AN EVALUATION OF THE VALUE OF SECURITY IN THE INTERNATIONAL MARINE SUPPLY CHAIN

by

Wai Leng Loke

B.BA, The National University of Singapore (2001)

A THESIS SUBMITTED IN PARTIAL FULFILLMENT OF
THE REQUIREMENTS FOR THE DEGREE OF

MASTER OF SCIENCE in BUSINESS ADMINISTRATION

in

THE FACULTY OF GRADUATE STUDIES

(Transportation and Logistics)

THE UNIVERSITY OF BRITISH COLUMBIA

(Vancouver)

April 2008

ABSTRACT

Since the events of 9/11, there has been tremendous amount of renewed interests in the study of trade security. There has been an influx of security regulations and the private sector has been trying to keep pace in complying with them. However, due to the public externalities of security improvements and the lack of quantified and proven benefits, the private sector is struggling to establish business cases for their security initiatives.

There is very little quantitative research in this area. Using exploratory factor analysis (EFA) and structural equation modeling (SEM), this study serves to fill this gap by introducing a statistical way of analysing and understanding the complex relationships amongst security effort, its motivators and performance and traditional supply chain performance (SCP). This study also proposes an evaluation framework for security efforts.

EFA results show that security is a dimension of SCP. This means that organizations have all along been measuring an aspect of their operations that relates to security. As such, organizations should not perceive the current heightened interests in security as throwing them off-balance. In evaluating security efforts, organizations should select key performance indicators (KPIs) that represent each of the four areas of information, cargo, people and cost.

SEM results show that organizations undertake security efforts as a result of both perceived security benefits and perceived collateral benefits, with perceived security benefits carrying a greater weight in the decision-making process. Results also show that organizations are implementing security initiatives out-of-compliance i.e. implementing initiatives that they perceive as not having significant impacts on security and SCP.

In view of the positive relationships among perceived security impact, security effort and security performance, there is further imperative for an objective method for evaluating security efforts to prevent effort justification behaviour in determining the effectiveness of the same. Results also show that organizations perceive an improved performance in security leads to an overall improvement in SCP. However, as with other supply chain strategies, there are tradeoffs and not all aspects of SCP are impacted in the same way. Time, responsiveness and efficiency for instance are negatively impacted while reliability is positively impacted.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

3PL	3rd Party Logistics Service Provider
9/11	September 11, 2001
ACE	Automated Commercial Environment
ACI	Advanced Commercial Information
ADF	Asymptotically Distribution Free
AMOS	Analysis of Moment Structures
AMR	Advanced Manifest Rule
ASN	Advanced Shipment Notice
Bil	Billion
BITSAFS	Bureau of Intelligent Transportation System and Freight Security
CBP	Customs and Border Protection
CBSA	Canadian Customs Border Service Agency
CCTV	Close-Circuit Television
CEO	Chief Executive Officer
CFI	Comparative Fit Index
CN	Hoelter's Critical N
CSCMP	Council of Supply Chain Management Professionals
CSDs	Container Security Devices
CSI	Container Security Initiative
C-TPAT	Customs -Trade Partnership Against Terrorism
DC	Distribution Center
DSC	Digital Signal Controller
DSRC	Dedicated Short-Range Communication
ECMT	European Conference of Ministers of Transport
EDI	Electronic Data Interchange
FAA	Federal Aviation Administration
FAST	Free and Secure Trade
FBI	Federal Bureau of Investigation
FCL	Full Container Loads
FDA	Food and Drug Administration
FMCG	Fast Moving Consumer Goods
GAO	General Accounting Office

GFI	Goodness-of-Fit Index
GLS	Generalized Least Squares
GPS	Global Positioning System
GSM	Global System for Mobile communications
IFI	Incremental Fit Index
IMO	International Maritime Organization
Incoterms	International Commercial Terms
ISPS	International Ship and Port Facility Security
ITS	Intelligent Transportation Systems
JBL	Journal of Business Logistics
JoC	Journal of Commerce
KPI	Key Performance Indicator
LCD	Liquid Crystal Display
LCL	Less-than-Container Loads
Mil	Million
Mgt	Management
ML	Maximum Likelihood
NBC	Nuclear, Biological, or Chemical weapons
NDA	Non-Disclosure Agreement
NFI	Normed Fit Index
OSC	Operations Safe Commerce
PIP	Partners in Protection
PIR	Passive Infrared
RFID	Radio-Frequency Identification
RMSEA	Root Mean Squared Approximation of Error
ROI	Return on Investment
Sarbox	Sarbanes-Oxley Act
SBU	Strategic Business Unit
SCA	Security Consent Agreement
SCOR	Supply-Chain Operations Reference
SCL	Supply Chain Logistics Council
SCP	Supply Chain Performance
SEM	Structural Equation Modeling
SMS	Short Message Service

SOX	Sarbanes-Oxley Act
SST	Safe and Secure Trade Lane
TEU	Twenty-Foot Equivalent Units
TLI / NNFI	Tucker-Lewis Index or Non-Normed Fit Index
TQM	Total Quality Management
U.K.	The United Kingdom
U.S.	United States of America
ULD	Unit Load Device
VDC	Voltage Direct Current
VMI	Vendor Managed Inventory
WCO	World Customs Organization
WLS	Weighted Least Squares
χ^2 Statistic	Chi-Square Statistic

ACKNOWLEDGMENTS

I would like to offer my enduring gratitude to Dr. Garland Chow, whose penetrating questions have taught me to question more deeply. Without his patient guidance and advice, his relentless support in the empirical work required for this study, this thesis would not have been successful.

I am also grateful to Professor Trevor D. Heaver and Dr. Chunyan Yu for the care with which they reviewed the original manuscript, the conversations and the challenging questions that have all served to enlarge and clarify my thinking on my work in the field of transportation and logistics. I am equally indebted to Dr. Chris Dubelaar and Dr. Ronald T. Cenfetelli for their patient guidance on the statistical aspects of this thesis, especially with the use of the Structural Equation Modeling statistical technique.

I would also like to offer my heartfelt thanks to the following groups of people. Without their valuable insights, suggestions and help, this study would not have been possible.

- Danny, Rena and Edmund who has contributed their valuable time in helping to make the online survey a reality and a success
- those who have been instrumental in making the field interviews a reality with special mention to Mr. Paul Tay in Shanghai
- all participants in the field interviews from Singapore, Shanghai and Vancouver
- all who have responded to this study's online survey

I would also like to express my thanks to the faculty, staff and my fellow students at the University of British Columbia (UBC), who have in one way or another, inspired me to continue my work in this field.

I also owe special thanks and deepest gratitude to my amazing parents and three wonderful sisters, who have given me their unconditional support and encouragement at critical and opportune times and basically in whatever I do. Special mention also goes to my twin sister Ashley for her great help on the Chinese translations and Sarah for proof reading and editing my final thesis.

to:

my amazing parents
and three wonderful sisters

CHAPTER 1 INTRODUCTION

Since the terrorist attacks on the U.S. soil on the 11th of September 2001 (also commonly known as "9/11"), there has been tremendous amount of renewed interests in the study of risk management in supply chain management especially in the areas of trade security and safety.

Since the tragic events of 9/11, there has been an influx of security regulations and mandates that include the Customs-Trade Partnership Against Terrorism (C-TPAT), the Container Security Initiative (CSI), the Advanced Manifest Rule (AMR) and the Free and Secure Trade initiative (FAST) from the public sector[1] and private organisations have been trying to keep pace in complying with these mandates.

Public Effects of Security Investments

The nature of the costs and benefits from security investments are such that they suggest public effects which are largely externalities to the private sector. Much of the expected benefits from improving security come from reduced danger and risks to human life and public properties. As such the public sector has been taking most of the initiatives in addressing trade security since the tragic events of 9/11. However, the responsibilities of ensuring secure trade movement are beginning to shift from the public to the private sector.

Organisations are now tasked to make appropriate supply chain security investments to protect their assets and improve the security of their supply chain. However, the very existence of public externalities has raised much discussion within the private sector as to who should assume the cost of security investments. Organisations are finding it challenging to evaluate the many security initiatives and/or technologies and build business cases for them. This is because the nature of security investments is such that they do not directly increase revenues and they defy many traditional methods of calculating Return on Investments (ROI) if firms only consider cost avoidance. Moreover, the fact that certain investments in traditional supply chain operations such as visibility tools, can easily overspill to affect the security of a supply chain, makes it even harder for private organisations to isolate the benefits of security investments.

---

[1] A study done by the Bureau of Intelligent Transportation Systems and Freight Security (BITSAFS) indicates that there are about 60 or more existing security related regulations in the United States and Canada.

Therefore, there needs to be a way to help organisations measure security performance so that they can use it to evaluate various security options and strategies and justify their investments accordingly.

Performance Measurement for Security Investments

Supply chain security performance as defined in this study is the overall confidence that the supply chain system will not be compromised, either as a target for terrorism and other criminal activities or as a vehicle to facilitate terrorist and other criminal activities.

The purpose of this study is to identify a key set of performance measurements that most appropriately reflects the security performance of the operations of an international maritime supply chain. Having a "common" set of performance measures for security performance will enable managers and policy makers to compare and contrast security initiatives, programs and technologies and thereby help them to make better investment and policy decisions.

Specifically, the study addresses the questions:

- What are the key performance measurements for security performance of an international maritime supply chain, from the industry practitioners' point of view?
- What is the relationship between security performance measurements and traditional[2] supply chain performance measurements?
- What is the relationship between security initiatives and supply chain security performance?
- What is the relationship between security initiatives and traditional supply chain performance?

1.1 Outline of Thesis

Chapter 2 reviews the literature of risk management in supply chain management, particularly focusing on the security aspects of supply chain risks. This chapter includes a history of supply chain risk management and introduces some recent frameworks for thinking about and managing supply chain risks. This chapter then moves on to introduce a specific aspect of

[2] Traditional supply chain performance measurements refer to those measurements that organizations commonly use to monitor their supply chain operations e.g. on-time deliveries, number of back orders per time period, information accuracy rates etc.

supply chain risk - security risks, and some of the ways that organisations both public and private, are currently employing to manage supply chain security risks.

Chapter 3 briefly reviews the methodologies employed in this study, namely, (1) Field Interviews, (2) Internet and mail survey, (3) Factor Analysis and (4) Structural Equation Modelling (SEM). This chapter discusses the rationale behind the use of each of these methodologies in their respective stages of this research study, their advantages, disadvantages and limitations.

Chapter 4 describes the data that is being used to investigate the primary questions of interests. The chapter describes the survey instrument used in the primary data collection, the respondent sample and provides some descriptive statistical analyses of the data collected.

Chapter 5 presents the results from the factor and SEM analysis of the survey data and discusses the steps taken. The results are used to discuss the primary research questions of interests and hypotheses.

Research Questions of Interest

- What are the key performance measurements for security performance of an international maritime supply chain, from the industry practitioners' point of view?
- What is the relationship between supply chain security performance measurements and traditional SCP measurements?
- What is the relationship between security initiatives and supply chain security performance?
- What is the relationship between security initiatives and traditional SCP?

Hypotheses

- The amount of an organization's security efforts is affected positively by how much impact on security performance the organization perceives the effort(s) will have.
- The amount of an organization's security efforts is affected positively by how much collateral benefits the organization perceives the effort(s) will bring.
- An organization's security efforts will positively affect their supply chain performance in terms of security.

- An organization's positive perception of the security impact of their security efforts will positively affect their self-perceived performance in the security of their supply chain operations.
- An improvement in the security performance of an organization's supply chain operations will have a positive impact on traditional SCP.

Chapter 6 concludes the study and addresses the contributions and limitations of the study, final thoughts and potential future research directions.

CHAPTER 2 LITERATURE REVIEW

2.1 Supply Chain Risks

Risk pervades every aspect of our lives. Risk, in itself a timeless element, is defined in 1921 by Knight and in 1992 by Warren, as the complete knowledge of the potential outcomes of a given situation, the objective probability of the occurrence of each and their consequences. Deloach (2000) defines business risk as the level of exposure to uncertainties that the enterprise must understand and effectively manage as it executes its strategies to achieve its business objectives and create value (Norrman and Lindroth, 2004).

The term "supply chain" describes an overall process that results in good being transported from the point of origin to their final destination and includes the movement of goods, the shipping data and the associated processes as well as a series of dynamic relationships (Peleg-Gillai et al., 2003). Supply chains exhibit risks in a variety of dimensions (Ritchie and Brindley, 2004). Within a supply chain network, there exist numerous participating stakeholders and hand-offs. The disparate nature of these stakeholders, their activities and interests, give rise to the many areas of vulnerability that are susceptible to negative impacts of events that might happen with or without certainty. A number of trends during the last decade have affected the supply chain risk situation. One is that the supply chain should be lean (Christopher and Towill, 2000; Towill and Christopher, 2003; Li et al.,2005; Cubalchini-Travis, 2006; Goldsby et al., 2006). Another is that it should be agile (Christopher, 2000; Christopher and Towill, 2000; Mason-Jones et al., 2000; Goldsby et al., 2006). A third trend is the evolution of sourcing strategies. Outsourcing resulted in more links in the chain. Single sourcing has increased an organization's supply dependence. Global sourcing takes advantage of lower product costs but has increased an organization's susceptibility to greater business uncertainty such as exchange rate fluctuations and longer lead times. All these trends are making supply chains more vulnerable to disruptions than they used to be.

The essence of supply chain risk is the risk of malfunctioning. A supply chain network can malfunction as a result of events as mild as a one hour delay in supply of raw materials that are running out of stock or a recall of a particular model of cars because of a faulty speedometer to

as serious as a complete shut down or destruction of a transportation service due to a terrorist attack.

Risk management in the realm of supply chain management is not new. However, several key developments have advocated the case for increased attention to the management of risk in supply chains (Ritchie and Bindley, 2004):

i. Strategies and structure relating to supply chains are evolving more rapidly in the search for competitive advantage. Table 2.1 lists some of the common supply chain strategies that organizations are adopting today to build competitiveness into their customer fulfilment process.

Table 2.1: Common supply chain strategies.

Design	**Purchasing**	**Manufacturing**	**Inventory Mgt**	**Distribution**	**Facility**
Push/Pull	Collaborate	Lean	VMI	Inter-modal	Lease vs Own
Outsource	Consolidate	Off-Shore	Risk Pooling	Cross-Dock	Network Design
	Multi Source	Just-In-Time	Decentralise	Hub and Spoke	Warehouse vs DC
	Single Source	Postponement	Virtual Inventories	Deconsolidate	
	Global Sourcing	Mass Customise			
	Reverse Auction				

Depending on the strategy(s) that an organization adopts, the organization exposes itself to various types of supply chain risks. For example, an organization facing competitive pressures to lower manufacturing costs may be prompted to outsource their manufacturing activities offshore. As a result, the organization's customer order fulfilment lead time is lengthened and they will have to assume greater capital risks due to the need to hold additional safety stock. The organization also runs the risk of non-supply should their supplier run into production problems and greater order fulfillment cycle time uncertainty due to a more extended supply chain.

ii. With the rapid advancement in telecommunications, Internet and its applications, technological changes provide opportunities to alter the shape and the relationships within supply chain networks.

Technological advancements provide enormous opportunities for companies to revolutionalize their supply chain networks through enriching their supply chain operations with information and integrating stakeholders along the same supply chain. For example, the project to convert NMS Communications to an electronically integrated, demand-driven (build-to-order (BTO)) supply chain was made possible through an extensive integration of trading partners' information systems. The increased real-time visibility allows stakeholders in the supply chain to synchronize their activities, reduce cycle time, and eliminate large buffers of inventory.[3] For instance, the extensive information system integration allows suppliers to see the demand in real time and begin mustering the raw materials needed to respond quickly.

iii. Increased exposure to global competitive pressures means that most organizations are exposed to new and additional risks that may impact more rapidly and with more severe consequences than previously.

