Journal of Marketing research, 19*(4), 440-452.

Fornell, C., & Larcker, D. F. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of marketing research, 18*(1), 39-50.

Fossey, E., Harvey, C., McDermott, F., & Davidson, L. (2002). Understanding and evaluating qualitative research*. *Australian and New Zealand journal of psychiatry, 36*(6), 717-732.

Gable, G. G. (1994). Integrating case study and survey research methods: an example in information systems. *European journal of information systems, 3*(2), 112-126.

Gassenheimer, J. B., Houston, F. S., & Davis, J. C. (1998). The role of economic value, social value, and perceptions of fairness in interorganizational relationship retention decisions. *Journal of the Academy of Marketing Science, 26*(4), 322-337.

Gauzente, C. (2004). Web merchants' privacy and security statements: how reassuring are they for consumers? A two-sided approach. *Journal of Electronic Commerce Research, 5*(3), 181-198.

Geels, F. W. (2004). From sectoral systems of innovation to socio-technical systems: Insights about dynamics and change from sociology and institutional theory. *Research policy, 33*(6), 897-920.

Gefen, D., Karahanna, E., & Straub, D. W. (2003). Trust and TAM in online shopping: an integrated model. *MIS Quarterly, 27*(1), 51-90.

Gefen, D., Straub, D., & Boudreau, M.-C. (2000). Structural equation modeling and regression: Guidelines for research practice. *Communications of the association for information systems, 4*(1), 7.

Gilbert, A., & Churchill, J. (1979). A paradigm for developing better measures of marketing constructs. *Journal of Marketing Research, 16*(1), 64-73.

Goldberg, A. I., Dar-El, E. M., & Rubin, A. H. E. (1991). Threat perception and the readiness to participate in safety programs. *Journal of Organizational Behavior, 12*(2), 109-122.

Goodhue, D. L., Lewis, W., & Thompson, R. (2012). Does PLS have advantages for small sample size or non-normal data? *Mis Quarterly, 36*(3), 891-1001.

Goodhue, D. L., & Straub, D. W. (1991). Security concerns of system users: A study of perceptions of the adequacy of security. *Information & Management, 20*(1), 13-27.

Gordon, L. A., Loeb, M. P., & Lucyshyn, W. (2003). Sharing information on computer systems security: An economic analysis. *Journal of Accounting and Public Policy, 22*(6), 461-485.

Gordon, L. A., Loeb, M. P., Lucyshyn, W., & Richardson, R. (2005). *2005 CSI/FBI computer crime and security survey*: Computer Security Institute San Francisco, CA.

Götz, O., Liehr-Gobbers, K., & Krafft, M. (2010). Evaluation of structural equation models using the partial least squares (PLS) approach *Handbook of partial least squares* (pp. 691-711): Springer.

Gray, W. B., & Deily, M. E. (1996). Compliance and enforcement: Air pollution regulation in the US steel industry. *Journal of environmental economics and management, 31*(1), 96-111.

Greene, J. C., Caracelli, V. J., & Graham, W. F. (1989). Toward a conceptual framework for mixed-method evaluation designs. *Educational evaluation and policy analysis, 11*(3), 255-274.

Griffith, D. A., Harvey, M. G., & Lusch, R. F. (2006). Social exchange in supply chain relationships: the resulting benefits of procedural and distributive justice. *Journal of operations management, 24*(2), 85-98.

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

Gunasekaran, A., & Ngai, E. (2004). Information systems in supply chain integration and management. *European Journal of Operational Research, 159*(2), 269-295.

Guo, F., Mu, Y., & Susilo, W. (2011). Improving security of q-SDH based digital signatures. *Journal of Systems and Software, 84*(10), 1783-1790.

Guo, K. H., & Yuan, Y. (2012). The effects of multilevel sanctions on information security violations: A mediating model. *Information & management, 49*(6), 320-326.

Guo, K. H., Yuan, Y., Archer, N. P., & Connelly, C. E. (2011). Understanding Nonmalicious Security Violations in the Workplace: A Composite Behavior Model. [Article]. *Journal of Management Information Systems, 28*(2), 203-236.

Gutierrez, X., & Hintsa, J. (2006). *Voluntary supply chain security programs: a systematic comparison.* Paper presented at the The International Conference on Information System, Logistics and Supply Chain, Lyon, France.

H.Rex, H. (1981). Database security—System architectures. *Information Systems, 6*(1), 1-22.

Haenlein, M., & Kaplan, A. M. (2004). A beginner's guide to partial least squares analysis. *Understanding statistics, 3*(4), 283-297.

Hair, J. F., Black, W.C., Babin, B.J. and Anderson, R.E (2010). *Multivariate data analysis, a global perspective* (7th Edition ed.). New Jersey: Pearson Prentice Hall.

Hair, J. F., Ringle, C. M., & Sarstedt, M. (2011). PLS-SEM: Indeed a silver bullet. *The Journal of Marketing Theory and Practice, 19*(2), 139-152.

Hair Jr, J. F., Anderson, R. E., Tatham, R. L., & William, C. (1995). *Black (1995), Multivariate data analysis with readings*. New Jersey, USA: Prentice Hall.

Hanson, W. E., Creswell, J. W., Clark, V. L. P., Petska, K. S., & Creswell, J. D. (2005). Mixed methods research designs in counseling psychology. *Journal of Counseling Psychology, 52*(2), 224.

Harland, C., Brenchley, R., & Walker, H. (2003). Risk in supply networks. *Journal of Purchasing and Supply management, 9*(2), 51-62.

Haughton, M. A., & Isotupa, K. S. (2013). Traffic control in Canada–USA border checkpoint operations: impacts on supply chain velocity, infrastructure spending, and national security. *International Journal of Services and Operations Management, 16*(3), 337-351.

Henseler, J., Ringle, C. M., & Sinkovics, R. R. (2009). The use of partial least squares path modeling in international marketing. *Advances in international marketing, 20*, 277-319.

Herath, T., & Rao, H. R. (2009a). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems, 47*(2), 154-165.

Herath, T., & Rao, H. R. (2009b). Protection motivation and deterrence: a framework for security policy compliance in organisations. *European Journal of Information Systems, 18*(2), 106-125.

Hewstone, M., Rubin, M., & Willis, H. (2002). Intergroup bias. *Annual review of psychology, 53*(1), 575-604.

Higgs, J., & Titchen, A. (1995). Propositional, professional and personal knowledge in clinical reasoning. *Clinical Reasoning in the Health Professions. Oxford, UK: Butterworth-Heinemann*, 129-146.

Hinkin, T. R. (1998). A brief tutorial on the development of measures for use in survey questionnaires. *Organizational research methods, 1*(1), 104-121.

Hintsa, J. (2010). A comprehensive framework for analysis and design of supply chain security standards. *Journal of Transportation Security, 3*(2), 105-125.

Hoepfl, M. C. (1997). Choosing qualitative research: A primer for technology education researchers.

Hoffman, A. J. (1999). Institutional evolution and change: Environmentalism and the US chemical industry. *Academy of Management Journal, 42*(4), 351-371.

Hoffmann, V. H., & Trautmann, T. (2006). *The role of industry and uncertainty in regulatory pressure and environmental strategy.* Paper presented at the Academy of Management Proceedings.

Homans, G. C. (1974). Social behavior: Its elementary forms.(Revised ed.).

Hsu, C., Lee, J.-N., & Straub, D. W. (2012). Institutional influences on information systems security innovations. *Information systems research, 23*(3-part-2), 918-939.

Hsu, S.-H., Chen, W.-H., & Hsieh, M.-J. (2006). Robustness testing of PLS, LISREL, EQS and ANN-based SEM for measuring customer satisfaction. *Total Quality Management & Business Excellence, 17*(3), 355-372.

Hu, Q., Hart, P., & Cooke, D. (2007). The role of external and internal influences on information systems security–a neo-institutional perspective. *The Journal of Strategic Information Systems, 16*(2), 153-172.

Huang, D.-L., Patrick Rau, P.-L., Salvendy, G., Gao, F., & Zhou, J. (2011). Factors affecting perception of information security and their impacts on IT adoption and security practices. *International Journal of Human-Computer Studies, 69*(12), 870-883.

Huddy, L., Feldman, S., Capelos, T., & Provost, C. (2002). The consequences of terrorism: Disentangling the effects of personal and national threat. *Political Psychology, 23*(3), 485-509.

Hui, I., Li, C., & Lau, H. (2003). Hierarchical environmental impact evaluation of a process in printed circuit board manufacturing. *International journal of production research, 41*(6), 1149-1165.

Huibin, S., & Yuan, L. (2014). Inter-Organizational Service Delivery in Chinese Hospital Industry: A Social Exchange Perspective. *Canadian Social Science, 10*(6), 64-73.

Hulland, J. (1999). Use of partial least squares (PLS) in strategic management research: a review of four recent studies. *Strategic management journal, 20*(2), 195-204.

Hwang, M.-S., Chong, S.-K., & Chen, T.-Y. (2010). DoS-resistant ID-based password authentication scheme using smart cards. *Journal of Systems and Software, 83*(1), 163-172.

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.

Ireland, R. D., & Webb, J. W. (2007). A multi-theoretic perspective on trust and power in strategic supply chains. *Journal of Operations Management, 25*(2), 482-497.

Iriondo, J. M., Albert, M. a. J., & Escudero, A. (2003). Structural equation modelling: an alternative for assessing causal relationships in threatened plant populations. *Biological Conservation, 113*(3), 367-377.

Jacobs, D. (1974). Dependency and vulnerability: An exchange approach to the control of organizations. *Administrative Science Quarterly, 19*(1), 45-59.

Jai-Yeol, S. (2011). Out of fear or desire? Toward a better understanding of employees' motivation to follow IS security policies. *Information & Management, 48*(7), 296-302.

Jarvenpaa, S. L., & Staples, D. S. (2000). The use of collaborative electronic media for information sharing: an exploratory study of determinants. *The Journal of Strategic Information Systems, 9*(2), 129-154.

Jarvis, C. B., MacKenzie, S. B., & Podsakoff, P. M. (2003). A critical review of construct indicators and measurement model misspecification in marketing and consumer research. *Journal of Consumer Research, 30*(2), 199-218.

Johanson, J., & Mattsson, L.-G. (1987). Interorganizational relations in industrial systems: a network approach compared with the transaction-cost approach. *International Studies of Management & Organization, 17*(1), 34-48.

Johnson, A. M. (2009). Business and security executives views of information security investment drivers: Results from a delphi study. *Journal of Information Privacy and Security, 5*(1), 3-27.

Johnson, M. L., Huggins, D. G., & DeNoyelles Jr, F. (1991). Ecosystem modeling with LISREL: a new approach for measuring direct and indirect effects. *Ecological Applications, 1*(4), 383-398.

Johnson, R. B., & Onwuegbuzie, A. J. (2004). Mixed methods research: A research paradigm whose time has come. *Educational researcher, 33*(7), 14-26.

Johnston, A. C., & Warkentin, M. (2010). Fear appeals and information security behaviors: An empirical study. [Article]. *MIS Quarterly, 34*(3), 549-A544.

Johnston, A. C., Warkentin, M., & Siponen, M. (2015). An enhanced fear appeal rhetorical framework: Leveraging threats to the human asset through sanctioning rhetoric. *Mis Quarterly, 39*(1), 113-134.

Kagan, R. A., Gunningham, N., & Thornton, D. (2003). Explaining corporate environmental performance: how does regulation matter? *Law & Society Review, 37*(1), 51-90.

Ke, W., Liu, H., Wei, K. K., Gu, J., & Chen, H. (2009). How do mediated and non-mediated power affect electronic supply chain management system adoption? The mediating effects of trust and institutional pressures. *Decision Support Systems, 46*(4), 839-851.

Ke, W., & Wei, K.-K. (2008). Trust and power influences in supply chain collaboration *Supply Chain Analysis* (pp. 223-239): Springer.