With the increase liberalisation in international trade and investments, organizations are experiencing mounting global competitive pressures. A tougher global playing field exposes organizations to disruptions not only on their home country but also those in other parts of the world. For example, the bird flu epidemic in China about four years ago brought chicken exports from China to the rest of the world to a sudden halt. Organizations around the world had to take immediate steps to either assure their customers of the supply source of their chicken meat or find alternative sources of chicken meat (if they had relied on chicken exports from China). Nonetheless, companies such as Kentucky Fried Chicken, who uses a large proportion of chicken meat on their menu, still experienced severe reductions in sales as a result of the bird flu epidemic in China regardless of whether they had relied on chicken exports from China or not.

[3] Supply Chain Management Review, January/February (2002).

2.1.1 What Events Represent Supply Chain Risks?

Supply chain risk is in essence the probability of a supply chain malfunctioning. Therefore any event or activity or action that can lead to the malfunctioning (be it permanently or temporarily) of an otherwise "healthy" supply chain, is one that introduces uncertainty and variability into the supply chain and they represent risks in supply chain management.

There are many ways to perceive and classify risks. Since management attention is a scarce resource, an appropriate and simple approach to classifying risks is based on how manageable they are.

Doherty (2000) defines risk quantitatively as both the range of possible outcomes and the distribution of respective probabilities for each of the outcomes. This is commonly referred to as the "Expected Value". Deloach (2000) classifies risks based on their sources into three categories – (1) Externally-driven or environmental risk, (2) Internally-driven or process risk and (3) Decision-driven or information risk. Deloach (2000) also advocates that risk is dynamic and that risk categories are interrelated, meaning that some risk events could be sources or drivers of other risk events. Jüttner et al. (2002) moved on to suggest that risk sources relevant for supply chains should be categorised into three categories – (1) External to the supply chain, (2) Internal to the supply chain and (3) Network related. Although these classification methods highlights to management, the source or driver of a risk, it does not indicate how preventable (i.e. manageable) a risk is.

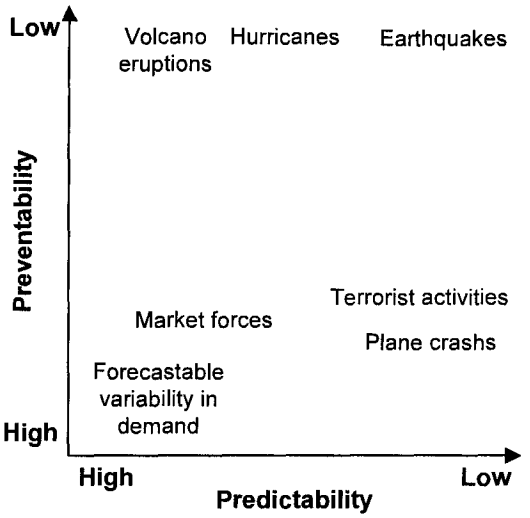
Hiles and Barnes (2001) categorises risks into five core groups – (1) Strategic, (2) Financial, (3) Operational, (4) Commercial and (5) Technical. Hiles and Barnes also indicate that these risk groups are not mutually exclusive. This classification method is based on where a risk has an impact. Although comprehensive in identifying the major areas of impact in a typical organization, this classification method does not guide management to the required or appropriate actions or efforts.

Although dealing with geographical and social risks, Wolpert's 1980 work on risk management lends some insightful ideas to classifying supply chain risks. Wolpert (1980) analysed, by means of case studies, the risk management and prevention of catastrophe caused by institutional and technological hazards. He introduced the concepts of competency and dangerousness into the

discussion of risk management and talked about the effects of the degree of competency or knowlegeability on one's ability to mitigate the potential impacts of risks and disruptions.

The ideas and academic contribution of these earlier works to classifying risks lead the author of this thesis to develop a framework that guides manager's supply chain risk management efforts according to how manageable (i.e. predictable and preventable) they are (see Figure 2.1).

Figure 2.1: Risk classification framework.



This classification framework consists of two dimensions. Both dimensions seek to determine how manageable a particular risk event is or will be.

The first dimension (horizontal axis) is predictability of a particular risk. Wolpert, in his 1980 work on institutional and technological hazards and the mechanisms for risk management and prevention of catastrophe, advocated the importance of the means of predicting, controlling and managing such risks so that their impacts can be curtailed or reduced (Wolpert, 1980). Predictability therefore refers to, how reasonably a particular risk can be anticipated and whether there are reliable tools or processes in place to monitor and anticipate it, such as market research for new market penetration risks, monitoring rain and water levels for flood potentials? This is the ability of the company and/or manager to anticipate or determine the probability of a risk event occurring. As illustrated in Figure 2.1, events that are less predictable if not unpredictable, fall towards the right end of the x-axis and are events that are external to the organization. They are relatively if not impossible to predict. Rare events such as natural

disasters (e.g. earthquakes[4]) and terrorist activities fall into this category. These events are usually catastrophic in magnitude and has either never occurred historically or occurs with such low probability that its next occurrence cannot be predicted (Wolpert, 1980). They therefore disturb our sense of competency and sense of security, stability and permanence and, thereby, threaten a very basic and elemental need and source of satisfaction (Wolpert, 1980).

The other dimension (vertical axis) indicates how preventable a risk event is. This is similar to what Wolpert refers to as competency or knowledgeability. It therefore refers to one's ability to reasonably prevent or minimise the probability of a risk event occurring or the negative consequences of that risk event. Such competency or knowledgeability may be impacted by the existence or lack thereof of risk assessment capabilities. Therefore most of the risks that lie towards the bottom of the framework are either risks that are internal to organization (e.g. operational process risks) or risks that organizations can do something about to mitigate their negative impacts. These risks are usually man-made hazards (e.g. terrorist activities). As opposed to natural disasters, man-made disruptions can be typically subjected to the development of a logic structure which can be used to analyse the preventability of the rare event (Wolpert, 1980).

2.1.2 Managing Supply Chain Risks

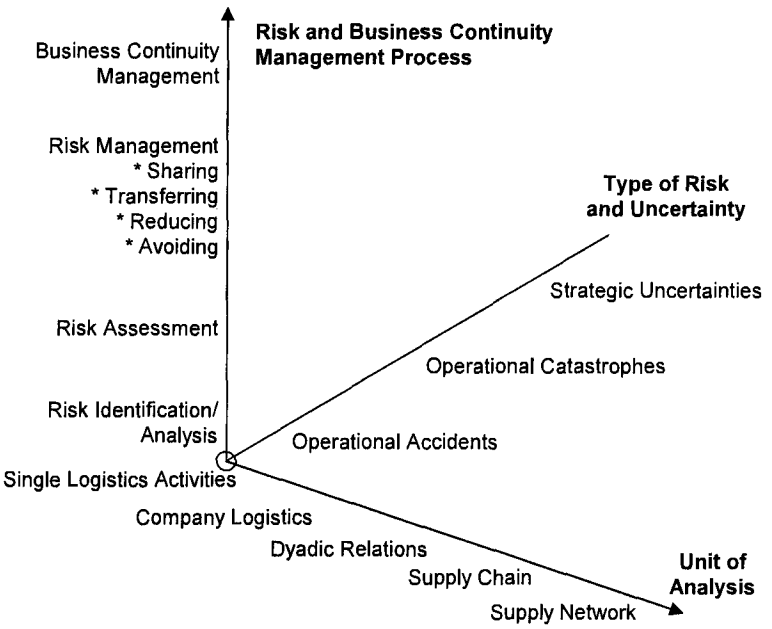
Different types of risks require different levels of management attention and management strategies. Although the study of risk management is not new, there are not many explicit definitions of supply chain risk management. Norrman and Lindroth (2002) defines supply chain risk management as the effort to collaboratively work with partners in a supply chain to apply risk management process tools to deal with risks and uncertainties caused by, or impacting on, logistics related activities or resources.

Subsequently in their 2004 work on supply chain risk and risk management, Norrman and Lindroth proposed a conceptual framework that seeks to categorise supply chain risk management issues (both research and managerial) along three dimensions (see Figure 2.2).

[4] "Although there are successful theory such as plate tectonics to explain why earthquakes happen, scientists still can't say when an earthquake will happen." – *The National Geographic,* April 2006, p. 126.

The first dimension is the logistics unit of analysis which seeks to define how complex the risk at hand is. The unit of analysis can range from a single logistics activity to the entire supply chain network, thereby taking into consideration the rippling effects for organizations in the same supply chain. The second dimension is the type of risk which seeks to define the nature of the risk in terms of whether it is an operational accident (e.g. collapse of a stack of block-stowed cartons and hurting a warehouseman), catastrophe (e.g. warehouse flooding, fires) or a strategic uncertainty (e.g. mergers and acquisitions, new market penetration). The third dimension is the stage of the risk management process, from risk identification and analysis to business continuity management.

Figure 2.2: A framework for assessing and positioning supply chain risk issues.



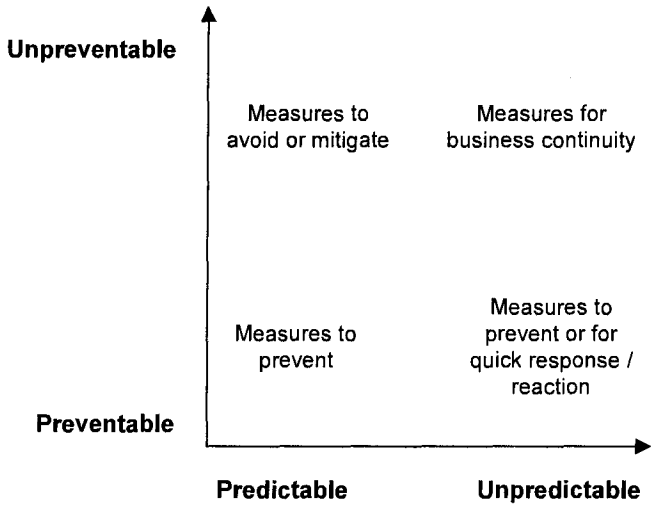
Source: Norrman and Lindroth (2004).

The purpose of this framework is to help position different managerial actions or research contributions in supply chain risk management. However, it does not guide managerial decision making in terms of what efforts or strategies or type of actions to take in response to a particular type of or particular risk.

Based on the proposed classification of the various types of risks in Figure 2.1, a more appropriate management decision guiding tool for supply chain risk management is shown in

Figure 2.3. The supply chain risk management framework in Figure 2.3 allows the management user to determine what type of managerial attention or strategies they should take in response to different types of risks.

Figure 2.3: Supply chain risk management framework.



In response to a risk / disruptive event, an organization may adopt one or more strategies or actions. These strategies or action plans can be classified into four major categories, namely, (1) Prevent, (2) Quick response / reaction, (3) Avoid or mitigate and (4) Business continuity. These are explained and elaborated in greater details below.

Linking the ideas illustrated in Figures 2.2 and 2.3, risks that are preventable and predictable include operational accidents such as the collapsing of a stack of block-stowed cargo, cargo pilferage, incorrect order picking etc. These are risks that one can be sure will occur if due diligence is not done to prevent them. The appropriate approach to managing such risks is to adopt or put in place preventive measures such as process monitoring and control mechanisms. For example, to prevent the negative impacts of receiving the wrong products, there should be tally checks during the inbound receiving process at the warehouse. Ti-Hi guidelines (that is, how many cartons per layer and how many layers to stack on a pallet) can be instituted to mandate how cargo should be safely block-stowed and close-circuit cameras (CCTVs) can be installed in a warehouse to deter pilferages.

Moving horizontally on the x-axis towards the other end of the continuum, risk events get more unpredictable and can include operational accidents such as an employee getting electrocuted due to carelessness, floods or catastrophes such as port closures due to terrorist activities or labour union strikes. Training and rigorous handling procedures may prevent carelessness but not eliminate or make accidents more predictable. Many of the process and infrastructural changes made by organizations seeking C-TPAT certification or shipping lines meeting the security requirements of the World Maritime Organization (WMO) seek to reduce the probability of successful terrorist incidents. For risks that are can be reasonably predicted although not with perfect certainty, one can undertake reasonable measures to prevent or respond quickly to their negative impacts. For instance, if a particular river is expected to flood every year during the monsoon season, an organization can either relocate its warehouse (that is, prevent) or set up barriers around the warehouse during the high-risk season to prevent flooding. For risks that are practically unpredictable or cannot be reasonably predicted but preventable such as terrorist events, organizations should have in place quick response plans such as evacuation for catastrophic disasters and exception management capabilities such as having alternative shipping routes or carriers in the event of port closures. They should also have in place robust risk assessment tools to competently reduce the dangerousness of such rare events.

Moving diagonally across the grid, we have risks that are unpreventable but predictable and these risks usually refers to natural disasters such as volcano eruptions and hurricanes. They can also include strategic uncertainties such as interest rates changes by the Federal Reserve or a relatively obvious impending increase in the price of oil. These are events that can be reasonably predicted but one cannot prevent them from happening. As such, in response to such risks, organizations should undertake measures to either avoid (e.g. refrain from locating your facility near volcanic mountains or flood-prone rivers) or mitigate (e.g. undertake sound hedging options) their negative impacts.

The top right hand corner of the framework illustrates risks that are both unpredictable and unpreventable such as earthquakes. Earthquakes are still one of the most catastrophic natural disasters that scientists are still unable to predict and such can be considered strategic uncertainties as well. For example, the Kobe earthquake on January 17, 1995, indirectly[5] brought about the collapse of United Kingdom's oldest investment bank - Barings Bank. The

[5] Coupled with the unsupervised speculative trading of Nicolas Leeson, Baring's appointed manager of a new operation in futures markets on the Singapore International Monetary Exchange (SIMEX).

collapse of the World Trade Center on September 11, 2001 destroyed the extensive computer networks and databases of many international investment companies whose operations depends largely if not solely on these information systems. It also led to the immediate closures of all major ports and airports in the U.S., halting many international movements of cargo. For disruptive events such as these, organizations should have in place measures for quick operations recovery and business continuity such as backup for its organization-wide information technology systems.

In summary, one can see that operational accidents, operational catastrophes and strategic uncertainties can fall anywhere on the predictability and preventability continuums. However, the more unpredictable a risk, the more catastrophic it's impact. Therefore, there is an essential need for organizations to be cognizant of the types of risks that their business operations are exposed to and take appropriate measures to manage them.

2.2 Supply Chain Security Risks

Since the terrorist attacks on the U.S. soil on the 11th of September 2001, there has been a tremendous amount of renewed interests in the study of risk management in supply chain management especially in the areas of trade security and safety.

The U.S. is the largest trading nation in the world for both imports and exports. Accounting for nearly 20% of world trade in goods, the combined value of US imports and exports of goods in 2004 was approximately US$2.23 trillion[6]. It is therefore small wonder why the terrorist attacks in New York and Washington in 2001, have created an unprecedented sense of urgency for all governments of countries worldwide which are engaged in international trade to look into improving international trade security, especially in terms of the physical movement of cargo.

Coupled with recent series of security breaches and disruptions that threaten the national security of many countries, such as the Madrid bombing in 2004, the Asia tsunami in December 2004 and the London attempted bomb attempt in 2005, business managers throughout the world have recently become more sensitised to the vulnerability of their supply chains. As

[6] Statistics from the World Shipping Council at http://www.worldshipping.org.

described by former U.S. Customs and Border Protection (CBP) Commissioner[7] Robert Bonner, "A terrorist attack using a container to conceal a so-called dirty bomb...could probably stop global trade in its tracks unless we have a maritime security system that can detect and deter such an attack." (Langhoff et al., 2005).