Keohane, R. O. (1986). Reciprocity in international relations. *International organization, 40*(01), 1-27.

Khalifa, M., & Liu, V. (2007). Online consumer retention: contingent effects of online shopping habit and online shopping experience. *European Journal of Information Systems, 16*(6), 780-792.

Khansa, L., & Liginlal, D. (2012). Whither information security? Examining the complementarities and substitutive effects among IT and information security firms. *International Journal of Information Management, 32*(3), 271-281.

Kingsolver, J. G., & Schemske, D. W. (1991). Path analyses of selection. *Trends in ecology & evolution, 6*(9), 276-280.

Komodromos, M. (2014). Employees' Perceptions of Trust, Fairness, and the Management of Change in Three Private Universities in Cyprus. *Journal of Human Resources, 2*(2), 35-54.

Kostova, T., & Roth, K. (2002). Adoption of an organizational practice by subsidiaries of multinational corporations: Institutional and relational effects. *Academy of management journal, 45*(1), 215-233.

Kotulic, A. G., & Clark, J. G. (2004). Why there aren't more information security research studies. *Information & Management, 41*(5), 597-607.

Kuber, R., & Yu, W. (2010). Feasibility study of tactile-based authentication. *International Journal of Human-Computer Studies, 68*(3), 158-181.

Lamertz, K. (2002). The social construction of fairness: Social influence and sense making in organizations. *Journal of Organizational Behavior, 23*(1), 19-37.

Lapinski, M. K., & Rimal, R. N. (2005). An explication of social norms. *Communication Theory, 15*(2), 127-147.

Lavastre, O., Gunasekaran, A., & Spalanzani, A. (2012). Supply Chain Risk Management in French companies. *Decision Support Systems, 52*(4), 828-838.

Lawrence, T. B., Winn, M. I., & Jennings, P. D. (2001). The temporal dynamics of institutionalization. *Academy of management review, 26*(4), 624-644.

Lee, & Wolfe, M. (2003). Supply chain security without tears. [Article]. *Supply Chain Management Review, 7*(1), 12-20.

Lee, H. L., & Whang, S. (2005). Higher supply chain security with lower cost: Lessons from total quality management. *International Journal of Production Economics, 96*(3), 289-300.

Lee, J., Palekar, U. S., & Qualls, W. (2011). Supply chain efficiency and security: Coordination for collaborative investment in technology. *European Journal of Operational Research, 210*(3), 568-578.

Lee, J., & Rao, H. R. (2007). *Exploring the causes and effects of inter-agency information sharing systems adoption in the anti/counter-terrorism and disaster management domains.* Paper presented at the Proceedings of the 8th annual international conference on Digital government research: bridging disciplines & domains, Philadelphia, Pennsylvania, USA.

Lee, Y. J., Kauffman, R. J., & Sougstad, R. (2011). Profit-maximizing firm investments in customer information security. *Decision Support Systems*, *51*(4), 904-920.

Lerman, J. (1996). Study design in clinical research: sample size estimation and power analysis. *Canadian journal of anaesthesia*, *43*(2), 184-191.

Leventhal, G. (1976a). What should be done with equity theory? New approachs to the study of fairness in social relationships. 1976. *Social Exchange: advances in theory and research. New York: Plenum*.

Leventhal, G. S. (1976b). The distribution of rewards and resources in groups and organizations. *Advances in experimental social psychology*, *9*, 91-131.

Levina, N., & Vaast, E. (2005). The emergence of boundary spanning competence in practice: implications for implementation and use of information systems. *MIS quarterly*, *29*(2), 335-363.

Levinson, A. (1996). Environmental regulations and industry location: international and domestic evidence. *Fair Trade and Harmonization: prerequisites for free trade*, *1*, 429-457.

Levitt, B., & March, J. G. (1988). Organizational learning. *Annual review of sociology*, *14*, 319-340.

Li, H., Zhang, J., & Sarathy, R. (2010). Understanding compliance with internet use policy from the perspective of rational choice theory. *Decision Support Systems*, *48*(4), 635-645.

Li, J., Sikora, R., Shaw, M. J., & Woo Tan, G. (2006). A strategic analysis of inter organizational information sharing. *Decision Support Systems*, *42*(1), 251-266.

Li, S., & Lin, B. (2006). Accessing information sharing and information quality in supply chain management. *Decision Support Systems*, *42*(3), 1641-1656.

Li, Y., Li, J., & Cai, Z. (2014). The timing of market entry and firm performance: A perspective of institutional theory. *Industrial Marketing Management*, *43*(5), 754-759.

Liang, H., Saraf, N., Hu, Q., & Xue, Y. (2007). Assimilation of enterprise systems: The effect of institutional pressures and the mediating role of top management. *MIS Quarterly*, *31*(1), 59-87.

Liao, Q., Luo, X., Gurung, A., & Li, L. (2009). Workplace management and employee misuse: Does punishment matter? *The Journal of Computer Information Systems*, *50*(2), 49-59.

Lili, S., Srivastava, R. P., & Mock, T. J. (2006). An Information Systems Security Risk Assessment Model Under the Dempster-Shafer Theory of Belief Functions. [Article]. *Journal of Management Information Systems, 22*(4), 109-142.

Lim, D., & Palvia, P. C. (2001). EDI in strategic supply chain: impact on customer service. *International Journal of Information Management, 21*(3), 193-211.

Lind, E. A., & Van den Bos, K. (2002). When fairness works: Toward a general theory of uncertainty management. *Research in organizational behavior, 24*, 181-223.

Loch, K. D., Carr, H. H., & Warkentin, M. E. (1992). Threats to Information Systems: Today's Reality, Yesterday's Understanding. [Article]. *MIS Quarterly, 16*(2), 173-186.

Lu, T., Guo, X., Xu, B., Zhao, L., Peng, Y., & Yang, H. (2013). *Next Big Thing in Big Data: The Security of the ICT Supply Chain.* Paper presented at the Social Computing (SocialCom), 2013 International Conference on, Alexandria, VA.

Luckenbill, D. F. (1982). Compliance under threat of severe punishment. *Social Forces, 60*(3), 811-825.

Malhotra, M. K., & Grover, V. (1998). An assessment of survey research in POM: from constructs to theory. *Journal of operations management, 16*(4), 407-425.

Maloni, M., & Benton, W. (2000). Power influences in the supply chain. *Journal of Business Logistics, 21*(1), 49-74.

Marucheck, A., Greis, N., Mena, C., & Cai, L. (2011). Product safety and security in the global supply chain: Issues, challenges and research opportunities. *Journal of Operations Management, 29*(7), 707-720.

Masterson, S. S., Lewis, K., Goldman, B. M., & Taylor, M. S. (2000). Integrating justice and social exchange: The differing effects of fair procedures and treatment on work relationships. *Academy of Management Journal, 43*(4), 738-748.

Maurer, I. (2010). How to build trust in inter-organizational projects: the impact of project staffing and project rewards on the formation of trust, knowledge acquisition and product innovation. *International Journal of Project Management, 28*(7), 629-637.

Maxion, R. A., & Reeder, R. W. (2005). Improving user-interface dependability through mitigation of human error. *International Journal of Human-Computer Studies, 63*(1-2), 25-50.

Meares, T. L., & Kahan, D. M. (1998). Law and (norms of) order in the inner city. *Law and Society Review, 32*(4), 805-838.

Mei, Z., & Dinwoodie, J. (2005). Electronic shipping documentation in China's international supply chains. *Supply Chain Management: An International Journal, 10*(3), 198-205.

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

Milhaupt, C. J. (2001). Creative norm destruction: The evolution of nonlegal rules in Japanese corporate governance. *University of Pennsylvania Law Review, 149*(6), 2083-2129.

Mizruchi, M. S., & Fein, L. C. (1999). The social construction of organizational knowledge: A study of the uses of coercive, mimetic, and normative isomorphism. *Administrative science quarterly, 44*(4), 653-683.

Molm, L. D. (1991). Affect and social exchange: Satisfaction in power-dependence relations. *American Sociological Review, 56*(4), 475-493.

Molm, L. D. (1994). Dependence and risk: Transforming the structure of social exchange. *Social Psychology Quarterly, 57*(3), 163-176.

Molm, L. D., Schaefer, D. R., & Collett, J. L. (2007). The value of reciprocity. *Social Psychology Quarterly, 70*(2), 199-217.

Morris, M. G., & Venkatesh, V. (2000). Age differences in technology adoption decisions: Implications for a changing work force. *Personnel psychology, 53*(2), 375-403.

Morris, M. G., & Venkatesh, V. (2010). Job characteristics and job satisfaction: understanding the role of enterprise resource. *MIS Quarterly, 34*(1), 143-161.

Morse, J., Barret, 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.

Morse, J. M., Barrett, M., Mayan, M., Olson, K., & Spiers, J. (2008). Verification strategies for establishing reliability and validity in qualitative research. *International journal of qualitative methods, 1*(2), 13-22.

Morse, J. M., & Mitcham, C. (2008). Exploring Qualitatively-derived Concepts: Inductive—Deductive Pitfalls. *International Journal of Qualitative Methods, 1*(4), 28-35.

Mouratidis, H., & Giorgini, P. (2007). Security Attack Testing (SAT)—testing the security of information systems at design time. *Information Systems, 32*(8), 1166-1183.

Mouratidis, H., Giorgini, P., & Manson, G. (2005). When security meets software engineering: a case of modelling secure information systems. *Information Systems, 30*(8), 609-629.

Mowery, D., & Rosenberg, N. (1979). The influence of market demand upon innovation: a critical review of some recent empirical studies. *Research Policy, 8*(2), 102-153.

Myers, M. D., & Newman, M. (2007). The qualitative interview in IS research: Examining the craft. *Information and organization, 17*(1), 2-26.

Myyry, L., Siponen, M., Pahnila, S., Vartiainen, T., & Vance, A. (2009). What levels of moral reasoning and values explain adherence to information security rules[quest] An empirical study. *European Journal of Information Systems, 18*(2), 126-139.

Nagelkerke, N. J. (1991). A note on a general definition of the coefficient of determination. *Biometrika, 78*(3), 691-692.

Narasimhan, R., Nair, A., Griffith, D. A., Arlbjørn, J. S., & Bendoly, E. (2009). Lock-in situations in supply chains: A social exchange theoretic study of sourcing arrangements in buyer–supplier relationships. *Journal of Operations Management, 27*(5), 374-389.

Ng, B.-Y., Kankanhalli, A., & Xu, Y. (2009). Studying users' computer security behavior: A health belief perspective. *Decision Support Systems, 46*(4), 815-825.

Nidjham, M. (2012). *Common Assessment and Analysis of risk in global supply chains, CASSANDRA.*

Niederman, F., Brancheau, J. C., & Wetherbe, J. C. (1991). Information systems management issues for the 1990s. *MIS Quarterly, 15*(4), 475-500.

Nissen, M. E. (2001). Agent-based supply chain integration. *Information Technology and Management, 2*(3), 289-312.

Oliver, C. (1997). Sustainable competitive advantage: Combining institutional and resource-based views. *Strategic management journal, 18*(9), 697-713.

Onwuegbuzie, A. J., & Collins, K. M. (2007). A Typology of Mixed Methods Sampling Designs in Social Science Research. *Qualitative Report, 12*(2), 281-316.

Onwuegbuzie, A. J., & Teddlie, C. (2003). A framework for analyzing data in mixed methods research. *Handbook of mixed methods in social and behavioral research*, 351-383.

Osarenkhoe, A. (2010). A study of inter-firm dynamics between competition and cooperation–A coopetition strategy. *Journal of Database Marketing & Customer Strategy Management, 17*(3), 201-221.

Pahnila, S., Siponen, M., & Mahmood, A. (2007). *Employees' behavior towards IS security policy compliance.* Paper presented at the System Sciences, 2007. HICSS 2007. 40th Annual Hawaii International Conference on.

Palincsar, A. S. (1986). The role of dialogue in providing scaffolded instruction. *Educational psychologist, 21*(1-2), 73-98.

Perrow, C. (1974). Is business really changing? *Organizational Dynamics, 3*(1), 31-44.

Pinder, P. (2006). Preparing Information Security for legal and regulatory compliance (Sarbanes–Oxley and Basel II). *Information Security Technical Report, 11*(1), 32-38.

Png, I. P. L., & Wang, Q.-H. (2009). Information Security: Facilitating User Precautions Vis-à-Vis Enforcement Against Attackers. [Article]. *Journal of Management Information Systems, 26*(2), 97-121.

Podsakoff, P. M., MacKenzie, S. B., Lee, J.-Y., & Podsakoff, N. P. (2003). Common method biases in behavioral research: a critical review of the literature and recommended remedies. *Journal of applied psychology, 88*(5), 879.

Podsakoff, P. M., & Organ, D. W. (1986). Self-reports in organizational research: Problems and prospects. *Journal of Management, 12*(4), 531-544.

Poksinska, B., Dahlgaard, J. J., & Eklund, J. A. (2003). Implementing ISO 14000 in Sweden: motives, benefits and comparisons with ISO 9000. *International Journal of Quality & Reliability Management, 20*(5), 585-606.

Polkinghorne, D. E. (2005). Language and meaning: Data collection in qualitative research. *Journal of Counseling Psychology, 52*(2), 137.

Porter, L. W., & Lawler, E. E. (1968). *Managerial attitudes and performance*. IL: Richard D.Irwin, Inc

Posey, C., Bennett, R. J., & Roberts, T. L. (2011). Understanding the mindset of the abusive insider: An examination of insiders' causal reasoning following internal security changes. *Computers & Security, 30*(6-7), 486-497.

Posey, C., Roberts, T. L., Lowry, P. B., & Hightower, R. T. (2014). Bridging the Divide: A Qualitative Comparison of Information Security Thought Patterns between Information Security Professionals and Ordinary Organizational Insiders. *Information & management*.

Posthumus, S., & Von Solms, R. (2004). A framework for the governance of information security. *Computers & Security, 23*(8), 638-646.

Princely, I. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers & Security, 31*(1), 83-95.

Provan, K. G., Beyer, J. M., & Kruytbosch, C. (1980). Environmental linkages and power in resource-dependence relations between organizations. *Administrative Science Quarterly, 25*(2), 200-225.

Puhakainen, P., & Siponen, M. (2010). Improving employee's compliance through information systems security training: An action research study. [Article]. *MIS Quarterly, 34*(4), 767-A764.

Ramsay, H., Scholarios, D., & Harley, B. (2000). Employees and High-Performance Work Systems: Testing inside the Black Box. *British Journal of industrial relations, 38*(4), 501-531.

Ransbotham, S., & Mitra, S. (2009). Choice and Chance: A Conceptual Model of Paths to Information Security Compromise. [Article]. *Information Systems Research, 20*(1), 121-139.

Rapley, T. J. (2001). The art (fulness) of open-ended interviewing: some considerations on analysing interviews. *Qualitative research, 1*(3), 303-323.

Ratnasingam, P. (2005). Trust in inter-organizational exchanges: a case study in business to business electronic commerce. *Decision Support Systems, 39*(3), 525-544.

Rees, L. P., Deane, J. K., Rakes, T. R., & Baker, W. H. (2011). Decision support for Cybersecurity risk planning. *Decision Support Systems, 51*(3), 493-505.

Richardson, R. (2008). CSI computer crime and security survey. *Computer Security Institute, 1*, 1-30.

Rimal, R. N., & Real, K. (2003). Understanding the influence of perceived norms on behaviors. *Communication Theory, 13*(2), 184-203.

Rimal, R. N., & Real, K. (2005). How behaviors are influenced by perceived norms a test of the theory of normative social behavior. *Communication Research, 32*(3), 389-414.

Ringle, C., Sarstedt, M., & Straub, D. (2012). A Critical Look at the Use of PLS-SEM in MIS Quarterly. *MIS Quarterly (MISQ), 36*(1).

Robert, W. (2006). Understanding the perpetration of employee computer crime in the organisational context. *Information and Organization, 16*(4), 304-324.

Rodríguez, C. M., & Wilson, D. T. (2002). Relationship bonding and trust as a foundation for commitment in US-Mexican strategic alliances: A structural equation modeling approach. *Journal of International Marketing, 10*(4), 53-76.

Romero, J. (2003). Prevention of Maritime Terrorism: The Container Security Initiative. *Chicago Journal of International Law, 4*, 597.

Ropohl, G. (1999). Philosophy of socio-technical systems. *Techné: Research in Philosophy and Technology, 4*(3), 186-194.

Roth, V., Straub, T., & Richter, K. (2005). Security and usability engineering with particular attention to electronic mail. *International Journal of Human-Computer Studies, 63*(1-2), 51-73.

Russell, D. M., & Saldanha, J. P. (2003). Five tenets of security-aware logistics and supply chain operation. *Transportation Journal, 42*(4), 44-54.

Ryan, S. D., & Bordoloi, B. (1997). Evaluating security threats in mainframe and client/server environments. *Information & Management, 32*(3), 137-146.

Saba, F., & Shearer, R. L. (1994). Verifying key theoretical concepts in a dynamic model of distance education. *American Journal of Distance Education, 8*(1), 36-59.

Sandelowski, M. (2000). Focus on Research Methods Combining Qualitative and Quantitative Sampling, Data Collection, and Analysis Techniques. *Research in nursing & health, 23*, 246-255.

Sarathy, R. (2006). Security and the global supply chain. *Transportation Journal, 45*(4), 28-51.

Schatzman, L., & Strauss, A. L. (1973). *Field research: Strategies for a natural sociology*: Prentice-Hall Englewood Cliffs, NJ.

Scheepers, P., Gijsberts, M., & Coenders, M. (2002). Ethnic exclusionism in European countries. Public opposition to civil rights for legal migrants as a response to perceived ethnic threat. *European sociological review, 18*(1), 17-34.

Schmitt, N., & Stults, D. M. (1985). Factors defined by negatively keyed items: The result of careless respondents? *Applied Psychological Measurement, 9*(4), 367-373.

Schopler, J. H. (1987). Interorganizational groups: Origins, structure, and outcomes. *Academy of management review, 12*(4), 702-718.

Scott, W. R. (1987). The adolescence of institutional theory. *Administrative science quarterly, 32*(4), 493-511.

Scott, W. R. (1995). *Institutions and organizations*. California: Thousand Oaks.

Scott, W. R., & Meyer, J. W. (1982). *The organization of societal sectors*.

Senbel, M., Ngo, V. D., & Blair, E. (2014). Social mobilization of climate change: University students conserving energy through multiple pathways for peer engagement. *Journal of Environmental Psychology, 38*, 84-93.

Settoon, R. P., Bennett, N., & Liden, R. C. (1996). Social exchange in organizations: Perceived organizational support, leader–member exchange, and employee reciprocity. *Journal of applied psychology, 81*(3), 219.

Shafiu, I., Wang, W. Y. C., & Singh, H. (2014). Mixed Method for New Scholars with Intrusive, Emerging and Complex Socio-Technical Topics *Knowledge Management in Organizations* (pp. 255-266): Springer.

Sheffi, Y. (1990). Third party logistics--present and future prospects. *Journal of Business Logistics, 11*(2).

Sheffi, Y. (2001). Supply chain management under the threat of international terrorism. *International Journal of Logistics Management, The, 12*(2), 1-11.

Sheu, C., Lee, L., & Niehoff, B. (2006). A voluntary logistics security program and international supply chain partnership. *Supply Chain Management, 11*(4), 363-374.

Shing, M.-L., Lee, H., & Shing, C.-C. (2014). Modeling in confidentiality and integrity for a supply chain network. *Communications of the IIMA, 7*(1), 4.

Siponen, M., Adam Mahmood, M., & Pahnila, S. (2014). Employees' adherence to information security policies: An exploratory field study. *Information & management, 51*(2), 217-224.

Siponen, M., & Vance, A. (2010). Neutralization: New insights into the problem of employee information systems security policy violations. [Article]. *MIS Quarterly, 34*(3), 487-A412.

Siponen, M., & Willison, R. (2009). Information security management standards: Problems and solutions. *Information & Management, 46*(5), 267-270.

Siponen, M. T., & Oinas-Kukkonen, H. (2007). A review of information security issues and respective research contributions. *ACM Sigmis Database, 38*(1), 60-80.

Smith, G., Watson, K., Baker, W., & Pokorski, J. (2007). A critical balance: collaboration and security in the IT-enabled supply chain. *International journal of production research, 45*(11), 2595-2613.

Smith, S., Winchester, D., Bunker, D., & Jamieson, R. (2010). Circuits of power: A study of mandated compliance to an information systems security de jure standard in a government organization. [Article]. *MIS Quarterly, 34*(3), 463-486.

Spears, J. L., & Barki, H. (2010). User participation in information systems security risk management. [Article]. *MIS Quarterly, 34*(3), 503-A505.

Spears, J. L., Barki, H., & Barton, R. R. (2013). Theorizing the concept and role of assurance in information systems security. *Information & management, 50*(7), 598-605.

Stanton, J. M., Stam, K. R., Mastrangelo, P., & Jolton, J. (2005). Analysis of end user security behaviors. *Computers & Security, 24*(2), 124-133.

Stevens, J. M., Kevin Steensma, H., Harrison, D. A., & Cochran, P. L. (2005). Symbolic or substantive document? The influence of ethics codes on financial executives' decisions. *Strategic Management Journal, 26*(2), 181-195.

Straub, D. W. (1989). Validating Instruments in MIS Research. [Article]. *MIS Quarterly, 13*(2), 147-169.

Straub, D. W., & Welke, R. J. (1998). Coping With Systems Risk: Security Planning Models for Management Decision Making. [Article]. *MIS Quarterly, 22*(4), 441-469.

Straub, J. D. W., & Nance, W. D. (1990). Discovering and Disciplining Computer Abuse in Organizations: A Field Study. [Article]. *MIS Quarterly, 14*(1), 45-60.

Straub Jr, D. W. (1990). Effective IS Security: An Empirical Study. [Article]. *Information Systems Research, 1*(3), 255-276.

Tarasewich, P., Gong, J., & Conlan, R. (2006). *Protecting private data in public.* Paper presented at the CHI'06 Extended Abstracts on Human Factors in Computing Systems.

Tenenhaus, M., Vinzi, V. E., Chatelin, Y.-M., & Lauro, C. (2005). PLS path modeling. *Computational statistics & data analysis, 48*(1), 159-205.

Theoharidou, M., Kokolakis, S., Karyda, M., & Kiountouzis, E. (2005). The insider threat to information systems and the effectiveness of ISO17799. *Computers & Security, 24*(6), 472-484.

Thibault, M., Brooks, M. R., & Button, K. J. (2006). The response of the U.S. Maritime Industry to the new container security initiatives. *Transportation Journal, 45*(1), 5-15.

Thibaut, J. W., & Kelley, H. H. (1959). *The social psychology of groups*. Oxford, England: John Wiley.

Thomas, D. R. (2006). A general inductive approach for analyzing qualitative evaluation data. *American Journal of Evaluation, 27*(2), 237-246.

Thorelli, H. B. (1986). Networks: between markets and hierarchies. *Strategic management journal, 7*(1), 37-51.

Tokman, M., Richey, R. G., Marino, L. D., & Weaver, K. M. (2007). Exploration, exploitation and satisfaction in supply chain portfolio strategy. *Journal of Business Logistics, 28*(1), 25-56.

Tolbert, P. S., & Zucker, L. G. (1999). The institutionalization of institutional theory. *Studying Organization. Theory & Method. London, Thousand Oaks, New Delhi*, 169-184.

Toosi, A. N., Calheiros, R. N., & Buyya, R. (2014). Interconnected Cloud Computing Environments: Challenges, Taxonomy, and Survey. *ACM Computing Surveys (CSUR), 47*(1), 7.