2.2.1 What are Supply Chain Security Risks?

Security as the word is defined means:

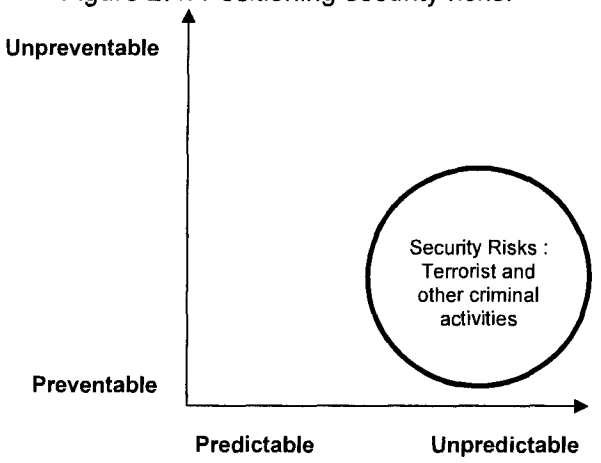
- freedom from risks or danger (i.e. safe),
- freedom from doubt, anxiety or fear (i.e. reliable)
- or measures that give or assure safety and prevent sabotage or attacks or other forms of criminal activities.

Security risks or security breaches are a subset of supply chain risks and are those events that threaten the safety, reliability and flexibility of the supply chain or its constituent parts. It includes mainly but not limited to, events such as contraband smuggling, theft of goods and vehicles, fraud, illegal immigration, drug smuggling, potential targeting of dangerous goods shipments and the targeting of transport vehicles and infrastructure by terrorists and last but not least, the use of one's supply chain as a delivery vehicle for chemical, biological, radiological or nuclear (CBRN) weapons. Using the risk classification framework in Figure 2.1, security risks are classified as unpredictable but preventable (see circle in Figure 2.4).

As noted by Wolpert (1980), one of the major distinctions between man-made rare events which can lead to catastrophe and the natural hazards is the notion that the event is possibly preventable. This is because as mentioned earlier, man-made or institutional hazards are typically subjected to the development of a logic structure which can be used to analyse the preventability of the rare event. Risk assessment methods such as fault-tree analysis, can be and have been used to establish a classification of some potential accident sequence and permit identification of procedures for estimating risks associated with these sequences (Wolpert, 1980). Also, depending on the effectiveness of the security measures and/or technologies adopted, these risks can reasonably be expected to be preventable.

[7] On 6 June 2006, W. Ralph Basham has sworn in as the new CBP Commissioner.

Figure 2.4: Positioning security risks.



These illegal activities pose serious daily problems for authorities and can have important impacts on a supply chain's ability to fulfill the 7R's[8] (Right product, Right place, Right time, Right quantity, Right condition, Right cost, Right customer) of supply chain operations.

2.2.2 Classification of Supply Chain Security Risks

Combining and summarising the classification ideas and perspectives mentioned earlier, there are several ways of classifying supply chain security risks (see Table 2.2).

Table 2.2: Classifying security risks.

Classification	Description
By nature of the security risks	• Controllable / uncontrollable • Internal / external • Human Inflicted / Natural Disasters
By the supply chain management area that the risk is impacting	• Demand security (unexpected surge in demand due to a security threat) • Supply security (unexpected cut in supply due to a security threat) • Conveyance security (unexpected denial of conveyance due to a security threat) • Information security (loss of access or theft of important information due to a security threat) • Financial security / cash flow security (loss of access to funds due to a security threat) • Operations security (loss of ability to operate or continue business due to a security threat) • Human resources security (loss of or loss of access to manpower due to a security threat)

[8] Page 6-7, Coyle et al. (1992).

Table 2.2 (continued): Classifying security risks.

Classification	Description
By type of impact	• Destroy (unrecoverable) • Disrupt (short term recoverable) • Paralyses (long term recoverable) • Slight tremors (immediate term recoverable / unaffected)
By types of reaction necessary	• Prevent • Quick response / React • Avoid • Mitigate

2.2.3 The Public Sector's Take on Supply Chain Security

> "For the first time in our nation's history, one agency has the lone responsibility for protecting our borders. As the single, unified border agency, CBP's mission is vitally important to the protection of America and the American people. CBP's priority mission is preventing terrorists and terrorist weapons from entering the United States, while also facilitating the flow of legitimate trade and travel."
>
> - Robert C. Bonner
> Commissioner of U.S. Customs and Border Protection (CBP)

Sheffi (2001) noted that much of the disruptions to the private sector after the 9/11 attack were not caused by the attack itself, but rather by the government's response to the attack – closing borders, shutting down air traffic, and evacuating buildings throughout the country.

Therefore since 9/11, the public sector, especially in the U.S., has taken unto itself a lot of initial responsibilities for instituting measures to improve national security[9]. With the responsibility to protect the public and their interests, the U.S. Federal government has taken steps to improve national security in the following ways[10].

- Improved their radiation detection capabilities by deploying 10,400 Personal Radiation Detectors to their officers and agents, more than 274 Radiation Portal Monitors to ports of entry, and in excess of 60 Radiation Isotope Identification Detection System to Border Patrol field locations.

[9] http://www.cbp.gov.

[10] <<Executive Summary CBP Actions Taken Since 9/11>>, word document posted on September 17, 2004 at http://www.cbp.gov/xp/cgov/toolbox/about/accomplish/.

- Improved inspection capabilities by deploying 87 additional non-intrusive inspection systems to detect terrorist weapons in vehicles and cargo.
- Improved remote monitoring, detection and illegal crossing response capabilities by increasing the use of remotely monitored cameras and sensing systems, aircraft, helicopters and unmanned aerial vehicles.
- Improved selectivity, screening and targeting by establishing the National Targeting Center as the centralized coordination point for all CBP's anti-terrorism efforts and implementing the 24-Hour Rule in December 2002 to obtain advance information to screen and assess all cargo, passengers and high risk imported food shipments before arrival into the United States.

The government also made efforts to work with the private sector and governments of other countries by establishing the C-TPAT program to emphasize a seamless security conscious environment throughout the supply chain and the CSI program to target and screen containers prior to them being loaded onto vessels destined for the U.S.

New security measures following the 9/11 events, are estimated to cost the U.S. economy alone over US$150 billion, of which US$65 billion is for changes in supply chains (Bernasek, 2000; Damas, 2001).

Internally, the government also made efforts to restructure themselves in order to better respond to any form of security breaches especially terrorist attacks. Since 11 September 2001, the U.S. government has successfully integrated four different organizations from three different departments into CBP. They have subsequently converted more than 18,000 Customs, Immigration and Agriculture Inspectors to two new positions – Customs and Border Protection Officer and Agriculture Inspector, thereby fully integrating the inspectional functions of CBP's legacy inspectors.

However, despite all these efforts, to date, the public sector still views supply chain security as pretty much the responsibility of the private sector. Governments have in essence 'contracted' out some responsibility in managing supply chain security to the private sector, in hope that the private sector can come up with innovative solutions (Chow et al., 2006). This can be seen from a couple of the key security regulations that they have since developed to counter terrorism and other acts of security breaches.

First, it's asking the private sector to assume legal responsibility for their supply chain security. Legally (and pre-9/11), an organization is responsible for a container only when it formally purchases it, which; precisely for that reason; usually doesn't occur until it reaches the destination port, either in the U.S. or abroad (Worthen, 2006). However, since the September 11 attacks, the government has instituted the C-TPAT program, which mandates importers to take responsibility for everything that occurs prior to purchase, even if the container is in the custody of a trucker in China or a longshoreman in Panama. The program is still very much voluntary and gives certain benefits, such as reduced inspections, to organizations that are able to show that they meet a minimum level of supply chain security.

C-TPAT seeks to certify known shippers through self-appraisals of security procedures coupled with Customs audits and verifications (Closs and McGarrell, 2004). There are currently three tiers of C-TPAT compliance, and containers belonging to members in the top tier sail through Customs virtually un-inspected. The first level simply requires an attestation that the company has performed a risk analysis of your supply chain and has taken steps to mitigate any vulnerabilities. By far, 5,757 of these attestations have been accepted by the U.S. Customs (Worthen, 2006). The second level requires that members have this attestation validated by Customs officials and so far, 1,511 organizations have achieved tier-two. Tier-three members are organizations that the U.S. Customs has determined to follow supply chain security best practices (although the U.S. Customs has not yet defined any) and these organizations are eligible for the Green Lane (Worthen, 2006). As of March 2006, only 126 organizations have qualified for this level, including Boeing, General Motors and Target.

Second, the public sector requires organizations to put in place reasonable safeguards against events that could materially affect the organization's value. The principle vehicle for this is the Sarbanes-Oxley Act (commonly known as SOX or Sarbox).

Third, the introduction of the Advanced Manifest Rule (AMR) and the more recent Advanced Commercial Information (ACI) requires shippers to submit detailed cargo data before the cargo is brought into U.S. and Canada respectively, by ocean, air, rail or truck. Since information needs to transfer from the private organization to government authorities in a timely manner, compatibility in technological standards is very important.

Despite all these compliance requirements, to date, the public sector has yet to make any clear indications in terms of the future standards of security technology and practices.

2.2.4 The Private Sector's Take on Supply Chain Security

The influx of compliance requirements may have pushed many organizations to step up on their supply chain security efforts but the compliance theory does not serve to fully account for the private sector's hesitation in investing in supply chain security for their self-interests. Rice and Spayd (2005) and Langhoff et al. (2005) has indicated that although there is a clear need for increased security in global supply chains and organizations are tasked to make appropriate supply chain security investments[11] to protect their assets and operations for their own private interests, there has been much hesitation among industry players. And there are several key reasons for this phenomenon.

Firstly, the nature of the costs and benefits from security investments are such that they suggest largely public effects which are externalities to private interests. Security improvements or lack thereof, come at a cost. A private-sector analysis conducted by the International Monetary Fund (IMF) estimates the increase to business costs due to higher security costs at $1.6 billion per year, the extra financing burden of carrying 10% higher inventories at $7.5 billion per year.[12] Another study estimates an increase in commercial insurance premiums of 20% at about $30 billion a year (Pelg-Gillai et al, 2003).[13] The results and conclusions from these studies also suggest that the private sector seems to consider holding additional safety stock and increasing insurance coverage as measures to improving security in their supply chain. If this is so, it is then small wonder that the private sector sees little "natural" business incentives to undertake more direct and sophisticated security improvements such as container tracking technology and electronic seals and undertake them out of self-interests.

---

[11] Supply chain security investments range from capital equipment, human resources, process changes and/or improvements and operating expenses for a range of activities including physical security improvements, monitoring and incident investigation.

[12] IMF Website, "World Economic Outlook: The Global Economy After September 11." December 2001. http://www.imf.org/external/pubs/ft/weo/2001/03.

[13] UBS Warburg, 2001.

The lack of public sector's directions for standards amidst of the influx of technologies only serves to make matters worse. The general lack of standards (especially for technology) and international jurisdiction is validated by the 2005 study done by Langhoff et al., which conducted multiple workshops with key industry stakeholders. The study found that although key industry stakeholders such as customs brokers, logistics service providers and shippers, feel that the International Ship and Port Facility Security (ISPS) code, World Customs Organization (WCO) framework, and the U.S. CBP's security pillars (i.e. CSI, C-TPAT and Advanced Trade Data) provide the right foundation to build a secure system of trade, improved execution needs to follow. And the public sector must lead and articulate a clear vision or the private sector will continue to delay investments in security.

Another reason for the private sector's hesitation is their difficulty in calculating the Return on Investment (ROI) for security investments (Closs and McGarrell, 2003; Rice and Spayd, 2005; Peleg-Gillai et al., 2006). Traditional ROIs of business investments focus on cost savings or avoidance but this is certainly not the case for security investments. This is because security improvements cannot be assessed for their effectiveness until something bad happens while the very purpose of investing in security initiatives is to prevent something bad from happening. And in most cases, other than theft reduction where there is tangible evidence of improvements when loss levels are reduced, it is difficult to measure the cost of a security breach or disruption that did not occur (Rice and Spayd, 2005).

Besides there is also currently no established or recognized way of measuring supply chain security performance. Without the ability to measure what one is trying to improve, organizations are finding it hard to build a business case for supply chain security investments. Although some focus was given to the importance of customs cycle time in the latest version of the Supply-Chain Operations Reference (SCOR version 8.0) model, the security dimension has not been incorporated into its performance metrics and best practices. And since SCOR is developed by a large team of private sector personnel and executives, this could suggest that security is still not considered as an important element in supply chain management benchmarking and best practices.

In addition, the fact that certain investments in traditional supply chain operations such as visibility tools, can easily spill over to affect the security of a supply chain, makes it even harder for private organizations to isolate the benefits of security investments. The ROI for one

organisation's security investments is a function of the spill-over effects from the security investments from the other players operating in the same supply chain. As Closs and McGarrell (2004) puts it "Not only must firms be concerned about security procedures within their own processes and those of first-tier suppliers, but also they are dependent on the security procedures throughout the entire supply chain". This also creates "free-rider" problems wherein those who do not invest can still benefit (Willis and Ortiz, 2004).

Therefore, one can see that despite having a common goal to conduct trade and business securely, there are considerable discrepancies between how the public sector and private sector views supply chain security investments and initiatives. For the profit-driven private sector, although they face the challenges of preparing for another attack, managing supply chains under increased uncertainty and increased complexity in their relationships with the government in this new era, the self-interest theory still has it that there clearly needs to be stronger incentives (be it monetary or non-monetary) for security investments. And the public sector as the authority with the ultimate jurisdiction should work jointly with the private sector, to look into how best these incentives can be provided or created.

2.3 Managing Supply Chain Security Risks

To manage supply chain risks is to become informed about security hazards, to know and be able to make good decisions and/or take appropriate actions to avoid, prevent and/or mitigate them. Supply chain managers therefore need to adopt a range of strategies from preventive to reactive / repair measures (refer to Figure 2.3).

An effective response to security threats and breaches thus involves a number of steps. First, taking preventive measures such as: (1) predicting actions through intelligence such as an appropriate adoption of intelligent freight information technologies that will allow the organization to track and be alerted in advance of any forms of intended foul play, (2) preventing actions by containment through the institution of necessary monitoring and control mechanisms and ensuring compliance with various security regulations, (3) protecting targets by enhanced physical measures and (4) interdicting attacks as they occur. Next, taking reactive / repair measures such as: (1) responding post-attack to minimize damage and disruption through having business continuity action plans and (2) identifying the perpetrators of attacks to support targeted retaliation.

2.3.1 Mitigating Supply Chain Security Risks

Langhoff et al. (2005) also found the following from their analysis of container movements and workshops with key industry stakeholders:

- Leave the container alone. Most technologies are not commercially viable and Container Security Devices (CSDs)[14] are the only viable container technology in the near-term
- Stakeholders agree that improved information sharing and profiling are the most important security controls
- Overseas commercial intelligence must be integrated and shared across the private and public sectors...

There is no easy solution, silver bullet technology, single policy or regulation that can comprehensively address this challenge. Supply chain security can only be achieved through practical solutions and effective collaboration between public and private sector stakeholders (Langhoff et al., 2005). Closs and McGarrell (2004) advocates that government agencies responsible for the movement of goods and people across borders must continuously review and update security procedures with the goal of enhancing both security and efficiency. This includes balancing the essential governmental obligation to protect citizens with the critical role of promoting economic viability through trade. Private sector's security improvements must also go beyond the organization itself and extend throughout the supply chain (Closs and McGarrell, 2004). The improvement focus should also be global, with the goal of expanding the number of trusted partners to enhance global trade.