Trkman, P., McCormack, K., de Oliveira, M. P. V., & Ladeira, M. B. (2010). The impact of business analytics on supply chain performance. *Decision Support Systems, 49*(3), 318-327.

Tsamenyi, M., Cullen, J., & González, J. M. G. (2006). Changes in accounting and financial information system in a Spanish electricity company: A new institutional theory analysis. *Management Accounting Research, 17*(4), 409-432.

Turker, D. (2014). Analyzing relational sources of power at the interorganizational communication system. *European Management Journal, 32*(3), 509-517.

Union, T. a. C. (2014). Security cooperation with third countries. *Taxation and Customs Union*, from http://ec.europa.eu/taxation_customs/customs/policy_issues/customs_security/cooperation_3thcountries/index_en.htm

Urciuoli, L. (2010). Supply chain security—mitigation measures and a logistics multi-layered framework. *Journal of Transportation Security, 3*(1), 1-28.

van der Linden, H., Kalra, D., Hasman, A., & Talmon, J. (2009). Inter-organizational future proof EHR systems: a review of the security and privacy related issues. *International Journal of Medical Informatics, 78*(3), 141-160.

Vance, A., Siponen, M., & Pahnila, S. (2012). Motivating IS security compliance: insights from habit and protection motivation theory. *Information & Management, 49*(3), 190-198.

Venkatesh, V., Brown, S. A., & Bala, H. (2013). Bridging the qualitative-quantitative divide: Guidelines for conducting mixed methods research in information systems. *MIS quarterly, 37*(1), 21-54.

Vespignani, A. (2012). Modelling dynamical processes in complex socio-technical systems. *Nature Physics, 8*(1), 32-39.

von Solms, R., van der Haar, H., von Solms, S. H., & Caelli, W. J. (1994). A framework for information security evaluation. *Information & Management, 26*(3), 143-153.

Vu, K.-P. L., Proctor, R. W., Bhargav-Spantzel, A., Tai, B.-L., Cook, J., & Eugene Schultz, E. (2007). Improving password security and memorability to protect personal and organizational information. *International Journal of Human-Computer Studies, 65*(8), 744-757.

Wagner, S. M., Coley, L. S., & Lindemann, E. (2011). Effects of supplier's reputation on the future of buyer-supplier relationships: The mediating roles of outcome fairness and trust. *Journal of Supply Chain Management, 47*(2), 29-48.

Wainer, J., Kumar, A., & Barthelmess, P. (2007). DW-RBAC: A formal security model of delegation and revocation in workflow systems. *Information Systems, 32*(3), 365-384.

Walker, H., Di Sisto, L., & McBain, D. (2008). Drivers and barriers to environmental supply chain management practices: Lessons from the public and private sectors. *Journal of purchasing and supply management, 14*(1), 69-85.

Wallace, L. L. M. A. (2011). Information Security and Sarbanes-Oxley Compliance: An Exploratory Study. [Article]. *Journal of Information Systems, 25*(1), 185-211.

Wang, J., Gupta, M., & Raj, R. (2015). Insider Threats in a Financial Institution: Analysis of Attack-Proneness of Information Systems Applications. *Management Information Systems Quarterly, 39*(1), 91-112.

Warkentin, M., Bapna, R., & Sugumaran, V. (2001). E-knowledge networks for inter-organizational collaborative e-business. *Logistics Information Management, 14*(1/2), 149-163.

Warkentin, M., & Willison, R. (2009). Behavioral and policy issues in information systems security: the insider threat. *European Journal of Information Systems, 18*(2), 101.

Werlinger, R., Hawkey, K., Botta, D., & Beznosov, K. (2009). Security practitioners in context: Their activities and interactions with other stakeholders within organizations. *International Journal of Human-Computer Studies, 67*(7), 584-606.

Westphal, J. D., & Zajac, E. J. (1994). Substance and symbolism in ceos'long-term incentive plans. *Administrative Science Quarterly, 39*(3), 367-391.

Westphal, J. D., & Zajac, E. J. (1995). Who shall govern? CEO/board power, demographic similarity, and new director selection. *Administrative Science Quarterly, 40*(1), 60-83.

Wetzels, M., Odekerken-Schroder, G., & Van Oppen, C. (2009). Using PLS path modeling for assessing hierarchical construct models: guidelines and empirical illustration. *Management Information Systems Quarterly, 33*(1), 177-188.

Whipple, J. M., Voss, M. D., & Closs, D. J. (2009). Supply chain security practices in the food industry: Do firms operating globally and domestically differ? *International Journal of Physical Distribution and Logistics Management, 39*(7), 574-594.

Whitford, A. B. (2002). Threats, institutions and regulation in common pool resources. *Policy Sciences, 35*(2), 125-139.

Williams, K. R., & Hawkins, R. (1986). Perceptual research on general deterrence: A critical review. *Law & Society Review, 20*(4), 545-572.

Williams, Z., Jason, E. L., & Stephen, A. L. (2008). Supply chain security: an overview and research agenda. [DOI: 10.1108/09574090810895988]. *International Journal of Logistics Management, The, 19*(2), 254-281.

Williams, Z., Lueg, J. E., Taylor, R. D., & Cook, R. L. (2009). Why all the changes? An institutional theory approach to exploring the drivers of supply chain security (SCS). *International Journal of Physical Distribution and Logistics Management, 39*(7), 595-618.

Willison, R., & Warkentin, M. (2013). Beyond deterrence: an expanded view of employee computer abuse. *Mis Quarterly, 37*(1), 1-20.

Wilson, J. Q. (1974). *Political Organizations*. New York: Basic Books.

Witte, K. (1992). Putting the fear back into fear appeals: The extended parallel process model. *Communications Monographs, 59*(4), 329-349.

Wong, K. K.-K. (2013). Partial Least Squares Structural Equation Modeling (PLS-SEM) Techniques using SmartPLS. [Technical Note]. *Marketing Bulletin, 24*, 32.

Woon, I. M. Y., & Kankanhalli, A. (2007). Investigation of IS professionals' intention to practise secure development of applications. *International Journal of Human-Computer Studies, 65*(1), 29-41.

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.

Wu, D.-J. (2001). Software agents for knowledge management: coordination in multi-agent supply chains and auctions. *Expert Systems with Applications, 20*(1), 51-64.

Wu, I.-L., Chuang, C.-H., & Hsu, C.-H. (2014). Information sharing and collaborative behaviors in enabling supply chain performance: A social exchange perspective. *International Journal of Production Economics, 148*, 122-132.

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.

Yang, T.-M., & Maxwell, T. A. (2011). Information-sharing in public organizations: A literature review of interpersonal, intra-organizational and inter-organizational success factors. *Government Information Quarterly, 28*(2), 164-175.

Yang, Y.-C. (2011). Risk management of Taiwan's maritime supply chain security. *Safety Science, 49*(3), 382-393.

Yang, Y. C. (2010). Impact of the container security initiative on Taiwan's shipping industry. *Maritime Policy and Management, 37*(7), 699-722.

Yi, X., & Zhang, Y. (2009). Privacy-preserving naive Bayes classification on distributed data via semi-trusted mixers. *Information Systems, 34*(3), 371-380.

Yin, R. K. (2012). *Applications of Case Study Research* (3rd Edition ed.). London: Sage

Yue, W. T., Çakanyıldırım, M., Ryu, Y. U., & Liu, D. (2007). Network externalities, layered protection and IT security risk management. *Decision Support Systems, 44*(1), 1-16.

Zaheer, A., McEvily, B., & Perrone, V. (1998). Does trust matter? Exploring the effects of interorganizational and interpersonal trust on performance. *Organization science, 9*(2), 141-159.

Zakaria, M. S., & Janom, N. (2011). Developing and validating readiness measures of inter-organizational E-commerce on SMEs. *Journal of Internet Banking and Commerce, 16*(3), 1-15.

Zhao, X., Huo, B., Flynn, B. B., & Yeung, J. H. Y. (2008). The impact of power and relationship commitment on the integration between manufacturers and customers in a supply chain. *Journal of Operations Management, 26*(3), 368-388.

Zhu, Q., & Sarkis, J. (2007). The moderating effects of institutional pressures on emergent green supply chain practices and performance. *International Journal of Production Research, 45*(18-19), 4333-4355.

Zhuang, G., & Zhou, N. (2004). The relationship between power and dependence in marketing channels: A Chinese perspective. *European Journal of Marketing, 38*(5/6), 675-693.

Zucker, L. G. (1987). Institutional theories of organization. *Annual review of sociology, 13*, 443-464.

Zukin, S., & DiMaggio, P. (1990). *Structures of capital: The social organization of the economy*. New York: Press Syndicate of the University of Cambridge.

Appendix A. Letter of Ethical Approval

AUTEC
SECRETARIAT

7 June 2013
William Wang
Faculty of Business and Law
Dear William

Re Ethics Application: **13/114 Inter-organisational information security compliance behaviour: The case of supply chains.**

Thank you for providing evidence as requested, which satisfies the points raised by the AUT University Ethics Committee (AUTEC).

Your ethics application has been approved for three years until 7 June 2016.

As part of the ethics approval process, you are required to submit the following to AUTEC:

- A brief annual progress report using form EA2, which is available online throughhttp://www.aut.ac.nz/researchethics. When necessary this form may also be used to request an extension of the approval at least one month prior to its expiry on 7 June 2016;
- A brief report on the status of the project using form EA3, which is available online throughhttp://www.aut.ac.nz/researchethics. This report is to be submitted either when the approval expires on 7 June 2016 or on completion of the project.

It is a condition of approval that AUTEC is notified of any adverse events or if the research does not commence. AUTEC approval needs to be sought for any alteration to the research, including any alteration of or addition to any documents that are provided to participants. You are responsible for ensuring that research undertaken under this approval occurs within the parameters outlined in the approved application.

AUTEC grants ethical approval only. If you require management approval from an institution or organisation for your research, then you will need to obtain this. If your research is undertaken within a jurisdiction outside New Zealand, you will need to make the arrangements necessary to meet the legal and ethical requirements that apply there.

To enable us to provide you with efficient service, please use the application number and study title in all correspondence with us. If you have any enquiries about this application, or anything else, please do contact us at ethics@aut.ac.nz.

All the very best with your research,

Madeline Banda
Acting Executive Secretary
Auckland University of Technology Ethics Committee

Cc: Ibrahim shafiu ishafiu@aut.ac.nz

Appendix B. Quantitative Survey Instrument

Table 26: Survey instrument used for the quantitative survey

	Demography Type of Organization Age Sex: Years of experience in the Industry …….	
	Regulatory Demands 1. The local government requires our firm to be compliance	1 2 3 4 5 6 7
	2. The other related authoritative organizations (foreign Customs) requires our firm to be compliant	1 2 3 4 5 6 7
	3. Competitive conditions are linked to rules and regulations which require our firm to be compliant	1 2 3 4 5 6 7
2	**Market Influence** 1. The extent of compliance by your collaborating firms	1 2 3 4 5 6 7
	2. The extent of compliance by your customers	1 2 3 4 5 6 7
	3. The extent to which local government's promotion of information security influences your firm to be compliant	1 2 3 4 5 6 7
3	**Peer pressure** Our main competitors who are compliant 1. have greatly benefitted	1 2 3 4 5 6 7
	2. are favorably perceived by others in the same industry	1 2 3 4 5 6 7
	3. are favorably perceived by their suppliers and customers	1 2 3 4 5 6 7
4	**Perceived Norm** 1. Organizations who influence our behaviour think that we should be compliant to information security requirements	1 2 3 4 5 6 7
	2. Organizations who are important to us think that we should be compliant.	1 2 3 4 5 6 7
5	**Perceived threat**	1 2 3 4 5 6 7

	1. Organizations that follow guidelines are given preferential treatment.	
	2. The compliance practices of some threaten us who do not	1 2 3 4 5 6 7
6	**Perceived benefits** 1. Our organization believe in the benefits of complying	1 2 3 4 5 6 7
	2. Our peers believe in the benefits of complying	1 2 3 4 5 6 7
	3. Our management team believes in the benefits of complying	1 2 3 4 5 6 7
7	**Fairness** 1. Uses procedures designed to collect accurate information to appeal or challenge decisions	1 2 3 4 5 6 7
	2. Uses procedures designed to hear the concerns of all sides affected by a decision	1 2 3 4 5 6 7
	3. Employs procedures designed to provide useful feedback regarding any decision	1 2 3 4 5 6 7
	4. Allows for requests for clarification or additional information about decisions	1 2 3 4 5 6 7
	5. Suppresses their personal biases	1 2 3 4 5 6 7
	6. Deal with you in an honest and truthful manner when making decisions. 7.	1 2 3 4 5 6 7
	8. **Applies objectives and standards so that decision can be made in a consistent manner**	1 2 3 4 5 6 7
	9. Provide justifiable explanations for their decisions	1 2 3 4 5 6 7
	10. Adequately consider your viewpoint in making decisions	1 2 3 4 5 6 7
	11. **Provide timely feedback on decisions and their implications**	1 2 3 4 5 6 7
	12. Treat you with respect and dignity in making decisions	1 2 3 4 5 6 7

8	**Reciprocity (reward)** 1. Offers reciprocal incentives when we were initially reluctant to cooperate with the information security compliance program	1 2 3 4 5 6 7
	2. We feel that by going along with the compliance program we will be reciprocated (rewarded) on other occasions	1 2 3 4 5 6 7
	3. Offers rewards as reciprocity so that we will go along with their wishes	1 2 3 4 5 6 7
9	**Symbolic and Substantive compliance** 1. To what extent are the documents generated in compliance with the information security requirements or general security guidelines in daily practice?	1 2 3 4 5 6 7
	2. To what extent has the information security requirements become part of your organization's regular routine?	1 2 3 4 5 6 7
	3. To what extent are information security compliances made at the last minute before information is submitted?	1 2 3 4 5 6 7

Appendix C. SPSS Result for Harman's Single Factor Test for CMB

Total Variance Explained (Extraction Method: Principal Component Analysis)

Component	Initial Eigenvalues			Extraction Sums of Squared Loadings		
	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
1	12.795	37.633	37.633	12.795	37.633	37.633
2	4.919	14.467	52.099			
3	4.461	13.121	65.221			
4	1.858	5.465	70.685			
5	1.650	4.854	75.539			
6	1.236	3.636	79.175			
7	.862	2.535	81.710			
8	.720	2.117	83.827			
9	.645	1.897	85.724			
10	.568	1.671	87.396			
11	.521	1.533	88.929			
12	.429	1.262	90.191			
13	.418	1.229	91.420			
14	.330	.972	92.392			
15	.322	.946	93.338			
16	.310	.911	94.249			
17	.270	.793	95.042			
18	.250	.736	95.778			
19	.223	.655	96.433			
20	.182	.534	96.967			
21	.170	.499	97.466			
22	.148	.435	97.901			
23	.134	.394	98.295			
24	.122	.359	98.654			
25	.096	.281	98.936			
26	.089	.263	99.198			
27	.087	.257	99.455			
28	.073	.213	99.668			
29	.052	.153	99.821			
30	.038	.111	99.932			
31	.015	.045	99.977			
32	.008	.023	100.000			
33	3.434E-018	1.010E-017	100.000			
34	-4.028E-017	-1.185E-016	100.000			

Appendix D. Square of Loadings to examine Indicator Reliability

	Original Sample (O)	Square(O)
EXT1R <- REGULATORY	0.9638	0.9289
EXTR2 <- REGULATORY	0.8652	0.7486
EXTR3 <- REGULATORY	0.9462	0.8953
FAIR10 <- FAIRNESS	0.8795	0.7736
FAIR7 <- FAIRNESS	0.8304	0.6895
FAIR8 <- FAIRNESS	0.8810	0.7762
MARK1 <- MARKET	0.9140	0.8354
MARK2 <- MARKET	0.8602	0.7399
MARK3 <- MARKET	0.8920	0.7957
NORM1 <- NORM	0.8224	0.6763
NORM2 <- NORM	0.8830	0.7797
PBEN1 <- BENEFICIAL	0.9304	0.8656
PBEN2 <- BENEFICIAL	0.9851	0.9704
PBEN3 <- BENEFICIAL	0.9851	0.9704
PEER1 <- PEER	0.9370	0.8780
PEER2 <- PEER	0.9546	0.9113
PEER3 <- PEER	0.8698	0.7566
PTRT1 <- THREAT	0.8645	0.7474
PTRT3 <- THREAT	0.8269	0.6838
REWARD1 <- RECIPROCITY	0.9391	0.8819
REWARD2 <- RECIPROCITY	0.8324	0.6929
REWARD3 <- RECIPROCITY	0.8527	0.7271
SUB1 <- COMPLIANCE	0.9426	0.8885
SUB2 <- COMPLIANCE	0.8785	0.7718
SYB1R <- COMPLIANCE	0.9158	0.8387

Appendix E. Literature Review on SCS

Table 27: Literature review on SCS by Voss et al. (2012)

Author(s)	Journal	Research Type	Focus of Study
Autry & Bobbit *(2008)* *Supply Chain Orientation: Conceptual Development and a Proposed Framework*	International Journal of Logistics Management	Qualitative	Proposes a conceptual framework for Supply Chain Security Orientation and its antecedents
Chopra & Sodhi (2009) *Managing Risk to avoid supply chain Breakdown*	Sloan Management Review	Conceptual	Proposed categories and drivers of risk and associated risk mitigation strategies
Christopher & Lee (2005) *Mitigating Supply Chain Risk Through Improved Confidence*	International Journal of Physical Distribution & Logistics Management	Conceptual	Discussed the concept of a risk spiral that can be mitigated if supply chain confidence is increased through visibility and control
Closs et al. (2008) *A Framework for Protecting your supply chain*	Supply Chain Management Review	Qualitative	Proposed ten security competencies and an associated supply chain security framework
Craighead et al. (2000) *The Severity of Supply Chain disruptions: design characteristics and Mitigation capabilities*	Decision Sciences	Qualitative	Developed six propositions examining the impact of supply chain design characteristics on the severity of a disruption and the impact of mitigation capabilities

Author(s)	Journal	Research Type	Focus of Study
Elkins et al. (2007) *18 Ways to guard against disruptions*	Supply Chain Management Review	Qualitative	Created a list of best practices to improving supply chain resiliency and risk management approaches
Guinipero & Eltantaway (1979) *Securing the Upstream Supply Chain: A Risk Management Approach."*	International Journal of Physical Distribution and Logistics Management	Conceptual	Develop propositions regarding four situational factors that influence risk management strategies
Hale & Moberg (1998) *Improving Supply Chain Disaster Preparedness: A Decision Process for Secure Site*	International Journal of Physical Distribution and Logistics Management	Conceptual	Proposed a decision making model based on location science, for secure site location
Harland et al. (2003) *Risk in Supply Networks*	Journal of Purchasing and Supply Management	Conceptual & Qualitative	Defined and classified types of risk and uses case studies to develop a conceptual risk tool
Kleindorfer & Saad (2005) *Managing Disruption Risks in Supply Chains*	Production and Operations Management	Conceptual & Qualitative	Proposed a framework for disruption risk management and security in global supply chains and used secondary data of chemical accidents to discuss implication for designing risk management systems.
Manuj & Mentzer (2010) *Global Supply Chain Risk Management Strategies*	International Journal of Physical Distribution and Logistics Management	Qualitative	Examined risk management and proposed a model of global chain risk management strategies

Author(s)	Journal	Research Type	Focus of Study
Peleg-Gilla et al. (1979) *Innovators in Supply Chain Security: Better Security Drives Business Value*	The Manufacturing Institute: The Manufacturing Innovation Series	Qualitative and Quantitative	Examined firms investments in supply chain security and the impacts of those investments on business performance and resulting benefits
Rice & Caniato (2003) *Building a Secure and Resilient Supply Network*	Supply Chain Management Review	Qualitative	Classified supply chain security initiatives from Basic to Advanced
Roth et al. (2008) *Unraveling the Food Supply Chain: Strategic Insights from China and the 2007 Recalls*	Journal of Supply Chain Management	Conceptual	Examined the six T's of supply chain quality management
Russel & Saldanha (2003) *Five Tenets of Security-Aware Logistics and Supply Chain Operation*	Transportation Journal *Does not use the term SCS	Conceptual	Discussed the five tenets of security aware logistics supply chain operations
Sarathy (2006) *Security and the Global Supply Chain."*	Transportation Journal	Conceptual	Identified security vulnerabilities across the supply chain and firm level strategies for developing secure supply chains
Sheffi (2001) *Supply Chain Management Under the Threat of Imitational Terrorism*	International Journal of Physical Distribution and Logistics Management	Conceptual	Examined corporate challenges of dealing with the threat of terrorism and operating in an environment of increased security
Sheffi & Rice (2005) *A Supply Chain View of the Resilient Enterprise*	Sloan Management Review	Qualitative	Proposed a framework of stages of disruptions as well as vulnerability maps

Author(s)	**Journal**	**Research Type**	**Focus of Study**
Speckman & Davis (2004) *Risky Business: Expanding the Discussion on Risk and the Extended Enterprise*	International Journal of Physical Distribution and Logistics Management	Conceptual	Explored the types of extended enterprises- related risks in a supply chain
Zsidisn & Smith (2005) *Managing Supply Risk with Early Supplier Involvement: A Case Study and Research Propositions*	Journal of Supply Chain Management	Qualitative	Case study examining the impact of early supplier involvement
Zsidisin et al. (2014) *An Analysis of Supply Risk Assessment Techniques*	International Journal of Physical Distribution and Logistics Management	Qualitative	Explored risk management and risk assessment techniques

Table 28: Literature Review by (Williams, et al., 2008)

Author(s)	Journal	Nature of study	Focus on	Findings and/or conclusions
Intra-organizational Hale & Moberg (2005) *Improving supply chain disaster preparedness: a decision process for secure site selection*	International Journal of Physical Distribution & Logistics Management	Conceptual	The location of critical supplies in preparation for supply chain disasters	Suggests that location science can lead to optimized locations for secure locations for critical supplies during disaster
Giunipero & Eltantawy (2004) *Securing the upstream supply chain: a risk management approach*	International Journal of Physical Distribution & Logistics Management	Conceptual	Situational factors that impact the level of risk management activities	Coordinated efforts are needed with the supply base in order to mitigate risk and create SCS.
Prokop (2004) *Smart and safe borders: the logistics of inbound cargo security*	The International Journal of Logistics Management	Conceptual	Governmental security measures for inbound cargo to the USA	True cross-border security is not the responsibility of the government; it is the responsibility of the supply chain partners
Rinehart et al. (2004) *Supplier relationships: the impact on security*	Supply Chain Management Review	Conceptual	Developing secure supplier relationships	Different supplier relationships require different security efforts

Author(s)	Journal	Nature of study	Focus on	Findings and/or conclusions
Banomyong (2005) *The impact of port and trade security initiatives on maritime supply chain management*	Maritime Policy and Management	Conceptual	Understanding the impact of new government programs on maritime supply chains	There should be organizational benefits, such as reduced transport costs, from investing in maritime security efforts
Sawhney & Sumukudas (2005) *Coping with customs clearance uncertainties in global sourcing*	International Journal of Physical Distribution & Logistics Management	Qualitative	Interactions between competitor firms for risk reduction and abiding by governmental regulations	Buyer-buyer relationships may be required to reduce supply chain risk
Zsidisin et al. (2005) *The dark side of supply chain management*	Supply Chain Management Review	Conceptual	Lean supply chains can be at higher risk	Supply continuity planning can lead to reduced risk. Quick response to disasters is needed
Combination Sheffi (2001) Sheffi & Rice (1990) *A supply chain view of the resilient enterprise*	MIT Sloan Management Review	Conceptual	Challenges of dealing with disasters and operating in a security focused environment	Security will take much effort, including: working with the government, prevention measures, creating redundancies, and changing organizational processes for security
Martha & Subbakrishna (2002) *Targeting a just-in-case supply chain for the inevitable next disaster*	Supply Chain Management Review	Conceptual	The need for supply chain redesign for disasters	Risk needs to be mitigated throughout the supply chain because disasters are unpredictable