Complying with Security Regulations

An organization's first step to improving supply chain security is to ensure compliance with any mandatory security regulations. Ensuring compliance and requiring compliance from other partners in the supply chain also helps build the necessary trusted partner network for an organization's supply chain. This is a new business reality and stakeholders in the supply chain and transportation sector cannot afford to take a lax approach towards compliance.

[14] CDSs reside on the inside of the container and detect unauthorized breaches or openings of container door. They communicate via hand-held or fixed readers over a given wireless range (Langhoff et al., 2005).

The events of 11 September 2001 in New York and Washington has served as a catalyst for a new wave of heightened security measures at international, national and local levels (ECMT, 2005). These new measures have been designed to take stock of the security weaknesses revealed in the 2001 attacks; specifically, they aim to minimize terrorist threats, share good practices and assess necessary technical, legal and legislative adjustments to ensure maximum protection from terrorist activity in transport (ECMT, 2005). The public sector's efforts in countering security breaches in the transportation sector primarily aim to reduce the "haystack" (i.e. the number of suspicious containers that they will need to inspect).

The importance of security in the current regulatory environment cannot be overstated (Chow et al., 2006). There are many new security regulations today and some overlap. Some pre-September 11 programs have also either been fully decommissioned or have been integrated into new programs. Of the current 38 new security regulations related to international trade movement (Chow et al., 2006), 17 of them were initiated by the U.S. CBP, two initiated jointly by the U.S. CBP and the Canadian Customs Border Service Agency (CBSA) and Immigration Canada, four initiated by the CBSA, three initiated by the International Maritime Organization (IMO), four initiated by the U.S. department of homeland security and eight by other stakeholders in the community such as port terminals and other federal departments in the U.S. government[15]. Many of these regulations and initiatives seek to increase data collection and availability and security monitoring. Chow et al. (2006) contains details of these regulations and their implications on supply chain management.

Ensuring corporate-wide compliance with these measures has now become an imperative for organizations engaged in international trade (in one way or another) especially with North America and taking this first step will, at the very least, ensure that an organization's supply chain flow will not be unduly delayed.

Even so, there are advocacies against compliance with these mushrooming new regulations. Instead of helping organizations move towards more secure networks, Piazza (2006) advocates that complying with these regulations may be having the opposite effect. This is similar to the concept of risk tradeoffs analysis commonly known in the healthcare industry where regulations undertaken to minimize or eliminate certain health risks often have the perverse effect of

[15] Other organizations include the Food and Drug Administration (FDA), the Department of Defense, the Transportation Security Administration within the Department of Homeland Security, Federal Aviation Administration (FAA) and the Federal Bureau of Investigation (FBI).

promoting other risks (Rascoff and Revesz, 2002). Viscusi and Gayer (2002) writes about how health and safety regulations have often fallen short of any reasonable standard of performance and how economic findings with respect to risk-risk tradeoffs highlight the fallacies inherent in a zero-risk mentality. Rather than focusing regulations on instances of market failure, the emphasis is on reductions of risks irrespective of cost (Viscusi and Gayer, 2002). Health and safety regulations that have the current inordinate imbalance between costs incurred and risk reductions achieved divert society's resources from a mix of expenditures that would be more health enhancing.

Similarly in supply chain security regulations, certainly more time is being spent on compliance than ever before. In terms of physical security, several publications have mentioned that despite the efforts spent on security thus far in terms of compliance are not making their supply chains any more secure than before. In her letter to The Council of Ministers at the Council Working Group September 4-5, Tina Sommer, President of the European Small Business Alliance said "We are concerned that the struggle to defeat terrorism, which we all of course support, is being misused to create a heavy-handed and bureaucratic system that will put many people out of work without actually increasing security." Tom Gould, a C-TPAT consultant with the Zisser Group in Los Angeles also said "I'm talking to people all the time who make comments like "We're no more secure than we were before 9/11." (Edmonson, 2006). Another cargo industry executive was quoted saying "Shutting down our commercial supply chains is one of the goals of terrorists. Wouldn't some of these legislative proposals do exactly that?" (Page, 2006). In an e-mail poll done by Journal of Commerce (JoC) to subscribers, when asked to rate the probability of such an attack on a scale of 1 to 10[16], 30% rated the probability at 5 and above. Only 3% rated it 1 (Edmonson, 2006).

In terms of information security, a survey done by Forsythe Solutions Group on 100 senior IT and data security professionals at Fortune 1000 companies across the U.S. found that 43% of respondents cited legislation-induced triumvirate of policy, process and procedures as their top priority. And majority of the respondents cited that they have or are in the process of planning for encryption, enhanced security awareness programs, and updating incident response plans and authentication processes. However, 28% of the respondents cited that they have little or no confidence that they had detected all significant security breaches in the past year and rated their current IT environment as more vulnerable than a year before. This, according to John

[16] Where "1" corresponds to 0% probability and "10" correspond to 100% probability.

Kiser, CEO of Gray Hat Research Corporation, may be a sign that time or money spent on ensuring compliance to top management are resources taken away from other crucial security tasks.

But it is also important to note that the current governmental regulation evaluation tools, known as "regulatory scorecards" may be fundamentally flawed in themselves. Parker (2003) demonstrated how three regulatory scorecard studies[17] are fundamentally flawed in terms of their use of undisclosed data and non-replicable calculations, biased regulatory samples, misrepresentation of ex ante guesses about costs and benefits as actual measurements and grossly underestimation of benefits, exclusion of all unquantified costs and benefits and disregards for all questions about the fairness of the distribution of cost and risk. Due to their fundamental flaws, Parker (2003) advocates that these studies prove nothing about the rationality of regulations.

Employing Intelligent Technology

According to Caton (2004), government agencies acting under the premise that they are protecting the U.S. from terrorism, are developing requirements that do little for security but will have a serious impact on foreign trade. Each agency has a specific responsibility, yet many of the regulatory issues overlap. The result is confusion that will do more harm than good for the US economy. Paper security (that is, by simply providing more information about the shipment) is relatively insignificant and can be easily circumvented. Therefore, any plan that does not include more physical inspections, along with the use of more sophisticated detection devices, is only as good as the paper it generates. The only real protection against terrorism is using advanced, strategically re-engineered technology to detect potential harm and to provide alerts.

Along with the heightened emphasis on secure trade movement is an influx of intelligent transportation systems, which seeks to enhance the secured movement of freight while improving freight movement efficiency. These technologies can be generally classified into five major categories based on their primary purpose/function – (1) Detection, (2) Sensoring / Identification and Monitoring, (3) Locking and Securing, (4) Access Control and Personnel

[17] Parker (2003) cites: A study by John Morrall, an OMB economist, claims that government regulations cost up to $72 billion per life saved. Another study, co-authored by Bush's regulatory "czar," John Graham, claims that over 60,000 people lose their lives each year due to irrational government regulation. A third study by Robert Hahn of the AEI-Brookings Joint Center for Regulatory Studies claims that over half of all major regulations issued since 1981 fail cost-benefit tests.

Security and (5) Backup and Protection. Most if not all of these intelligent transportation systems claim to enhance the security of an international supply chain while improving its efficiency. Table 2.3 provides some examples consolidated from volume 50, issues 4 to 6 of the Security Management magazine.

Table 2.3: Examples of freight security technologies.

Category	Name	Description of Capabilities	Application
Detection	Mobile NBC Reconnaissance Robot	- highly perceptive sensors - determine type and concentration of gases while simultaneously transmit video images from location to a control center	Container inspection at port or other container rest points.
	MVXR5000 Multi-View X-Ray (for Explosives Detection)	- provides enhanced image and dual energy x-ray images enabling automated detection of explosives materials - process up to 1,800 bags per hour	In line hold baggage system
	OmniView Gantry Inspection System	- scanning platform operates by moving on rails past stationary vehicles and cargo - compact footprint accommodates limited space in congested areas and minimise radiation zones - bi-directional, multiple views. provides high energy penetration of densely loaded cargo	Detecting security threats and contraband in cargo and vehicles
Sensoring and Identification / Monitoring	Exit Sensor	- combines radar motion sensing and lens passive infrared (PIR) technologies - uses physical motion and heat to trigger device, thus resisting common attempts to defeat sensors using only PIR. - limits duration door can be opened	Facilities containing highly sensitive information, cargo or materials.
	IP Video – Omnicast 4.0	- enables citywide video surveillance by managing multiple independent systems from numerous organizations as a single, unified security system, real time	
	LifeTrak Real-Time GPS Tracking System	- reports time, location, speeding violations and ignition on/off for vehicles in real time for effective management of cars and trucks - GPS, 24/7 control center monitoring, notifications to cell phones or email of unauthorised usage and optional real time messaging between dispatchers	Fleet management and theft prevention and facilitates recovery of stolen vehicles

Table 2.3 (continued): Examples of freight security technologies.

Category	Name	Description of Capabilities	Application
Sensoring and Identification / Monitoring	secureCam (housing for CCTV)	- made of heavy gauge stainless steel - protects preset bearing with tamper resistant bracket mount. withstands hurricane-force winds, torrential rain and corrosive environments	Protect cameras at terrorist targets and high-crime locations
Sensoring and Identification / Monitoring	RoomGuard	- installed in a room and constantly monitors for illicit listening devices by detecting unusual radio frequency activity - can work online/offline. Using distributed intelligence, monitor several rooms simultaneously over a network or remotely	Facilities that are potential terrorist targets or in high-crime locations
	ASI 2000 Security Integrator Version 3.11	- includes new audit capabilities for improved user accountability, database partitioning options for restricted viewing of cardholder records, a new hot key for instant access to frequently used transaction activity screens and a real-time master report	
	Combi-Booster LEGiL (auto long-range vehicle identification)	- in-vehicle mounted device based on RFID smart card technology - using directional beam, can identify vehicles up to 10m away at high speeds and solve multilane, entry and exit reader challenges encountered in parking lots and secured areas	Control vehicle access to facilities/gated areas such as air and sea port. Use for automated parking payments, fleet management, and toll collections
Lock / Secure	Electric Lockset (for doors)	- offers a choice of failsafe or failsecure mode. clutch for vandal resistance and dual 12 and 24 Voltage Direct Current (VDC) power input - assess control or key entry	Securing container at origin or sensitive handoffs.
	NO-REZ Security Seals	- printable and adaptable to die-cutting adhesive seals that detect tampering without leaving residue on the container - when seal is tampered with, it displays the message "VOID OPEN VOID", informing inspectors that a break-in has occurred - can be used with most conventional label dispensing devices and in conjunction with other sealing products	Single-use decals, such as parking validations, and seals for data ports, envelopes, and documents

Table 2.3 (continued): Examples of freight security technologies.

Category	Name	Description of Capabilities	Application
Personnel Security / Access Control	Visitor Signature Tablet	- preconfigured for use with visitor management solutions - interactive LCD to capture signatures - programmed to automatically display NDAs[18], SCAs[19] and other notices	Facilities containing highly sensitive information, cargo or materials
	MAPSANDS	- modular perimeter security and non-lethal defense system - includes software, wireless communications, remote power systems, detection and tracking sensors, directed energy acoustics and a suite of non-lethal munitions - relies on advanced radars to detect and track intruders and aim acoustic devices that deliver clear verbal warnings and aversive warning tones	Secure perimeters that range from < 1 mile in length to several hundred continuous miles e.g. sovereign borders, power plants, pipelines, seaports and other high value facilities
	Iris on the Move (biometric identification)	- powerful, accurate and reliable capture of subject's iris image while in motion - allows up to 20 subjects per min	Facilities with highly restricted access
Backup / Protection	DSC GSM universal wireless alarm communicator	- connects alarm control panel to the GSM network. When alarm is triggered, the communicator assesses its connections to the phone line. If line is disrupted, it connects to GSM network to send an alarm signal to central monitoring station - operate as an SMS dialer to automatically dial up to 8 phone numbers to deliver alarm message - can control externally connected devices such as lights and powered gates via SMS messaging though cellular phones	Backup to traditional phone lines against accidental line cuts caused by storms, construction, or tampering
	Mobile Guard Shelter	- bullet-resistant booth mounted on a double-axle, heavy-duty trailer. - equipped with a rooftop air conditioning unit and a platform-mounted generator to create an immediate security checkpoint.	For trailers on long hauls deliveries

A report – Review of ITS Technologies with Application to the Security and Efficiency of Cross-Border Freight Movement, by Chow et al. (2006) contains a comprehensive review of available intelligent transportation systems for secure freight movement. Specifically, the study reviewed

[18] Non-disclosure Agreements.

[19] Security Consent Agreements.

custom trade compliance systems, pre-screening and pre-processing systems, in-bond cargo systems, and supply chain cargo tracking systems. It also examined the technologies that are used to support these systems, namely, electronic data interchange (EDI), web-based interfaces, radio-frequency identification (RFID), dedicated short-range communication (DSRC), transponders, e-seals, global system for mobile communications (GSM), global positioning system (GPS) and risk assessment systems.

Instituting Secured Processes (TQM Concepts)

Regardless of the type of freight security technology used, the security efforts in a supply chain can only be as effective as the process of freight movement itself. Some of the principles of total quality management (TQM) can and should therefore be applied to guide an organization's efforts towards creating a secured supply chain (Lee and Wolfe, 2003). Table 2.4 lists the features of TQM.

Most if not all of the TQM principles listed in Table 2.4, should be applied to an organization's efforts for continued improvement in freight movement security. First and foremost, the goals and values for a secured supply chain should be provided and championed by top management, who must recognise that security is a long term strategy and any analysis and decisions should be at the group / organization level. The employees within the company should then be provided with the necessary skills and tools, guidelines and empowerment to innovate and implement security best practices. Measurement, monitoring and benchmarking should also be in place to ensure operational effectiveness of any security efforts. Last but not least, efforts should also be invested to archive the security knowledge and best practices to facilitate transfer of knowledge and continuous learning. In summary, global logistics security systems can learn form the quality movement by focusing on "prevention" and adopting the "total supply chain" approach (Sheu et al., 2006).

Table 2.4: TQM features.

Sub Systems	Basic Variables	TQM Features
Governance	Time perspective	Medium / long term
	Level of analysis	Group and organization
	Empowerment	Oriented to improvement of customer service
	Decision-making focus	Tending towards perfect rationality
	Innovation	Continuous and incremental changes
	Objectives	Priority given to efficiency
	Orientation of the culture	People / employees as a resource
	Content of the culture	Professional development
Goals and Values	Origin of the shared vision	Provided by the leader
	Content of the shared vision	Specific and oriented towards quality in a general sense (multiple dimensions of quality) Achievement of excellence
	Styles of learning	Implicit and adaptive (single loop learning)
	Transfer of knowledge	Exploitation of professional knowledge
Psychosocial	Processes associated with learning	Intuition (expert) Interpretation (specialist) Integration (formal) Institutionalisation
	Consideration of mental models	Implicit
	Type of structure	Organic
	Linking mechanisms	Expert coordination
Structural	Team working	Improvement teams and quality circles
	Cause-effect analysis	Static and more effective at the operational level
	Focus of anticipation of customer needs	Explicit
Operational	Critical techniques	Quantitative, analytical, positive
	Analysis and diagnosis	Emphasis on retrospective approach (measurement, self monitoring, benchmarking)

Source: Ferguson et al. (2005).

2.4 Security Risks in an International Maritime Supply Chain

It is estimated that as many as 25 different parties are involved in the global movement of a container (buyers, sellers, inland transportation service providers, ocean carriers, middlemen such as customs brokers and banks, government) (Russell and Saldanha, 2003; Sheu et al., 2006). As products and information travel through those parties, the potential increases for loss of information, damage to products and delay. Companies operating within this complex network also experience more complex barriers including documentation requirements, transportation modes, information processing and varying regulations (Sheu et al., 2006). For instance Cassidy (2003) cited that a typical cross-border transaction might involve filing 35

documents, communicating with 25 parties and complying with more than 600 laws and 500 trade agreements.