Author(s)	Journal	Nature of study	Focus on	Findings and/or conclusions
Helferich & Cook (2002) *Securing the supply chain*	Council of logistics management	Conceptual	Present framework for supply chain plans for prevention and response to disasters	Organizations should plan for disasters using proven planning guides, such as the FEMA approach
Sheffi (2002) *Supply chains and terrorism, The Towers Lost and Beyond*,	A Collection of Essays on the WTC, Massachusetts Institute of Technology Available at: http://web.mit.edu/civenv/wtc/	Conceptual	New challenges for supply chain management after the terrorist attacks on 9/11	Many trade-offs and decisions have to be made for SCS. Suggests the adoption of a chief security officer and security minded culture
Knight (2003) *Supply chain security guidelines*	White Paper, IBM, available at: www.ibm.com	Conceptual	Guidelines for SCS gathered from many government agencies	More collaboration on security is needed; firms cannot approach security with the "four-walls" approach
Lee & Wolf (2003) *Supply chain security without tears*	Supply Chain Management Review	Conceptual	Using TQM philosophy for SCS	TQM philosophy applied to SCS can lead to efficiency, effectiveness, and mitigates risk
Quinn (2003) *Security matters*	Supply Chain Management Review,	Qualitative	Discussion of loss prevention and security programs	SCS can lead to profitability
Rice & Caniato (2005) *Building a secure and resilient supply network*	Supply Chain Management Review	Qualitative	Understanding how supply chains have responded to the threat of global terrorism	SCS and resiliency have been created by organizations through the use of many different security-related activities

Author(s)	Journal	Nature of study	Focus on	Findings and/or conclusions
Rice & Spayd (2005) *Investing in supply chain security: collateral benefits*	Special Report Series, IBM Center for The Business of Government, available at: www.ibm.com.	Conceptual	Need to build secure supply chains that also exhibit resiliency	Firms need to work with all levels of governments and supply chain partners, have mode shifting capabilities, implement better communication, create contingency plans, and approach SCS as the military would
Russell & Saldanha (2003) *Five tenets of security-aware logistics and supply chain operation*	Transportation Journal,	Conceptual	Building a security best practice list for organizational business plans	Offers four primary recommendations for SCS: (1) leadership, (2) public-private partnerships, (3) more research on SCS, and (4) education and training
Closs & McGarrel (2004) *Enhancing security throughout the supply chain*	Special Report Series, IBM Center for The Business of Government, available at: www.	Qualitative	Creating synergy between supply chain management and security efforts	Prevention, TQM, source inspection, process control, and continuous improvement should lead to risk mitigation and higher SCS
Lee &Whang (2005) *Higher supply chain security with lower cost: lessons from total quality management*	International Journal of Production Economics	Conceptual	Quality improvement programs that can be used for SCS	Resiliency has much to do with organizational culture

Author(s)	Journal	Nature of study	Focus on	Findings and/or conclusions
Sheffi (2005a) *Preparing for the big on*	IEE Manufacturing Engineer,	Conceptual	Describing organizational resiliency in the event of disasters	Resiliency will help firms respond to disasters and should benefit supply chains in other ways, such as increasing flexibility
Sheffi (2005b) *The Resilient Enterprise: Overcoming Vulnerability for Competitive Advantage* .	The MIT Press, Cambridge, MA	Conceptual	Explaining how firms can prevent and recover from disasters	Resiliency will help firms respond to disasters and should benefit supply chains in other ways, such as increasing flexibility
Sarathy (2006) *Security and the global supply chain*	Transportation Journal,	Conceptual	Examining the threats to global supply chains	Firms should design security into the overall supply chain strategy, which will mitigate disruptions
Sheu et al. (2006) *A voluntary logistics security program and international supply chain partnership*	Supply Chain Management: An International Journal,	Qualitative/Quantitative	Examining effect of C-TPAT on supply chain collaboration	Voluntary government programs, particularly C-TPAT, should lead to better collaboration with supply chain partners
Thibault et al. (2006) *The response of the US maritime industry to the new container security initiatives*	Transportation Journal,	Qualitative	Understanding maritime industry response to new government security program	New SCS requirements have created stronger public-private collaborative efforts

Author(s)	Journal	Nature of study	Focus on	Findings and/or conclusions
Ritter (2007) *Securing Global Transportation Networks: A Total Security Management Approach,*	McGraw-Hill, New York, NY	Conceptual	Presenting the concept of TSM	Firms should be managing transportation security in a holistic manner, which should result in value for the firm.
Closs et al (2008) *A framework for protecting your supply chain*	Supply Chain Management Review	Conceptual	Developing a SCS framework for protection	Firms should implement security institutive into their culture, their strategy, and their supply chains
Autry & Bobbit (2008) *Supply chain security orientation: conceptual development and a proposed framework*	The International Journal of Logistics Management,	Quantitative	Developing the notion of organizational SCSO	SCSO is an intra- and inter-organizational propensity to secure supply chains, which likely results in performance outcomes
SCS and Performance Bearing Point (2003) *Asia-Pacific economic cooperation STAR-BEST project cost-benefit analysis*	White Paper, available at: www.bearingpoint.com	Quantitative	Understanding the outcomes of the Asia-Pacific Economic Cooperation security project named STAR-BEST	Firms importing to the USA should gain financial benefits from SCS

Author(s)	Journal	Nature of study	Focus on	Findings and/or conclusions
Eagers (2004) *Prospering in the secure economy, A Deloitte Research Study*	Deloitte Touche Tohmatsu, New York, NY, available at: www.deloitte.com	Conceptual	Suggesting firms are at the forefront of the war on terrorism	SCS can have positive performance outcomes for firms. Needs to be cooperation with the public sector
Gonzalez (2004) *Linking supply chain security with Sarbanes-Oxley and the bottom line*	ARC Advisory Group White Paper, available at: www.ctl.ca	Conceptual	SCS activities and their impact on performance	SCS should be viewed and implemented holistically. If SCS is approached in this manner, performance should be impacted positively
Rice & Spayd (2005) *Investing in supply chain security: collateral benefits*	Special Report Series, IBM Center for The Business of Government, available at: www.ibm.com.	Conceptual	Additional "collateral" benefits to organizations that invest in SCS	Many other benefits exist for organizations who invest in the correct SCS programs and activities
Peleg-Gillai & Sept (2005) *Innovators in supply chain security: better security drives business value*	The Manufacturing Innovation Series, available at: www.ibm.com	Quantitative	The impact of SCS on organizational performance	Firms who are innovative in SCS should realize organizational benefits

Table 29: Summary table of source literature on SCS

Author(s)/ Title	Journal	Nature of Study	Focus / Findings	Theoretical Framework/ Method and Sample size
Flynn (2000) *Beyond border control*	Foreign Affairs	Anecdotal/ Conceptual	Points out the concepts of New Border Control Measures	None
Sheffi (2001) *Supply chain management under the threat of international terrorism*	International Journal of Logistics Management	Conceptual	Identifies the following as important to SCS Operating in a heightened security environment Preparing for the Worst -Supplier Relations -Inventory Management -Knowledge and Process backup Managing SC under Uncertainty -Shipment visibility -Improved collaboration -Risk Pooling Public Private Partnership -Sharing information -Assuming Security Roles and responsibilities	None
Lee & Wolfe (2003) *Supply chain security without tears*	Supply Chain Management Review	Conceptual	Proposes the following Strategies: -Comprehensive tracking and monitoring -Total Supply Network visibility -Flexible sourcing strategies -Balanced inventory management -Product and process redesign -Demand based management	None
Closs & McGarrell (2004) *Enhancing security throughout the supply chain*	Special Report to the IBM Centre for the Business of Government	Conceptual	Defines SCS, provides a methodology to assess the SCS, defines the dimensions of SCS, recommends the integration mechanism, identifies requirements and roles for developing SCS	None

Author(s)/ Title	Journal	Nature of Study	Focus / Findings	Theoretical Framework/ Method and Sample size
Lee & Whang (2005) *Higher supply chain security with lower cost: Lessons from total quality managements*	International Journal of Production Economics	Hypothetical Case Study	-Provides the total quality framework as means to ensure SCS. -Identifies TQM, source inspection, process control and improvement cycle.	None
Banomyong (2005) *The impact of port and trade security initiatives on maritime supply-chain management*	Maritime Policy and Management	Conceptual	-Investigates the GSCS initiatives and its impacts focusing on financial implications -Identifies governments, traders, ports, service providers and insurance providers as key players	None
Sarathy (2006) *Security and the global supply chain*	Transportation Journal	Conceptual	Identifies the following strategies for SCS: -Collaboration across SC -Configuring robustness and resilience in SC -Cooperation strategies among SC partners -Harnessing Technologies -Performance metrics and models - Cost benefit analysis -Internal readiness (organizational security culture) -Corporate Social Responsibility	None
Gutierrez & Hintsa (2006) *Voluntary supply chain security programs: a systematic comparison*.	The International Conference on Information Systems Logistics and Supply Chain	Conceptual: Conference Paper	Proposes a security management framework	None
Sheu et al. (2006) *A voluntary logistics security program and international supply chain partnership*.	Supply Chain Management	Research	Identifies significant impacts of GCSC initiatives such as C-TPAT on the international trade	Case Study using 5 companies (one customer broker, three importers, one freight forwarder) and secondary data

Author(s)/ Title	Journal	Nature of Study	Focus / Findings	Theoretical Framework/ Method and Sample size
Smith et al. (2007) *A critical balance: collaboration and security in the IT-enabled supply chain*	International journal of production research	Literature Review	Identifies information security as a source of risk of supply chain. Discusses the benefits of collaboration facilitated by IT integration.	
Williams et al. (2009) *Supply chain security: an overview and research agenda*	International Journal of Logistics Management	Literature Review	-Identifies the need for more academic focus -Categorizes SCS into main categories such as intra-organizational, inter-organizational, a combination of intra-organizational and inter-organizational	
Williams et al. (2009) *Why all the changes? An institutional theory approach to exploring the drivers of supply chain security (SCS)*	International Journal of Physical Distribution and Logistics Management	Research	Identifies four primary drivers of SCS namely government, customers, competitors, and society	Qualitative with 19 in-depth interviews Theoretical Framework: Institutional Theory
Hintsa (2010) *A comprehensive framework for analysis and design of supply chain security standards*	Journal of Transportation Security	Research	Proposes a theoretical framework for the analysis and design of SCS standards for the benefit of government policy makers, supply chain and security experts.	Qualitative, interviews

Author(s)/ Title	Journal	Nature of Study	Focus / Findings	Theoretical Framework/ Method and Sample size
Whipple et al. (2009) *Supply chain security practices in the food industry: Do firms operating globally and domestically differ?*	Journal of Operations Management	Research	Studies the link between security initiatives and firm performance in terms of security outcomes, product quality, and customer service. Results indicate that international firm's perception of security are higher and are more likely to assess the security procedures of their partners. Findings also suggest that international firms perceive they perform better in terms of the ability to detect and recover from security incidents.	Mixed Methods: Qualitative interviews: 50 managers from 15 firms (Grounded Theory). The findings from the Qualitative interviews were used to design a quantitative survey. The samples (major food manufacturers and security related industries and participating government industries) were n = 195. Domestic = 88, international = 107
Urciuoli (2010) *Supply chain security—mitigation measures and a logistics multi-layered framework*	Journal of Transportation Security	Research	Findings suggest the areas to be improved for SCS are government initiatives, management strategies, operative routines and technical system as major areas that need improvement.	Qualitative, interviews
Yang (2010) *Impact of the container security initiative on Taiwan's shipping industry*	Maritime Policy and Management	Research	Identifies Cargo Security Initiative (CSI) risk assessment factors. Findings suggest that the balance between the efficiency of maritime logistics and SCS is of vital importance to trading countries dealing with security risk issues;	Quantitative surveys n= 65 including customs brokers, freight forwarders, shipping agencies, managers and deputy managers.

Author(s)/ Title	Journal	Nature of Study	Focus / Findings	Theoretical Framework/ Method and Sample size
Martens et al. (2011) *Examining Antecedents to Supply Chain Security Effectiveness: An Exploratory Study*	Journal of Business Logistics	Research	Explores the relationship between security management and perceived effectiveness of SCS. Findings suggest that Internal and external integration efforts, a nodal planning focus, and proactive motivations related to security measures were found to be positively related to security effectiveness.	Quantitative Survey, Sample size: 69 from Supply Chain; Theoretical Framework: Resource Based View (RBV)
Speier et al. (2011) *Global supply chain design considerations: Mitigating product safety and security risks.*	Journal of Operations Management	Research	Proposes a framework to examine the threat of potential disruptions on SC process and focuses on mitigation strategies. Findings suggest that security initiatives depend on top management mindfulness, operational complexity, product risk, and coupling	Mixed Methods Qualitative interviews: use to guide the development of measures and constructs for quantitative analysis. 75 participants across 25 different firms. Theoretical Frameworks: Normal Accident Theory and High Reliability Theory.
Lee et al. (2011) *Supply chain efficiency and security: Coordination for collaborative investment in technology*	European Journal of Operational Research	Mathematical Model	Examines the incentive mechanism between a manufacturer and a retailer for jointly investing in a new technology that has the potential to improve the efficiency and security of the supply chain. Findings suggest that: (1) When security concerns are not strong enough to dominate efficiency concerns, stakeholders may not have a sufficient incentive to invest; therefore, at least one stakeholder under invests. (2) When security concerns are strong enough to dominate efficiency concerns, stakeholders may not invest at all because of the uncertainty of other stakeholders' behaviour, rather than the lack of an incentive to invest in the technology.	

Author(s)/ Title	Journal	Nature of Study	Focus / Findings	Theoretical Framework/ Method and Sample size
Lu et al. (2013) *Next Big Thing in Big Data: the Security of the ICT Supply Chain.*	International Conference on Social Computing IEEE 2013	Conference Paper: Conceptual.		
Voss & Williams (2003) *Public–Private Partnerships and Supply Chain Security: C-TPAT as an Indicator of Relational Security*	Journal of Business Logistics	Research	Studies PPP with a focus on the C-TPAT certification. Findings suggest that certified firms outperform noncertified firms in security performance, firm performance, and resilience. Argues that costs are justified in terms of achieving internal targets in performance.	Quantitative Survey Sample Size: 338
Bueno-Solano & Cedillo-Campos (2014) *Dynamic impact on global supply chains performance of disruptions propagation produced by terrorist acts*	Transportation Research Part E: Logistics and Transportation Review	Research	A dynamic assessment model establishing analysis scenarios the effects of the materialization and simultaneous propagation of disruptions produced by terrorist acts on global supply chain performance.	The simulation data was captured from a Case Study data with one company

Appendix F. Information Security Literature Review

Table 30: Perceived Importance of information security

Author(s) / Topic	Journal	Focus/Findings	Nature of Study
Straub Jr. (1990) *Effective IS Security: An Empirical Study*	Information System Research	Information security is not a high priority for most managers	Quantitative survey Sample Size: 1211 (random) Theoretical Framework: criminological theory of general deterrence
Ryan & Bordoloi (1997) *Evaluating security threats in mainframe and client/server environments*	Information & Management	Significance of information security not appreciated During the earlier stages of migration from mainframe to client server computer viruses were not seen as a significant threat	Quantitative survey Sample Size: 52 (IT professionals) Theoretical Framework: None
Loch et al.(1992) *Threats to Information Systems: Today's Reality, Yesterday's Understanding.*	MIS Quarterly	Identification of the most serious threats. (mainframes, client/server micro) Belief that the internal threats are minimal contrary to security expert's warnings and perceive external network risks are higher. Virus is not a concern	Quantitative Survey Sample Size: 129 (IT Professionals) Theoretical Framework: None

Author(s) / Topic	**Journal**	**Focus/Findings**	**Nature of Study**
Goodhue & Straub (1991) *Security concerns of system users: A study of perceptions of the adequacy of security.*	Information and Management	Users concern about security is a function of three different constructs: industry risk, company actions and individual awareness. Findings suggest individual awareness is significant.	Quantitative Survey Sample Size: 570 (from a IT professional association) Sample Size: 357 (end users)
El-Gayar & Fritz (2010) *A web-based multi-perspective decision support system for information security planning.*	Decision Support Systems	Presents a theoretical basis for a design of a web based multi-perspective decisions support system for multi criteria security control selection decision problem	Theoretical
(Posey, et al., 2014) *Bridging the Divide: A Qualitative Comparison of Information Security Thought Patterns between Information Security Professionals and Ordinary Organizational Insiders*	Information and Management	Assesses the mindsets of insiders regarding their relationships with information security efforts. Reports the difference in perspective on information security between the IT Security professionals and ordinary users within an organization.	Qualitative Sample size: 22 ordinary insiders and 11 information security professionals

Table 31: Deterrence

Author(s) / Topic	Journal	Focus/Findings	Nature of Study
Spears et al. (2013) *Theorizing the concept and role of assurance in information systems security. Information & management.*	Information & Management	Findings -Suggest that unless an organization's assurance claims are based on achieving Level 4 (capability Maturity Model, which says performance is managed by using established, measurable goals) maturity, assurance will be based on symbolism than effectiveness.	Theoretical and Conceptual Theoretical Framework: Institutional Theory The capability maturity model
Werlinger et al. (2009) *Security practitioners in context: Their activities and interactions with other stakeholders within organizations.*	International Journal of Human-Computer Studies	Reveals that the tools used by our participants to perform their security tasks provide insufficient support for the complex, collaborative interactions that their duties involve	Qualitative Sample Size: 30 interviews
Von Solms et al. (1994) *A framework for information security evaluation.*	Information & Management	Proposes an information security management model	Conceptual
Straub & Welke (1998) *Coping With Systems Risk: Security Planning Models for Management Decision Making.*	MIS Quarterly	Use of security risk planning model, education/training in security awareness and countermeasure matrix analysis can effectively deal with in implementing the most effective controls.	Comparative qualitative studies two firms

Author(s) / Topic	Journal	Focus/Findings	Nature of Study
Lili et al. (2006) *An Information Systems Security Risk Assessment Model Under the Dempster-Shafer Theory of Belief Functions*	Journal of Management Information Systems,	Develops an evidential reasoning approach for the risk analysis of ISS under Dempster-Shafer Theory of belief model	Mathematical model based on hypothetical case Theory of Belief Functions
Kotulic & Clark (2004) *Why there aren't more information security research studies.*	Information & Management	Proposes a conceptual model based on the study of SRM at the firm level. An indirect contribution of the research study is the information extracted from those who were willing to discuss their reasons for not wishing to participation *Email and intrusive studies	Unsuccessful
Chen et al. (2011) *Correlated failures, diversification and information security risk management.*	MIS Quarterly	Model for measuring security loss due to unavailability of systems	Mathematical

Table 32: Risk Management and Analysis

Author(s) / Topic	Journal	Focus/Findings		Nature of Study
Spears et al. (2013) *Theorizing the concept and role of assurance in information systems security. Information & management.*	Information & Management	-Suggest that unless an organization's assurance claims are based on achieving Level 4 (capability Maturity Model, which says performance is managed by using established, measurable goals) maturity, assurance will be based on symbolism than effectiveness.		Theoretical and Conceptual **Theoretical Framework:** -Institutional Theory -The capability maturity model Qualitative: 13 interviews
Werlinger et al. (2009) *Security practitioners in context: Their activities and interactions with other stakeholders within organizations.*	International Journal of Human-Computer Studies	Reveals that the tools used by our participants to perform their security tasks provide insufficient support for the complex, collaborative interactions that their duties involve		Qualitative Sample Size: 30 interviews
Von Solms et al. (1994) *A framework for information security evaluation.*	Information & Management	Proposes an information security management model		Conceptual (no empirical evidence)
Straub & Welke (1998) *Coping With Systems Risk: Security Planning Models for Management Decision Making.*	MIS Quarterly	Use of security risk planning model, education/training in security awareness and countermeasure matrix analysis can effectively deal with in implementing the most effective controls.		Comparative qualitative studies two firms

Author(s) / Topic	Journal	Focus/Findings		Nature of Study
Lili et al. (2006) *An Information Systems Security Risk Assessment Model Under the Dempster-Shafer Theory of Belief Functions*	Journal of Management Information Systems,	Develops an evidential reasoning approach for the risk analysis of ISS under Dempster-Shafer Theory of belief model		Mathematical model based on hypothetical case Theory of Belief Functions
Kotulic & Clark (2004) *Why there aren't more information security research studies.*	Information & Management	Proposes a conceptual model based on the study of SRM at the firm level. An indirect contribution of the research study is the information extracted from those who were willing to discuss their reasons for not wishing to participation *Email and intrusive studies		Unsuccessful
Chen et al. (2011) *Correlated failures, diversification and information security risk management.*	MIS Quarterly	Model for measuring security loss due to unavailability of systems		Mathematical
Von Solms et al. (1994) *A framework for information security evaluation.*	Information & Management	Proposes an information security management model		Conceptual

Author(s) / Topic	Journal	Focus/Findings		Nature of Study
Straub & Welke (1998) *Coping With Systems Risk: Security Planning Models for Management Decision Making.*	MIS Quarterly	Use of security risk planning model, education/training in security awareness and countermeasure matrix analysis can effectively deal with in implementing the most effective controls.		Comparative qualitative studies two firms
Lili et al. (2006) *An Information Systems Security Risk Assessment Model Under the Dempster-Shafer Theory of Belief Functions*	Journal of Management Information Systems,	Develops an evidential reasoning approach for the risk analysis of ISS under Dempster-Shafer Theory of belief model		Mathematical model based on hypothetical case Theory of Belief Functions
Kotulic & Clark (2004) *Why there aren't more information security research studies.*	Information & Management	Proposes a conceptual model based on the study of SRM at the firm level. An indirect contribution of the research study is the information extracted from those who were willing to discuss their reasons for not wishing to participation *Email and intrusive studies		Unsuccessful

Table 33: User Compliance Behaviour

Author(s) / Topic	Journal	Focus/Findings	Nature of Study
Ifnedo (2014) *Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition.*	Journal of Information & Management	-Social bonds that are formed at work largely influence attitudes towards compliance and subjective norms, with both constructs positively affecting employees' ISSP compliance. -Employees' locus of control and capabilities and competence related to IS security issues also affect ISSP compliance behavioural intentions	**Quantitative survey** -Sample size: 124 responses -Analysis: SEM PLS **Theoretical Framework:** -Theory of Planned Behaviour -Social cognitive theory -Social bond theory
Vance et al. (2012) *Motivating IS security compliance: insights from habit and protection motivation theory*	Information & management	-Habitual IS Security compliance strongly reinforced the cognitive process theorized by PMT. -Addressing employees' past automatic behaviour in order to improve compliance is of importance	**Quantitative Survey** -Sample size: 210 -Analysis: PLS **Theoretical Framework** -Protection Motivation Theory -Habit Theory
Jai-Yeol (2011) *Out of fear or desire? Toward a better understanding of employees' motivation to follow IS security policies*	Information & management	Variable rooted in the intrinsic motivation model contributed significantly more than the extrinsic motivation model in explaining the variance of employee's compliance.	**Quantitative survey** -Sample Size: 602 -Analysis: PLS Structuring model **Theoretical Framework** -Deterrence Theory