The ocean transportation supply chain, with its many stakeholders and handoffs, therefore exhibits many of the security risk issues and characteristics mentioned above.

2.4.1 Relative Importance of Maritime Transportation

There are more than 2,000 ports in the world, from single berth locations handling a few hundreds tons a year to multipurpose facilities handling up to 300 million tons a year. More than 80% of international trade with origins or destinations in developing countries, in tonnage, is enabled by ocean conveyance[20].

The U.S. alone operates about 15% of all the ports in the world. Of the combined value of U.S. imports and exports of goods in 2004, approximately US$948.7 billion was international trade moved via ocean conveyance arriving at or departing from U.S. ports. And US$521.4 billion, or 55% of that, was containerized cargo carried on liner vessels. This averages out to about US$1.43 billion worth of containerized goods moving through U.S. ports each day. Additional waterborne U.S. imports and exports worth roughly US$30 billion were transshipped via Canadian and Mexican ports.

As at the beginning of 2005, the worldwide fleet of ocean containers in circulation is estimated to be about 13 million, with overall capacity of approximately 20 million Twenty Foot Equivalent Units (TEUs).[21] It is estimated that there are more than 4 million containers in use at any given time in the U.S. trades.[22] In 2004, more than 23.5 million TEUs of containerized cargo were imported or exported from the U.S. on roughly 1,050 different individual containerships making more than 18,000 total port calls.[23]

---

[20] Statistics from http://www.ibm.com

[21] Statistics from http://www.ibm.com.

[22] Statistics from http://www.ibm.com.

[23] Statistics from http://www.ibm.com.

Growth in global container trade was 12.6% in 2004, while shipping capacity rose by around 8%. With the addition of global shipping capacity, as a result of the launch of more than 100 vessels in the coming two to three years and also the introduction of larger vessels with capacity of 8,000 TEUs or more, we can expect to see continued growth in global container trade as shipping rates adjust themselves according to the laws of demand and supply.

It is no doubt that ocean shipping is a key lubricant of international trade and the attributes of the transportation system are precisely what make it attractive as a terrorist target. It is open and accessible, by design. Ocean shipping is global in its reach but institutionally diverse with many providers and operators. And it can be brutally efficient, whether moving sneakers or weapons of mass destruction. The sheer scale of ocean conveyance operations thus presents numerous opportunities for foul play and enhancing the security (and safety as a spill over effect) of container trade movement is therefore an emerging imperative for organizations.

2.4.2 Potential Security Breach Points

Anonymity of contents, opaque ownership arrangements for vessels, and corruption in foreign ports have facilitated the efforts of those who are inclined to use container shipping for illegal purposes (Willis and Ortiz, 2004). And given that millions of containers enter the U.S. very year through its seaports and only very few of these containers are physically inspected, the containerized shipping system seems to present itself as an attractive target (GAO, 2003). Therefore security experts believe it is only a matter of time before the U.S. or one of it allies is the victim of a terrorist attack using a shipping container, resulting in significant loss of life and in widespread and global economic damage (Willis and Ortiz, 2004).

According to Worthen (2006), between 2002 and 2005, the Department of Homeland Security spent US$75 million to track several companies' cargo containers into the U.S. via seaports in Seattle/Tacoma, Los Angeles/Long Beach and New York/New Jersey. Called Operation Safe Commerce (OSC), this project aims to identify weak links in the global supply chain, by using GPS technology and radio frequency identification (RFID) to monitor cargo from a handful of major importers (including Sara Lee and Motorola) as it made its way from overseas factories to its final destination in the U.S. (Worthen, 2006). Although one of the startling realizations of the OSC is that organizations actually know very little about what goes on in their supply chains, some common unsafe practices were managed to be identified by the project participants.

These include truckers dropping off containers without ever encountering terminal security, containers left in unsecured areas and containers bypassing a port that is considered (even if scheduled to pass through that port) and travelling instead through a country that poses a greater threat, without either the organization or the U.S. CBP being informed (Worthen, 2006).

Langhoff et al.'s 2005 industry study reveals the following thoughts about security from key industry stakeholders:

- Illegitimate entities or demand are a real and probable vulnerability
- Buying terms (i.e. Incoterms) have implications on ownership, liability and security
- Stuffing integrity at the overseas source is a necessity
- Overseas inland drayage is the most vulnerable link in the supply chain and there are no direct controls that currently mitigates these risks

In line with the concept of "garbage-in, garbage-out", one of the most vulnerable loop holes for security breaches are at source of the supply chain i.e. the upstream origin of the goods. Also, considering the various major handoffs along an ocean shipping supply chain[24], the probability of something bad happening is higher when the container is not in motion.

2.5 Supply Chain Security Performance

What Constitutes a Secured Supply Chain?

Specifically, in the realm of supply chain management, a secured supply chain would refer to a supply chain that is safe from predictable destructive dangers (such as forecasted natural disasters), resilient against relatively unpredictable destructive dangers (such as unpredicted natural disasters, union strikes and terrorist attacks etc.) and have measures in place that can protect the supply chain against such predictable or unpredictable acts of destruction or disruption.

[24] Major handoffs include: (1) factory-truck, (2) truck-origin port container yard, (3) origin port container yard-vessel, (4) vessel-destination port container yard, (5) destination port container yard-truck, (6) truck-distribution center, (7) distribution center-retail store/final customer.

Measuring Supply Chain Performance (SCP)

SCP, can be viewed as consisting of five key dimensions. These dimensions were determined after a rigorous review of past scholarly research on SCP as well as recent security-related studies on SCP.

Keller et al. (2002) conducted an extensive study on items and constructs used in logistics performance research for the past 40 years. Their study covered a wide range of latent performance concepts in logistics and supply chain management, from customer satisfaction and organizational leadership to operating performance and employee satisfaction.

The Supply-Chain Operations Reference-Model (SCOR) version 8.0, a process reference model that has been developed and endorsed by the Supply-Chain Council (SCC) as the cross-industry de facto standard diagnostic tool for supply chain management, is another extensive piece of research that contains 307 key indicators that measure the performance of supply chain operations. These key performance indicators (KPIs) are derived from the experience and contribution of the Council members.

A rigorous review of 20 of the 116 relevant research studies summarized in Keller et al. (2002) and SCOR version 8.0 revealed the following five key dimensions for SCP:

- Efficiency
  refers to the accomplishment of or ability to accomplish a job with a minimum expenditure of time and effort. Example: asset turnover, total logistics costs, productivity, asset utilization.

- Timeliness
  refers to the time performance aspect of supply chain operations including duration and speed. Example: delivery lead time, on-time delivery, truck turnaround time, order cycle time.

- Reliability
  refers to the dependability and accuracy of supply chain operations. Examples: amount of customer complaints, claims, information transmission accuracy.

- Availability

  refers to the ability to ensure undisrupted supply of products and/or services and/or information. This could be achieved through the provision of shipment information, ensuring supply of special equipment or products, ensuring that sales force is readily available to respond to customers' inquiries and needs. Examples: Order fill rate, supply rate, amount of backorders, provision of shipment transit information.

- Responsiveness

  refers to the accomplishment of or ability to react to demand or supply side changes and/or requests. This capability includes flexibility and agility and could be enhanced by the use of information technology in terms of greater visibility and/or configuration of business operations to allow operations scaling flexibility and agility. Example: customer satisfaction survey results, problem respond lead time.

Key scholarly studies that advocated the use of these dimensions for SCP include Raghunathan et al. (1988), Fawcett et al. (1997), and Sharma and Lambert (1990). Other studies that have proven these as important dimensions include Gassenheimer et al. (1989), Novack et al. (1994), Daugherty et al. (1998), Mentzer et al. (1999), Maloni and Benton (2000) and Stank et al. (2001).

Measuring Supply Chain Security Performance

Because organizations have multiple and frequently changing and conflicting goals, measuring performance of any kind, has always been a challenge for researchers (Hall 1991). One of the challenges that come along with securing the supply chain is measuring the success of your security efforts. In other words, how do you know you have prevented something that has not happened? (Rice and Spayd, 2005 and Worthen, 2006). In an effort to measure how secured a supply chain is, one encounters the same complexity as measuring supply chain performance (SCP), from defining the performance to be measured to selecting the right measure(s) to use so that the performance is most appropriately, objectively and adequately measured.

Helferich and Cook (2003), a recent study on supply chain security, identified five "V" elements for SCP - Value, Velocity, Variability, Visibility and Vulnerability. An analysis of these five "Vs" reveals that each of the "Vs" are end results in itself except for Visibility, which is more a means to achieving outstanding SCP rather than an end result.

Willis and Ortiz (2004) also listed the capabilities of the global container supply chain using similar categories:

- Efficiency
  deliver goods more quickly and more cheaply than other modes of transport, when volume and mass are taken into consideration.

- Shipment Reliability
  behaving as expected, retrieving and delivering goods as directed, with a minimum amount of loss due to theft and accident.

- Resilience
  ability to return to normal operating conditions quickly after the failure of one or more components and make it's services available.

- Fault Tolerance
  ability to respond to disruptions and failures of isolated components without bringing the entire system to a grinding halt.

- Shipment Transparency
  the goods that flow through a supply chain must be legitimately represented to authorities and must be legal to transport.

Each of these categories are also all end results in itself except for shipment transparency, which is more a means to achieving outstanding SCP rather than an end result.

Other scholarly works that have been done on supply chain security dealt with the topic of the value of security efforts (Lee, 2004, Rice and Spayd, 2005 and Worthen, 2006) where the ROI for security investments was of interest. The ROI as an important motivator and incentive for the private sector in making security investments is also an important driver for successful security policy implementation since the private sector has been "given" the responsibilities to ensure that their supply chains are secure.

Security is an abstract aspect of SCP. Moreover, different supply chains have different operating environments, constraints and objectives. As such, in order to provide or create the necessary incentives for security investments, there needs to be means to evaluate performance so as to evaluate the incentives.

2.6 Summary and Research Gap

As mentioned, risk management is not new and there are many studies and works on risk assessment, risk classification and management. Risk management in supply chain is certainly not new to supply chain professionals either, in the academia and industry alike.

Heightened Interests in Supply Chain Security Risk Management

However, the recent surge in terrorist activities worldwide has brought unprecedented interest and attention on a particular subset of supply chain risk management – security risk.

The review of existing literature has shown that since the 9/11 attacks in New York and Washington, the U.S. government has undertaken several initiatives at the public level to improve national security. From reorganising the country's border and customs related agencies, setting up national security councils and special agencies to working with foreign governments to heighten trade security and intelligence. Some of these initiatives have impacts on the private sector and they come mainly in the form of regulations such the CSI and the C-TPAT. Although most of these regulations are not currently mandatory, one key trend that can be observed is the shifting of supply chain security responsibilities from the public to the private sector.

Private Sector's Hesitation in Making Supply Chain Security Investments

The private sector however, has been quite hesitant about investing in security initiatives. Most of the security initiatives undertaken in the private sector currently are driven by compliance. Supply chain security initiatives in the private sector, motivated by self-interests are still considered rather limited. And several studies have indicated the following reasons for this lack of enthusiasm:

- private sector's difficulty in calculating ROI for security investments due to the very nature of "security improvements"
- lack of proven collateral benefits from security investments
- lack of clear direction from the public sector in terms of security standards
- the influx of intelligent technologies for security but no clear directions of technology standards from the public sector

These reasons together with the existence of public externalities in the costs and benefit nature of security investments are making it difficult for private organizations to justify investments in security.

It is therefore hypothesized that companies will look at improvements to both security performance and traditional aspects of supply chain management performance (i.e. collateral benefits), when making decisions about their security efforts.

Hypothesis 1:
The amount of an organization's security efforts is affected positively by how much impact on security performance the organization perceives the effort(s) will have.

Hypothesis 2:
The amount of an organization's security efforts is affected positively by how much collateral benefits the organization perceives the effort(s) will bring.

Need for the Ability to Evaluate Supply Chain Security Performance

And it certainly doesn't help that there is currently no supply chain security performance measurement metric available to help management measure what they are trying to improve. And as the saying goes, you cannot improve what you cannot measure.

> "For the government official, the desired outcome is to be able to say, "We have increased security to maximize the protection of our citizens while facilitating the efficient movement of goods across borders." For the CEO, the desired goal is to be able to say, "We are better off competitively because of our investments in supply chain security."
>
> - Closs and McGarrell (2004)

The quotation above illustrates the imperative to develop a way to help organizations measure and evaluate the security performance of the supply chains that they participate in. This will enable private organizations to appraise various security options and strategies and justify their investments accordingly and public organizations in developing and implementing public policies.

One of the key purposes of this study is therefore to identify a key set of performance measurements/indicators for the security performance of the operations of an international maritime supply chain. In doing so, this study will also shed light on the relationships between security performance and traditional SCP and their measurements respectively.

Research question of interest 1:
What are the key performance measurements for security performance of an international maritime supply chain, from the industry practitioners' point of view?

Research question of interest 2:
What is the relationship between supply chain security performance measurements and traditional SCP measurements?

Need for Better Understanding of the Relationship Between Various Supply Chain Security Initiatives and Supply Chain Security Performance

As mentioned in Section 2.3.1 previously, there are ways in which organizations can mitigate the security risks in their supply chain, from compliance with regulatory requirements to employing intelligent transportation systems to TQM principles in everyday operations.

Examples of key security initiatives implemented by the government of the United States since 9/11 include the following:

- Container Security Initiative (CSI)
  This program aims to identify high-risk containers before they arrive in the U.S. by placing U.S. Customs inspector at foreign ports where they screen U.S.-bound containers.

- Customs-Trade Partnership Against Terrorism (C-TPAT)
  This program is a joint government-business initiative to build cooperative relationships that strengthen overall supply chain and border security.

- Advanced Manifest Rule (AMR) for ocean carriers
  This rule allows Customs to evaluate containerized shipments for potential terrorist threats before they are loaded onto ships. Ocean carriers must submit a complete manifest for all shipments with Customs at least 24 hours before they are due for departure from a foreign port bounding for the U.S.

- Free and Secure Trade (FAST) program for truckers
  Using dedicated lanes, this program allows expedited processing of trucks that have been identified prior to arrival at the border as carrying low risk shipments.

- Safe and Secure Tradelane (SST) program
  This program focuses on deploying security of goods from the point of origin to the point of delivery across multiple global trade countries.

- Operations Safe Commerce (OSC) program for ocean containerized cargo movement.
  This program is a collaborative effort between the federal government, business interested and the maritime industry to develop and share best practices for the safe and expeditious movement of containerized cargo.

- Partners-in-Protection (PIP)
  The government of Canada has also responded to the need for better security in trade movement by implementing the Partners-in-Protection (PIP) program, an equivalent of C-TPAT.

For more security options and best practices, please refer to the following studies: (1) Closs and McGarrell (2004), (2) Rice and Spayd (2005), (3) U.S. CBP (2006) and (4) Peleg-Gillai et al. (2006).

With the wide array of security solutions available, there needs to be a better understanding of the relationship between supply chain security options and practices and their respective

impacts on supply chain security performance so that organizations can prioritize and make more informed decisions with regards to their security investments.

There have been several studies done on the impact of security initiatives on overall business cost and performance (Helferich and Cook, 2003; Closs and McGarrell, 2004; Koch, 2004; Banomyong, 2005; Langhoff et al., 2005; Rice and Spayd, 2005; Peleg-Gillai et al., 2006). But none has yet to statistically identify the actual impact of security initiatives on security performance itself.

This study takes current research further by attempting to statistically analyze the relationship between security initiatives and perceived supply chain security performance.

Research question of interest 3:
What is the relationship between security initiatives and supply chain security performance?

It is therefore hypothesized that any security efforts will positively impact the security performance of an organization's supply chain operations.