Author(s) / Topic	**Journal**	**Focus/Findings**	**Nature of Study**
Siponen & Vance (2010) *Neutralization: New insights into the problem of employee information systems security policy violations*.	MIS Quarterly	Neutralization significantly affects the predisposition to violate IS security policy and is a good predictor of employees' intention to violate IS Security.	**Quantitative survey** -Sample Size: 1449 -Analysis: PLS SEM -Used a scenario Analysis technique **Theoretical Framework** -Neutralization Theory -Deterrence Theory
Robert (2006) *Understanding the perpetration of employee computer crime in the organisational context.*	Information and Organization	Conceptual	**Theoretical Framework** -Rational Choice -Situational Crime Prevention
Puhakainen & Siponen (2010) *Improving employee's compliance through information systems security training: An action research study.*	MIS Quarterly	Reports nine key findings on the development of an IS Security policy compliance training program.	**Action Research** (interviews, survey, participatory observation)

Li et al. (2010) *Understanding compliance with internet use policy from the perspective of rational choice theory*	Decision Support Systems	-Employees' intention to comply with the IUP involves a cost–benefit analysis. -Employees are more likely to comply with the IUP when perceived benefits are overridden by potential risks from formal sanctions and security threats -The deterrence effect of formal sanction risks is largely exerted through detection probability rather than sanction severity -Sanction severity is not an effective deterrence mechanism for the majority of employees. -The social influence from important others or subjective norms, is not a significant predictor for the intention to comply with the Internet use policy -The effect of subjective norms is also contingent upon people's experience. They are more likely to take effect in the early stages of experience when an individual's knowledge and beliefs are relatively ill-formed; -Compliance intention is also influenced by employees' personal norms or moral standards against Internet abuses -Sanction probability exerts a largely direct impact on IUP compliance intention. -Personal norms moderate the impact of perceived sanction severity on the compliance intention. -Organizational norms against Internet abuses and organizational identification indirectly influence employees' compliance intention through developing and/or strengthening employees' personal norms against Internet abuses Harsh sanctions may undermine the trust or loyalty toward a firm and, therefore, generate a counterproductive effect on the compliance intention among those with moderate to high personal norms against Internet abuses	**Quantitative survey** -Sample Size:246 -Analysis: PLS SEM **Theoretical Framework** Theory of Rational Choice

Author(s) / Topic	Journal	Focus/Findings	Nature of Study
Posey et al. (2011) *Understanding the mindset of the abusive insider: An examination of insiders' causal reasoning following internal security changes*	Computers & Security		
Huang et al. (2011) *Factors affecting perception of information security and their impacts on IT adoption and security practices.*	International Journal of Human-Computer Studies	People's compliance to security practice, such as setting strong passwords for IT systems, can be enhanced by changing their perceived knowledge, severity and possibility.	Experiment among 64 participants
Ng et al. (2009) *Studying users' computer security behaviour: A health belief perspective*.	Decision Support Systems	-Perceived susceptibility, perceived benefits, and self-efficacy are determinants of email related security behaviour. -Perceived severity moderates the effects of perceived benefits, general security orientation, cues to action, and self-efficacy on security behaviour	**Quantitative survey** -Sample size: 134 -Analysis: Multiple Regression **Theoretical Framework** -Health Belief Model
Myyry et al. (2009) *What levels of moral reasoning and values explain adherence to information security rules[quest] An empirical study*	European Journal of Information Systems	Explains noncompliance in terms of moral reasoning and values.	**Quantitative survey** -Sample size: 132 -Analysis: Multiple regression and *t*-statistics **Theoretical Framework** -Theory of Cognitive Moral Development -Theory of Motivational Types Values

Author(s) / Topic	**Journal**	**Focus/Findings**	**Nature of Study**
Johnston & Warkentin (2010) *Fear appeals and information security behaviours: An empirical study*	MIS Quarterly	Findings suggest that fear appeals do impact end user behavioural intentions to comply.	**Laboratory experiment** -Sample size: 275 -Analysis: PLS SEM **Theoretical Framework** -Protection Motivation Theory
Adams & Blandford (2005) *Bridging the gap between organizational and user perspectives of security in the clinical domain.*	International Journal of Human-Computer Studies	Importance of user's security awareness and control are reviewed within the context of communities of practice.	**Qualitative** Interviews and focus groups
Herath & Rao (2009b) *Protection motivation and deterrence: a framework for security policy compliance in organisations.*	European Journal of Information Systems	-Threat perceptions about the severity of breaches and response perceptions of response efficacy, self-efficacy, and response costs are likely to affect policy attitudes; -Organizational commitment and social influence have a significant impact on compliance intentions; -Resource availability is a significant factor in enhancing self-efficacy, which in turn, is a significant predictor of policy compliance intentions.	**Quantitative survey** -Sample size: 312 out of 78 organizations -Analysis: PLS SEM **Theoretical Model** -Integrated Protection Motivation and Deterrence Model -Decomposed Theory of Planned Behaviour

Author(s) / Topic	**Journal**	**Focus/Findings**	**Nature of Study**
K. Guo et al. (2011) *Understanding Nonmalicious Security Violations in the Workplace*: *A Composite Behaviour Model*	Journal of Management Information Systems	-Utilitarian outcomes (relative advantage for job performance, perceived security risk), normative outcomes (workgroup norms), and self-identity outcomes (perceived identity match) are key determinants of end user intentions to engage in NMSVs. -In contrast, the influences of attitudes toward security policy and perceived sanctions are not significant.	**Quantitative survey** -Sample size: 167 -Scenario based -Analysis: PLS SEM **Composite behaviour model** -Theory of Reasoned Action -Theory of Planned Behaviour
Dinev & Qing (2007) *The Centrality of Awareness in the Formation of User Behavioural Intention toward Protective Information Technologies*	Journal of the Association for Information Systems	-Awareness of the threats posed by negative technologies is a strong predictor of user behavioural intention toward the use of protective technologies. -In the presence of awareness, the influence of subjective norm on individual behavioural intention is weaker among basic technology users but stronger among advanced technology users. -Determinants 'perceived ease of use' and 'computer self-efficacy' is no longer significant in the context of protective technologies.	**Quantitative survey** -Sample size: 339 -Analysis: PLS SEM **Theoretical Framework** -Theory of Technology Acceptance
de Paula et al. (2005) *In the eye of the beholder: A visualization-based approach to information system security.*	International Journal of Human-Computer Studies	Security is a joint production of system and user	Qualitative and Laboratory experimental Sample size: 20 interviews

Author(s) / Topic	**Journal**	**Focus/Findings**	**Nature of Study**
Bulgurcu et al. (2010) *Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness.*	MIS Quarterly	Employee's attitude is influenced by benefit of compliance, cost of compliance, and cost of noncompliance, which are beliefs about the overall assessment of consequences of compliance or noncompliance	**Quantitative survey** -Sample Size: 446 -Analysis PLS SEM **Theoretical Framework** -Theory of Planned Behaviour -Rational Choice Theory
Boss et al. (2009) *If someone is watching, I'll do what I'm asked: mandatoriness, control, and information security.*	European Journal of Information Systems	-Specifying policies and evaluating behaviours are effective in convincing individuals that security policies are mandatory. -The perception of mandatoriness is effective in motivating individuals to take security precautions, thus if individuals believe that management watches, they will comply.	**Quantitative survey** -Sample size: 1698 -Analysis: PLS SEM
Anderson & Agarwal (2010) *Practicing safe computing: A multimethod empirical examination of home computer user security behavioural intentions.*	MIS Quarterly	Home computer user's intention to perform security-related behaviour is influenced by a combination of cognitive, social, and psychological components	**Quantitative Survey** -Sample Size: 594 -Experiment with 101 -Analysis: PLS SEM **Theoretical Framework** Protection Motivation Theory

Author(s) / Topic	Journal	Focus/Findings	Nature of Study
Siponen et al. (2014) *Employees' adherence to information security policies: An exploratory field study*.	Information & management	Perceived severity of potential information security threats, employees' belief as to whether they can apply and adhere to information security policies, perceived vulnerability to potential security threats, employees' attitude toward complying with information security policies, and social norms toward complying with these policies had a significant and positive effect on the employees' intention to comply with information security policies	**Quantitative survey** -Sample size: 669 -Analysis PLS SEM **Theoretical Framework** -Protection Motivation Theory, -Theory of Reasoned Action, -The Cognitive Evaluation Theory

Table 34: Organizational Information Security Behaviour

Author(s) / Topic	Journal	Focus/Findings	Nature of Study
Baskerville et al. (2014) *Incident-centered information security: Managing a strategic balance between prevention and response*	Information & management	Reports that information security strategies employ prevention and response paradigms. Organizations choose to balance between prevention and response as ground for its current information security posture.	**Qualitative case study** -Sample size: 3 organizations **Theoretical Framework** -Incident centered security framework
Wallace (2011) *Information Security and Sarbanes-Oxley Compliance: An Exploratory Study.*	Journal of Information Systems,	The implementation of suggestive controls from international standards depended on a company's status as public, private, the size of the company and in the industry which it operates.	**Quantitative survey** Sample size: 636
Theoharidou et al. (2005) *The insider threat to information systems and the effectiveness of ISO17799*	Computers & Security		
Siponen & Willison (2009) *Information security management standards: Problems and solutions*	Information & Management	-International standards are were generic or universal in scope; -they do not pay enough attention to the differences between organizations and the fact that their security requirements are different. -guidelines were validated by appeal to common practice and authority and that this was not a sound basis for important international information security guidelines.	Content Analysis
Png & Wang (2009) *Information Security: Facilitating User Precautions Vis-à-Vis Enforcement Against Attackers*	Journal of Management Information Systems	For both mass and targeted attacks, facilitating end-user precautions reduces the expected loss of end users.	Mathematical

Author(s) / Topic	Journal	Focus/Findings	Nature of Study
Dhillon & Torkzadeh (2006) *Value focused assessment of information system security in organizations.*	Information Systems Journal	Maintaining IS Security in organizations, it is necessary to go beyond technical considerations and adopt organizationally grounded principles and values.	**Qualitative** -Sample size: 103 managers
Backhouse et al. (2006) *Circuits of power in creating de jure standards: Shaping an international information systems security standard.*	MIS Quarterly	Mandated standards can be inhibited by insufficient resource allocation, lack of senior management input and commitment Factors contributing to resistance to adopt standards can be group norms and cultural biases	Canonical action research. A total of 79 agencies in one year and 89 in the other.
Ransbotham & Mitra (2009) *Choice and Chance: A Conceptual Model of Paths to Information Security Compromise*.	Information Systems Research	Distinguishes between deliberate and opportunistic paths of compromise.	Grounded Theory Research using secondary data from intrusive systems
Hsu et al. (2012) *Institutional Influences on Information Systems Security Innovations.*	Information Systems Research	In addition to institutional forces there are six other economic base considerations that influences on the degree of the adoption and assimilation of information security management.	**Mixed Methods** -Sample Qualitative: 10 interviews Quantitative Sample: 140 -Analysis: PLS-SEM **Notes**: Following the extensive literature review was to conduct 10 qualitative interviews with managers in charge of information security management and top IS managers. The purpose of the interviews was to validate and supplement critical factors or drivers

Author(s) / Topic	Journal	Focus/Findings	Nature of Study
			identified in the extant literature with managers who were leading information management security initiatives. Theoretical Framework: Institutional Theory on Innovation Diffusion Analysis: PLS SEM
Baskerville et al. (2014) *Incident-centered information security: Managing a strategic balance between prevention and response.*	Information & management	Information security strategies employ principles and practices grounded in both the prevention and response paradigms. The prevention paradigm aims at managing predicted threats. Although the prevention paradigm may dominate in contemporary commercial organizations, the response paradigm (aimed at managing unpredicted threats) retains an important role in protecting information security in today's dynamic threat environment.	Qualitative comparative case study: 3 Companies.