Hypothesis 3:
An organization's security efforts will positively affect their supply chain performance in terms of security.

Because of the existing general trend of sentiments that any effort to improve security will yield positive improvement in security performance, it is therefore hypothesized that in the absence of any objective KPIs, an organization's positive perception of the security impact of their security efforts will positively affect their self-perceived performance in the security of their supply chain operations.

Hypothesis 4:
An organization's positive perception of the security impact of their security efforts will positively affect their self-perceived performance in the security of their supply chain operations.

Need for Better Understanding of the Relationship Between Various Supply Chain Security Initiatives and Traditional SCP

A few studies have been done on this aspect of supply chain security research such as Helferich and Cook (2003), Rice and Spayd (2005) and Peleg-Gillai et al. (2006).

Helferich and Cook (2003) advocated that the supply chain security challenge is to effectively manage the "Five V's" – Value, Velocity, Variability, Visibility and Vulnerability. Value refers to the value that the customer gets in return for their money on a certain good or service. Velocity refers to order fulfillment cycle time. Variability refers to the consistency of an organization's order fulfilment performance. Visibility refers to an organization's ability in responding to customers' requirements and problem resolutions through leveraging on greater visibility of its supply chain. Vulnerability refers to a supply chain's susceptibility to disruptions. Effective and efficient supply chains require the balancing of the five "V" elements to provide customer value while minimising the cost and threat vulnerability.

Rice and Spayd (2005) raised a similar need for organizations to consider the collateral benefits (that is, benefits to other traditional aspects of SCP) of security investments but they also highlighted the fact that at this time, the collateral benefits approach remains difficult to quantify and there is little if any analysis of hard data documenting the actual collateral ROI in security, as very few firms have taken a systematic and disciplined approach to understand and create collateral benefits.

Peleg-Gillai et al. (2006) took this a step further and investigated via an industry survey to identity the collateral or indirect benefits that organizations can receive from security investments. The study's conclusions were based on a sample of eleven manufacturers and three logistics service providers and respondents were asked to do a self-assessment of the benefits that they have experienced as a result of their investments in security. Besides a limited sample, this study also does not take into account the potential differences in the extent of collateral benefits as a result of varying degrees of implementation of a security initiative.
This study therefore takes this approach further by using a larger sample of organizations so as to statistically determine the relationship between security initiatives and traditional SCP.

Research question of interest 4:

What is the relationship between security initiatives and traditional SCP?

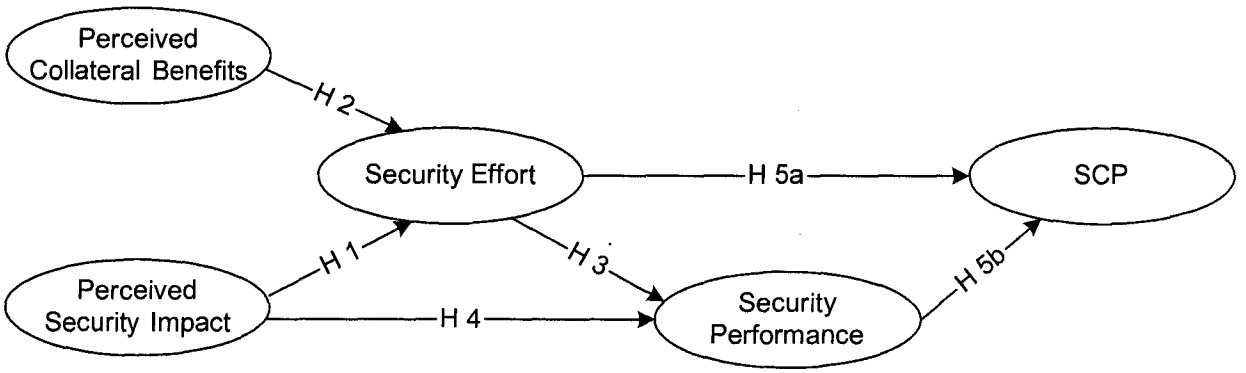
It is therefore hypothesized that an improvement in security performance will have a positive impact on other aspects of traditional SCP.

Hypothesis 5:

An improvement in the security performance of an organization's supply chain operations will have a positive impact on traditional SCP. This impact could be a direct result of security effort (H5a) or it could be an indirect result from an improvement in security (H5b).

These research questions and hypotheses can be illustrated in Figure 2.5.

Figure 2.5: Structural model for research questions and hypotheses.



CHAPTER 3 METHODOLOGY

The early development of modern logistics performance measurements has focused largely on the "hard" or more "objective" dimensions (e.g. cost tradeoffs and efficiency and fulfillment lead times.) of logistics and supply chain management. Researchers and practitioners applied econometrics, simulation modeling, and management science analytical techniques to evaluate cost tradeoffs between manufacturing, storing, and transporting raw materials, component parts, and finished goods (Keller et al., 2002). Examples of scholarly studies include Blanchard (1992), Dunn et al. (1994), Mossman et al. (1977).

More recently, the logistics discipline has evolved in directions that reflect greater influences from marketing, organizational behaviour, and strategic management research and practice These disciplines have helped logisticians better understand and manage the behavioural dimensions (that is, the "soft" or the more "subjective" dimensions) of logistics and supply chain management including customer satisfaction, integration, collaboration, partnerships and the development of logistics personnel (Keller et al., 2002). Research focusing on attitudinal and behavioural concepts differs notably from traditional approaches applied to studying say inventory levels or facility locations in that they are not directly measurable, that is, these concepts are "latent". And researchers in the field of logistics and supply chain management have since begun to use tools and techniques developed in the social sciences to examine these "latent" concepts.

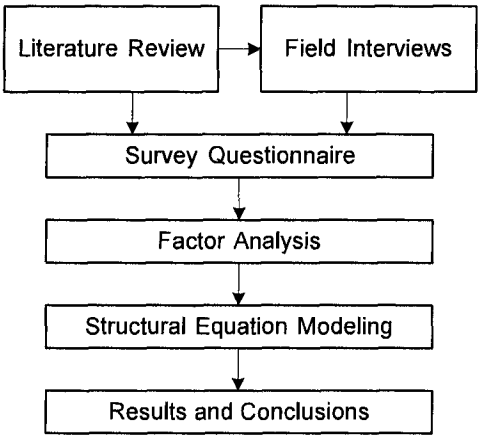
Keller et al. (2002) advocates that the evolution of more established business fields suggests that logistics researchers should continuously work to develop, test, and strengthen a complete set of measures for latent logistics concepts.

This research study, in its endeavour to shed light on the relationships between security performance and traditional SCP and their measurements respectively, is also dealing with a latent logistics concept. Therefore, this study uses tools and techniques developed and commonly used in social sciences research.

3.1 Key Phases in this Study

There are several key phases in this study (see Figure 3.1). An extensive review of existing literature was first done on the areas of supply chain risk management and supply chain security (see Chapter 2) and four research questions of interests were raised to be answered and five hypotheses were identified to be tested using the factor analysis and structural equation modeling (SEM) techniques.

Figure 3.1: Key phases in study.



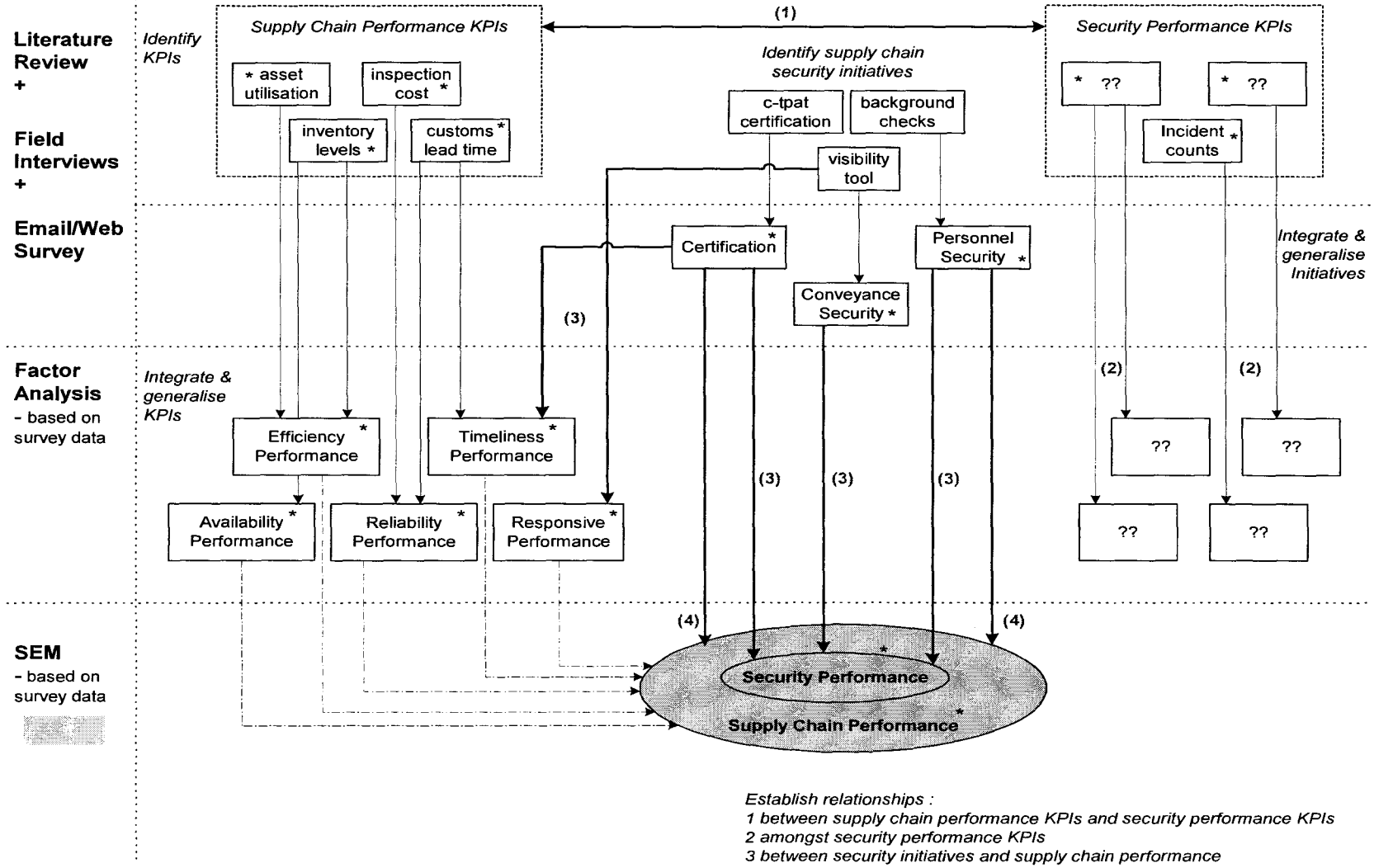
The set of preliminary hypotheses or issues were initially tested and subsequently refined by a series of comprehensive field interviews conducted with various stakeholders in the international maritime supply chain. This series of field interviews collected inputs which led to the development of a web/e-mail survey questionnaire. The survey questionnaire used in this study was developed and finalised after extensive reviews with field practitioners and academicians. The data collected were then analysed using factor analysis and SEM.

This chapter discusses the methodologies employed in this study including the rationale behind their use in various stages of the study, their advantages, disadvantages and limitations and also their application in this study.

3.2 Research Conceptual Framework

The research framework in Figure 3.2 guides the collection and analysis of the data in this study.

Figure 3.2: Research framework.



The literature review provided an initial set of hypotheses for testing during the field interviews. Specifically, an initial list of KPIs and security initiatives was drawn up to guide interviewees who face difficulties in articulating their responses. The list of KPIs for SCP included indicators such as asset turnover, inventory holding cost, delivery lead times, customer response time, inventory accuracy and shipment information transmission accuracy and were grouped based on the five key dimensions identified in Chapter 2. The list of KPIs for security included indicators commonly mentioned in existing security related literature, such as amount of pilferage, customs clearance lead time, inspection cost and inventory discrepancies. They are not pre-grouped because this is an exploratory study on security KPIs. A list of ten groups of security initiatives was also drawn up based on the classification of security initiatives in the Supply Chain Security Best Practices Catalogue (U.S. CBP, January 2006).

A close-ended survey questionnaire is then developed to collect more structured opinions on the appropriateness of each listed KPIs as an indicator for SCP and security performance. This will then allow the employment of factor analysis to reduce the list of KPIs into groups that reflect meaningful aspects of SCP and security performance that organizations should be monitoring and measuring. This is indicated as relationships (1) and (2) in Figure 3.2.

In order to understand the inter-related relationships between security initiatives, SCP and security performance, the more complex multivariate statistical technique - Structural Equation Modeling (SEM) is used so that multiple regression equations can be performed simultaneously while taking into account the reliability of observed variables and allowing the representation of latent concepts such as security efforts and SCP. This is indicated as relationships (3) and (4) in Figure 3.2.

3.3 Fieldwork/Interviews

Field work involves either the researcher or trained field workers making contact with respondents, collecting and recording primary data and information necessary for the purpose of the research study.

3.3.1 The Use of Fieldwork in Logistics Research

The use of field interviews in logistics and supply chain management research has been pretty extensive. Mentzer and Kahn (1995) reviewed all the articles published in the Journal of Business Logistics (JBL) from 1978 to 1993 and Table 3.1 below shows their results.

Table 3.1: Use of different methods in logistics research.

Category	% of Articles Published in JBL
Survey	54.3
Simulation	14.9
Interviews	13.8
Archival Studies	9.6
Math Modelling	4.3
Case Studies	3.2

Source: Mentzer and Kahn (1995).

A similar investigation performed by Dunn et al. (1993) which looked at methods used in the research presented in four logistics journals between 1998 and 1992, also indicated the extensive use of surveys/structures interviewing at 36%. Although popularity does not conclusively indicate the effectiveness of a method, it does reflect the practical applicability of the technique in the relevant field of research.

Field interview is an appropriate approach for this study because it this study is exploratory in nature with no primary data available about industry's opinions on appropriate security KPIs and the impact of specific security initiatives on SCP. Field interviews therefore help gather enough information to initiate a preliminary structure for subsequent close-ended data collection for statistical analyses.

Advantages of Field Interviews and Surveys

Field interviews are exploratory in nature. Unstructured or semi-structured interviews are usually used by researchers endeavouring to understand peoples' perspectives on a scene, to retrieve their experiences from the past, to gain expert insight or information. This is especially useful when the problem or question on hand is new and complex.

Although relatively less exploratory in nature, the structured survey is an excellent way to help researchers obtain primary data that are not available from public sources, private data companies or previous research studies at the time of their research. The data obtained are also reliable because responses are limited to the alternatives stated. This use of fixed-response questions reduces the variability in the results that may be caused by differences in interviewers. Most importantly, the data collected can be coded, analysed and interpreted using appropriate statistical analytical techniques.

Challenges and Limitations of Field Interviews and Surveys

As with all tools and techniques, there are challenges and limitations associated with the use of field interviews and surveys. For one, respondents may be unable or unwilling to provide the information due to sensitivity or inability to understand what is being asked for. As such, conducting the series of field interviews prior to the web survey have also helped to identify potentially sensitive questions for omission.

In addition, when using field interviews and surveys to gather data and information, the researcher or the field worker has to be very cognizant of the wording of each question, the sequence in which the questions are being asked and even the manner in which each question is asked. This is because even a slight change in the wording, sequence or manner in which a question is asked can distort its meaning and bias the response.

Rationale for Using Field Interviews in This Study

As can be seen from the review of existing literature, research in the area of supply chain security is still in its infancy. As such, the questions of interest of this study are best dealt using field interviews and surveys. This will allow the researcher to investigate the complex nature of the issue and obtain the necessary data non-existent at the time of this investigation. Moreover, since the questions of interest in this study are of intimate concern to the industry, it is important that their viewpoints and expertise be taken into consideration in the analysis.

3.3.2 Field Interviews in This Study

A total of 21 field interviews were conducted in Vancouver, Canada; Shanghai, China and Singapore from 14 January 2007 to 16 March 2007. The interviews were conducted over a six-week period with two weeks in each location. All interviews were conducted in-person except for

three which were done over-the-phone due to unavailability of one interviewee and impractical travelling distance required for the other two interviewees. Each interview lasted between one and two hours. All interviews were conducted using the English language except for those conducted in Shanghai, China, which were conducted in Mandarin. A series of questions were asked to gather the following information about the respondent's organization:

- performance measurements used in evaluating supply chain performance such as efficiency, timeliness, responsiveness, availability and reliability and the organization's perceived performance in these measures relative to their competition.
- performance measurements used in evaluating supply chain security performance and the organization's perceived performance in these measures relative to their competition.
- security initiatives adopted or to be adopted
- opinions about the relative importance and contributions of supply chain security to supply chain performance.
- basic demographical information about the organization size in terms of annual revenue and number of employees, key trade routes, logistics set up and supply chain strategy.

A pre-prepared interview questionnaire was used to structure the interview session. The questionnaire was prepared in both English and Chinese and consists of four sections A to D. Section A asks general information about the respondent's organization such as annual revenues, major trade routes, number of employees, scope of supply chain control and the extent to which supply chain management is a business driver. Sections B and C ask respondents to identify the KPIs that they are using to measure their supply chain and security performance respectively. They are also asked to self-rate their performance on these KPIs as best as possible on a 5-point Likert scale. Section D is the last section of the questionnaire and asks the respondent to identify the security initiatives that their organization has undertaken both before and after the 9/11 incident. On a 5-point Likert scale, respondents are also asked to express their opinions about the impacts of these initiatives on their supply chain and security performance as best as possible. Appendix A contains copies of the interview questionnaire in both the English and Mandarin.

The interviewees were selected to adequately represent the different stakeholders (i.e. shippers, ocean carrier, customs authority, port, terminals etc.) in the international marine supply chain as much as possible.

Prior to each interview, the interview questionnaire was shared with the interviewees for the purpose of their preparing and gathering necessary information. The interviewees were also informed of the purpose of the study.

Each interview was recorded both on paper and on a voice recorder whenever possible. Any discrepancies in the information collected during the interviews were dealt with by follow-up emails with the respective interviewee(s).

Details of the profile of the stakeholders interviewed and the findings from the field interviews can be found in Chapter 4.

3.4 Web/Email Survey

Information gathered from the field interviews were combined with knowledge from earlier scholarly works on SCP and supply chain security to develop the questions on the close-ended web/email survey tool used in this study.

The findings from the field interviews suggest additional hypotheses below and the appropriate questions were included in the survey to collect the necessary data for subsequent statistical analyses.

Hypothesis 6: Organization size affects attitude towards security.
Hypothesis 7: The nature of cargo handled (hazardous or lack thereof) affects attitude towards security.
Hypothesis 8: Typical shipment size (FCL or LCL) affects attitude towards security.
Hypothesis 9: Scope of supply chain decision control/influence affects attitude towards security.

The stakeholders in the international maritime supply chain community were grouped into two major groups. The first group consists of those stakeholders who initiate trade and includes buyers (importers) and sellers (exporters). The second group consists of the rest of the stakeholders who facilitates the realization of trade movement and includes the logistics service providers, the ports and terminals and customs authorities. This is an appropriate way of grouping because cargo final ownership and general nature of business operations, can speak a lot about the reasonable and expected amount of security due diligence an organization

should or would assume or have already assumed. A similar study done by The Manufacturing Institute (Peleg-Gillai et al., 2006) also divided their sample into manufacturers and logistics service providers.

One survey questionnaire was developed for each of the two major groups, a Shipper Survey and a Service Provider Survey. Both surveys were prepared in English and Mandarin (see Appendix B). The English version of the surveys is administered to samples residing in primarily English-speaking countries like U.S., Canada and Singapore. The Chinese version of the surveys is administered to the sample in primarily Chinese-speaking China. The Chinese sample has the option to respond to the English version as well.

The Shipper survey and the Service Provider surveys are different only in the guiding examples for some of the KPIs due to the inherent differences between the business nature of a shipper and that of a service provider.

Both surveys were administered to a much larger sample of organizations in the international maritime supply chain community. The mailing lists used to create the sample size for this study included entries from Council of Supply Chain Management Professionals (CSCMP) membership in Canada, China, Hong Kong, Singapore and U.S., persons receiving the Canadian Transportation & Logistics weekly e-newsletter and members of Supply Chain Logistics Council (SCL) Canada.

Each potential respondent received an email informing them of the study, its purpose and the value of the findings and results and are invited to participate in the online web survey. All potential respondents received the same information regarding the study and survey. Emails to the CSCMP mailing lists were sent out using a mailbox created and dedicated to this research project. It is not personal and respondents were only able to identify the sender of the email (without opening the mail) as "Freight Security Study". Emails to the Canadian Transportation & Logistics mailing list were sent together with the magazine's weekly e-newsletter. Emails to the SCL Canada mailing list were sent directly from the association's mailbox together with an endorsement letter from them.

The first emails to potential respondents residing in North America under the CSCMP mailing list were sent out on 1st June 2007 (Friday) 08:00 hours Pacific Time. Those under the

Canadian Transportation & Logistics mailing list received their first notification on 7th June 2007 (Thursday) 08:00 Pacific Time. The first emails to respondents residing in Asia under the CSCMP mailing list were sent out on 3rd June 2007 (Sunday) 20:00 hours Pacific Time and this is done to avoid the weekend time difference between North America and Asia. All respondents were given a dateline of 30th June 2007 to respond to the survey.

A second email was sent to all respondents on 11th June 2007 (Monday) 08:00 hours Pacific Time. Finally, a reminder email was sent to all potential respondents on 18th June 2007 (Monday) 08:00 hours Pacific Time.

3.4.1 Survey Characteristics

The sections that follow describe in greater details the different sections in the web survey. There are five sections in the web survey (Sections A to E) and Sections A to D utilize Likert scales extensively to capture the required data. Therefore, first and foremost, an introduction to the fundamental principles of the design of the Likert scales used in the survey is discussed. These scale design principles are employed in the designing the scales used in sections A to D of the web survey.

3.4.1.1 Scale Design

An effective construct is a function of the number of items in the construct and the number of response categories (i.e. intervals) in the measuring scale (Roznowski, 1989). A construct is a concept that is made up of one or more objective and measurable indicators.

Number of Items in a Construct

Constructs with too many items can create problems with respondent fatigue or response bias (Anastasi, 1976). Although, keeping the number of items in a construct few may be an effective means of minimizing response bias (Schmitt and Stults, 1985; Schriesheim and Eisenbach, 1990), constructs with too few items may lack content and construct validity, internal consistency and test-retest reliability (Kenny, 1979; Nunally, 1976), with single-item construct particularly prone to these problems (Hinkin and Schriesheim, 1989). However, additional items also means more time in both the development and administration of a construct (Carmines and Zeller, 1979). Cook et al. (1981) advocated that as few as three items can provide adequate

internal consistency reliabilities. Carmines and Zeller (1979) went further to suggest that adding items indefinitely makes progressively less impact on construct reliability. Keller et al. (2002) indicated a trend of using about four to five items per construct in logistics researches that uses multi-item constructs in the last 20 years.

In this study, each potential construct in SCP (i.e. efficiency, time, reliability, availability and responsiveness) and including security, has at least five KPI items, yielding a list of at least 30 KPIs in the final survey questionnaire. The KPIs representing each construct are determined after a rigorous review of the Keller et al. (2002) study and SCOR version 8.0 (see Appendix C for the complete list of KPIs included in the survey questionnaire).

Number of Response Categories on the Measuring Scale

Determining the optimal number of response categories is especially important in constructing the ubiquitous Likert-type scale, which is often used in collecting attitudinal and image data in marketing and public opinion research (Jacoby and Matell, 1971). Jacoby and Matell (1971) advocate that too few response categories may result in too coarse a scale and loss of much of the raters' discriminative powers while too fine a scale may go beyond the raters' limited powers of discrimination.

Likert scales are used in this study to capture respondents' self ratings on SCP, their opinions on KPIs for SCP and security performance and their opinions on the impact of security initiatives on their SCP. Each of these purposes will require Likert scales of different lengths depending on how discriminatory the data has to be in order to fulfill each research purpose.

A literature review was done on the impact of different number of response categories on reliability of results. This was followed by a review of the scales used in past logistics research was done, using the comprehensive study on multi-item scales used in logistics research by Keller et al. (2002). This information were then combined with the data requirements of each of the above mentioned research purposes to determine the optimal number of response categories for their respective scales.

Hinkin (1995) advocates that it is important that the measuring scale used, generate sufficient variance among respondents for subsequent statistical analysis. But how many is sufficient? Symonds (1924) was the first to suggest that reliability (in this case inter-rater reliability) of

scores is optimized by the use of seven response categories. Subsequent studies have shown that the coefficient alpha reliability with Likert-type scales increase more significantly up to seven response categories and levels off (Lissitz and Green, 1975; Cox, 1980; Preston and Colman, 1999) (see Table 3.2 below).

Table 3.2: Reliability of rating scales.

Test-retest	Response Categories										
	2	3	4	5	6	7	8	9	10	11	101
Reliability	0.88	0.86	0.89	0.91	0.92	0.93	0.94	0.94	0.93	0.92	0.90
Cronbach's α	0.81	0.79	0.82	0.82	0.83	0.85	0.85	0.85	0.85	0.86	0.85

Source: Preston and Colman (1999).

Preston and Colman's study reported statistical significance at $p < 0.05$ for the differences between:

- the 2-point scale and the scales with 6, 7, 8, 9 and 10 response categories
- the 3-point scale and the scales with 6, 7, 8, 9, 10 and 11 response categories
- the 4-point scale and the scales with 8 and 9 response categories

All other differences between the Test-retest reliability coefficients were statistically non-significant in Preston and Colman's study.

Since the differences in reliability are non-significant among scales with between five to nine response categories, we look to their respective Cronbach's α value to determine the appropriate length for the scale. Scales with between seven to nine response categories have slightly higher Cronbach's α value at 0.85.

Miller (1956) suggested in an influential article that the human mind has a span of apprehension capable of distinguishing about seven different items (plus or minus two). This implies a limit of about seven on the number of response categories that people are able to use in making judgements about the magnitudes of unidimensional stimuli and suggests that little if any additional information can be obtained by increasing the number of response categories beyond about seven. Thus, balancing the human apprehension capability with the goal of obtaining adequate response variance, a 7-point scale is deemed appropriate.

The practicality and popular adoption of 7-point scales (both Likert-type scales and other attitude and opinion measures) are noted by Bearden et al. (1993), Peter (1979) and Shaw and Wright (1967). In the area of supply chain management and logistics, the extensive use of 7-point Likert scales is supported by Keller et al.'s study[25] (see Table 3.3).

Table 3.3: Popularity of Likert scales used in logistics research.

Scale Type	Used in Number of Studies	% Used / Popularity
< 3 points	119	17.25%
3 points	8	1.16%
4 points	21	3.04%
5 points	256	37.10%
6 points	18	2.61%
7 points	250	36.23%
8 points	9	1.30%
9 points	5	0.72%
10 points	2	0.29%
> 10 points	2	0.29%
Total	**690**	**100%**

For the purpose of this study, a 7-point Likert scale is therefore used where respondents are asked to self-rate their performance because a good amount of discrimination is desired for performance data. A 3-point Likert scale is used instead where respondents are asked to indicate whether a particular KPI is an appropriate indicator for SCP and/or supply chain security performance. A 3-point scale is deemed suitable for this purpose because it is not necessary to discriminate among degrees of appropriateness or inappropriateness in this study.

3.4.2 Self Performance Appraisal

Section A is a self-appraisal of the responding person's organization's supply chain performance and security performance. This section is made up of questions A1, A2 and A3 on the questionnaire. The first question sets the context within which the respondent is answering the survey questions. It asks if the respondent is responding on behalf of the entire firm or just the specific strategic business unit (SBU) that he/she is responsible for. The other two questions

[25] Keller et al.'s study focuses on all survey research studies employing multi-item measures published in the International Journal of Logistics Management, International Journal of Physical Distribution and Logistics Management, Journal of Business Logistics, and Transportation Journal from 1961 to 2000. A total of 116 studies, done over a span of 40 years, employing a total sample of 690 multi-item scales, all of which have been subjected to at least minimal development procedures to assess the reliability and validity of the measures as part of the research process.

allow the respondent to appraise his/her organization's overall supply chain operations performance and security performance respectively, using a 7-point Likert scale (1=Not Acceptable, 2=Very Poor, 3=Poor, 4=Fair, 5=Good, 6=Very Good, 7=Excellent).

Security is defined to be how probable the respondent thinks his/her organization's supply chain(s) can be or will be compromised in terms of pilferages, thefts, damages, terrorism and other crimes such as smuggling, contraband etc.

SCP, on the other hand consists of the five dimensions that were determined after a rigorous review of past scholarly research on SCP including SCOR and other recent security-related studies on SCP. The Cronbach's Alpha of the individual items within each of these dimensions were greater than 0.70 (the recommended level by most studies using multi-item scales). Table 3.4 is a quick recap of these dimensions and they are compared to those advocated by Helferich and Cook (2003) and Willis and Ortiz (2004).

Table 3.4: Comparison of SCP dimensions.

SCP Aspect	**Corresponding**		**Other Relevant Studies**
	5 V's Helferich and Cook (2003)	**Categories Willis and Ortiz (2004)**	
Efficiency	Value	Efficiency	McGinnis et al. (1981), Mentzer and Konrad (1991), Stank and Lackey (1997), Koch (2004), Lee (2004).
Timeliness	Velocity	-	Sterling and Lambert (1987), McGinnis (1990), Matear and Gray (1993), Novack et al. (1994), Emerson and Grimm (1996), Stank and Lackey (1997), Crosby and Lemay (1998), Menon et al. (1998), Stank et al. (2001), Koch (2004), Price (2004), Banomyong (2005).
Reliability	Variability	Shipment reliability	McGinnis et al. (1981), Sterling and Lambert (1987), McGinnis (1990), Mentzer and Konrad (1991), Matear and Gray (1993), Emerson and Grimm (1996), Menon et al. (1998), Pearson and Semeijn (1999), Koch (2004).
Availability / Resilience	Vulnerability	Resilience & Fault tolerance	Emerson and Grimm (1996).
Responsiveness	Visibility	Shipment transparency	Sterling and Lambert (1987), Matear and Gray (1993), Novack et al. (1994), Emerson and Grimm (1996).

As can be seen from Table 3.4, the five dimensions synthesized from an extensive review of current literature on SCP are aligned with those proposed by Helferich and Cook (2003) and Willis and Ortiz (2004). These five dimensions are therefore deemed comprehensive enough for the purpose of this research study.

3.4.3 Organization Profiling

This is Section B on the questionnaire and collects data about the responding person's organization's nature of business and operating environment. There are eight questions in this section and is included because results from the field interviews revealed that certain key variables in an organization's operating environment seem to affect their attitude and performance in terms of security.

Industrial Sector

The type of business determines the primary nature of an organization's supply chain operations. In turn, the nature of an organization's supply chain operations has an impact on the types of activities that are managed and the kinds of vulnerabilities experienced. Example: importer, exporter, logistics service provider, port, terminal, ocean carrier and customs broker.

Type of Supply Chain and Hazardous Cargo Content

The type and nature of the commodities carried determines the vulnerability of the supply chain or lack thereof.

With regards to types of supply chains, supply chains handling cargo of higher value may be seen as more vulnerable to pilferages. However, their shipment size may be typically small (i.e. less-than-container-loads) and thus a less attractive target for terrorist acts such as planting a bomb compared to cargo typically shipped in full-container-loads. The question designed to collect the type of supply chain information is close-ended and includes the following answer choices: fast moving consumer goods, electronics, perishables/food products, automotive, pharmaceuticals, chemicals, heavy machinery and aerospace.

The hazardous nature of the products also impacts the extent to which an organization might be concerned about security and they may have different security initiatives. A separate question is asked to collect information about the percentage of hazardous cargo handled.

Average Shipment Size

Does the responding organization ship a greater proportion in full-container-loads (FCL) or less-than-container-loads (LCL)? The average shipment size determines how a typical shipment is handled (e.g. the number of handoffs in the process) and affects the kinds of vulnerabilities that a shipment is exposed to.

Key Trade Routes

An organization's major trade routes determine the kind of operating environments and logistics challenges that it is most often exposed to. It also identifies the types and degree of mandatory security regulations that they are subjected to. It can be reasonably expected that these operating factors affect an organization's stance and efforts toward security. This observation is supported by preliminary results from the field interviews.

The question designed to collect this information is close-ended and includes both the east-bound and west-bound routes between any two of the five major continents.

Organization Size Based on Annual Revenues

Annual revenue is a common measure for organization size in scholarly studies. In this study, the annual revenues of an organization can indicate the extent of what can be at stake if the organization's ability to satisfy their customers is disrupted. This can affect the organization's attitude towards crisis and risk management. The financial capability of an organization may also affect the type of security investments that they can undertake.

Responses from organizations during the field interviews indicate this to be highly sensitive and confidential information. As such, close-ended ranges instead of open-ended estimates are used. The annual revenue ranges used in this study is adopted from a recent supply chain security study done by Closs et al. (2006).

Scope of Decision Making

For the purpose of this study, it is more important to gather information about the scope of decision making authority the organization as a whole has over their supply chain as opposed to

the individual respondent. This is because the scope of supply chain control has direct implications on which business entity in a particular supply chain relationship has the responsibility to do the due diligence in ensuring security.

Based on the author's professional experience and interviews with industry practitioners in international freight movement, 15 and 16 key logistics activities involved in international freight were identified for the Service Provider and Shipper surveys respectively. The activity of selecting suppliers/manufacturers is not relevant for service providers. Respondents are asked to indicate whether or not each of these activities is applicable to their organization's operations and if they are, if their organization makes the final decision regarding that activity.

Supply Chain Management Strategy Drivers

For the purpose of this study, we need to know what drives an organization's excellence in supply chain operations because that had direct implications on how their supply chain is organized, and how related efforts and investments are prioritised. For instance, an organization that places greater emphasis on cost and efficiency may be more hesitant in adopting security initiatives especially those that are perceived to be unable to bring positive impact to the organization's bottom line. On the contrary, an organization that places greater emphasis on timeliness performance in their customer fulfilment may be more ready to adopt security initiatives that will help improve customs clearance lead times.

The supply chain drivers used are the key supply chain performance dimensions identified for measuring SCP in Section A.

3.4.4 Key Performance Indicators (KPIs)

This is Section C of the questionnaire and contains two questions which collect information about the respondent's opinions on what the appropriate KPIs for SCP and security performance should be.

The first question initiates the respondent's thinking in this aspect by asking them if it is at all necessary to have KPIs for supply chain security performance. This is followed by the second question which contains a list of 32 different KPIs. This list of KPIs is the result of past literature review and responses gathered during field interviews. For each KPI, respondents are asked to

use 3-point Likert scales (1=Not Appropriate, 2=Indifferent, 3=Appropriate), to indicate whether or not they think that a particular KPI is an appropriate indicator for SCP and security performance respectively.

The same list of KPIs is used for both SCP and security performance so that a subsequent comparison can be made to determine if security performance indicators are a subset of current common SCP indicators.

3.4.5 Supply Chain Security Initiatives

This is Section D of the questionnaire and asks the respondent to indicate their opinions on whether various groups of security initiatives have been implemented. And if a particular group of initiatives has been implemented, what has been the impact on their SCP, if any.

These security initiatives are classified into 10 key groups based on the classification of security initiatives in the Supply Chain Security Best Practices Catalogue (U.S. CBP, January 2006) (see Table 3.5). The best practices included in this catalogue were identified through more than 1,400 validations and site visits conducted by C-TPAT Supply Chain Security Specialists. The examples of security practices in this catalogue include not only advanced security technologies but also lower cost security practices. They are grouped according to the primary purpose of each practice such as to secure conveyance, to secure containers or ensure security of personnel safety. For example, concerning "conveyance security", the intended purpose of accurately tracking conveyance movements and detect deviations can be achieved through the use of GPS tracking systems, or through a lower cost security practice of requiring drivers to follow designated routes with predetermined average travel times, along with periodic communication between the truck driver and company officials (U.S. CBP, 2006).

Table 3.5: Security initiatives.

Group	Security Initiative	Examples (for details, refer to Supply Chain Security Best Practices Catalogue (U.S. CBP, Jan 2006))
1	Operations/Security Related Certifications	• Customs-Trade Partnership Against Terrorism (C-TPAT) (U.S.). • Partners-In-Protection (PIP) (Canada). • Free and Secure Trade (FAST) (U.S. and Canada).
2	Advanced Data	• 24-hours Advance Manifest Rule & Automated Commercial Environment (ACE) (U.S.). • Advanced Commercial Information (ACI) (Canada). • Advanced shipping notices (ASNs).
3	Business Partners Requirements	• Contractual obligations and supplier code of conduct. • Verify business references, credit checks. • Establish routine pickup/drop-off points.
4	Security Training & Outreach Programs	• Communicate terrorism information to employees and provide incentives for incident reporting. • Periodic training, specialized training in handling breaches, conducting investigations, inspections etc. • Collaborate with local law enforcement.
5	Procedural Security	• Establish internal security personnel network. • Establish incident database and procedures to handle suspicious activities, reporting and response. • Barcode/RFID scanning to detect discrepancies and ensure only manifested cargo is loaded.
6	Physical Security & Access Control	• 24-hours security guard and/or police patrol, fence/gate with magnetic sensors, alarm systems. • Biometric technology, color-coding uniforms, photo ID cards and password controlled locks. • Screen/random inspect incoming packages/vehicles.
7	Tracking & Monitoring (Conveyance Security)	• Monitor "unusual" requests and time lags for container turnaround time on premises. • Global Positioning System (GPS), truck transponders, online shipment visibility tool, CCTVs. • Examine fuel consumption to detect route deviations, satellite monitoring and detect stowaways
8	Personnel Security	• Pre-employment background checks. • Termination procedures. • Employee handbook for internal code of conduct and security awareness training.
9	Container/Trailer/Unit Load Device (ULD) Security.	• Exterior inspection, container and seal condition, and seal no. verification and seal issuance controls. • E-seals, other advanced container locking technology. • "Smart Box" – container with heavy-duty seal and electronic security device that communicates evidence of tampering, register every legitimate and unauthorized opening of container.
10	Management Support & Sponsorship	• Establish security committee and conduct periodic briefings • Incorporate security into "Continuous Improvement" philosophy and mission statement • Top management maintains high level of familiarity with overseas business partners, their practices and affiliations and ensures all subsidiaries develop and implement a sound security plan

For each group of security initiatives, respondents are asked whether it is being implemented in their organization. Respondents are presented with three options: (1) Implemented, (2) Planning to Implement or (3) Not Implementing. With each group of initiatives that the respondent's organization has implemented or is planning to implement, the respondent will be directed to an additional question related to that group of initiatives. This additional question requires the respondent to indicate their opinions about the impacts (if any) a particular initiative has or will have on their SCP based on the six dimensions of efficiency, timeliness, reliability, availability, responsiveness and security. The respondents voice their opinions using a 7-point scale where 1=Extremely Negative, 2=Very Negative, 3=Moderately Negative, 4=Unsure/Neutral, 5=Moderately Positive, 6=Very Positive and 7=Extremely Positive.

The purpose of this question is to gather data to understand the existence or lack thereof of the collateral benefits of security initiatives. For instance, if a responding organization has implemented security/operations related certifications and indicates a significantly positive impact on efficiency, this expression of opinion reflects the existence of the collateral benefit of efficiency of having a security certification even though this benefit is not quantified. The quantification of collateral benefits is not a purpose of this study.

3.4.6 Respondents' Information

This is Section E of the questionnaire and there are six questions to collect demographical information about the respondent. These demographical information will serve the purpose of understanding the impact of demographics on the results.

The first question asks the respondent how he/she learned about the existence of this research study and survey exercise. The channel through which a person was informed about the study may influence their readiness to respond. For example, it is expected that a personal contact of the author would be more ready to respond to the survey compared to someone who got the email through a mass mailing list.

The second question asks the respondent to indicate the physical location which they are residing in. Preliminary information gathered from suggested that one's physical location can have significant impact on one's viewpoints and perspectives on the criticality and urgency of

supply chain security issues. For instance, the results from the field interviews with Chinese companies suggest to a large extent that Chinese companies currently do not see security issues as imminent problems compared to their counterparts in North America. Thus this question was included.

The third question asks the respondent for his/her position within their organization. The purpose of this question is the collect information to understand how much decision making authority the respondent has in his/her organization and how much of a bird's eye view[26] the respondent has about his/her organization's business directions. This information will affect how substantial some of the information provided in the survey is. For instance, someone at the strategic planning level can be expected to have a better grasp of the impact of a security initiative on the organization's supply chain's reliability compared to someone at the ground operation level.

The fourth question is an optional question and asks for the respondent's organization's name.

Research of the past two decades has shown that cultures exert considerable influence over emotion (Matsumoto, 1993). And strategic behaviors differ across nations (Hofstede, 1980; Kagono et al., 1985; Kelley et al., 1987; Sallivan and Nonaka, 1988; Schneider and Meyer, 1991). Schneider and Meyer's study in 1991 on the effect of perceptions of environmental uncertainty and organizational control on strategic behaviors also found that national cultures influence the interpretation and response to strategic issues. Specifically, the results of the study showed that national cultures have significant influences over whether an issue is seen as a crisis, as a stimulant or as a threat. It also affects the interpretations of the issue's difficulty, urgency, certainty and future outlook.

Because the sample for this study includes respondents from more than one country, it is more important to capture the cultural similarities and differences between countries rather than within countries. Moreover, preliminary results from the field interviews are suggesting more significant differences in attitudes between countries than within countries. A fifth question is thus included to ask the respondent which national culture influences his/her business perspectives and attitude the most. The countries are then grouped based on the clustering synthesis by Gupta et al. (2002) (see Table 3.6). The variables used to cluster these 61 countries are performance

[26] An English idiom that refers to a view from high above i.e. gaining the ability to see the big picture.

orientation, uncertainty avoidance, future orientation, humane orientation, institutional collectivism, in-group collectivism, gender egalitarianism, assertiveness and power distance.

Table 3.6: Societal cluster classification.

Cluster Name	Countries
Anglo Cultures	Australia, Canada, England, Ireland, New Zealand, South Africa (White Sample), USA
Arab Cultures	Egypt, Kuwait, Morocco, Qatar, Turkey
Confucian Asia	China, Hong Kong, Japan, Singapore, South Korea, Taiwan
Eastern Europe	Albania, Georgia, Greece, Hungary, Kazakhstan, Poland, Russia
Germanic Europe	Austria, Germany, Switzerland, The Netherlands
Latin America	Argentina, Bolivia, Brazil, Colombia, Costa Rica, Ecuador, El Salvador, Guatemala, Mexico, Venezuela
Latin Europe	France, Israel, Italy, Portugal, Spain, Switzerland (French Speaking)
Nordic Europe	Denmark, Finland, Sweden
Southern Asia	India, Indonesia, Iran, Malaysia, Philippines, Thailand
Sub-Sahara Africa	Namibia, Nigeria, South Africa (Black Sample), Zambia, Zimbabwe

3.5 Factor Analysis

Factor analysis is used in this study to reduce the KPI data to a smaller set of key dimensions in two areas. Firstly, the SCP KPIs are factor analyzed in order to reveal if there is a dimension within SCP that measures security. Secondly, factor analysis is also employed on security KPIs to uncover the key dimensions for performance measurements within the area of security.

There are other grouping techniques such as cluster analysis and multidimensional scaling. Cluster analysis is not appropriate for the purpose of data reduction because the technique seeks to group objects (i.e. respondents) based on certain characteristics that they possess, as opposed to grouping characteristics. Multidimensional scaling seeks to determine the perceived relative image of a set of objects (such as products or ideas). This technique is based on the comparison of objects and therefore not appropriate for the purpose of this study, which does not assume KPIs to be interdependent on one another.

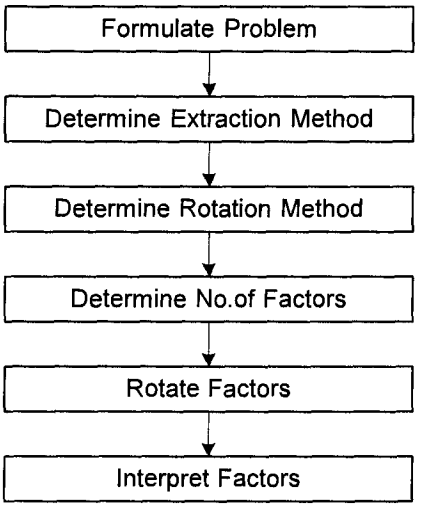
3.5.1 What is Factor Analysis?

Factor analysis is concerned with the resolution of a set of variables into a smaller number of meaningful categories or "factors". Factor analysis is commonly used in psychology and other areas of social sciences where exploratory studies are common. Exploratory studies typically use a large initial set of variables because no prior factor items are available. Exploratory studies are also very common in logistics research[27] and examples of such studies include Gassenheimer et al. (1989), Novack et al. (1994), Daugherty et al. (1998), Mentzer et al. (1999), Maloni and Benton (2000), Stank et al. (2001) and many more can be found in Keller et al. (2002). Factor analysis is therefore appropriate for this exploratory study because it serves to organize and reduce the KPI data collected via the online survey into fewer more meaningful and manageable groups, thereby achieving scientific parsimony.

3.5.2 Use of Factor Analysis in This Study

There are six key steps involved in the factor analysis in this study (see Figure 3.3). The variables that will be factor analyzed in this study are the KPIs for SCP and security performance. Discussion of the steps taken can be found together with the results in Chapter 5.

Figure 3.3: Conducting factor analysis.



[27] According to Mentzer and Kahn (1995), exploratory studies published in the Journal of Business Logistics are the second most popular type of research performed with an overall percentage of 36.2%.

3.5.3 Advantages and Challenges of Factor Analysis

Although factor analysis has the advantage of expediting the computation of multiple regression statistics (see Craeger, 1958 and Dwyer, 1940) and allows data reduction (i.e. parsimony in scientific explanation), Fabrigar et al. (1999) contented that perhaps more than any other commonly used statistical method, factor analysis requires a researcher to make a number of important decisions with respect to how the analysis is performed. They suggest that there are at least five major methodological issues that should be considered:

i. The variables that should be included in the study and the size and nature of the sample on which the study is based.
ii. Appropriateness of factor analysis given the goals of the research.
iii. Selecting the right procedure to fit the model to the data.
iv. Determining the number of factors that should be included in the model.
v. Selecting a method for rotating the initial factor analytic solution to a final solution that can be more readily interpreted.

Several other studies (Armstrong and Soelberg, 1968; Catell, 1978; Comrey, 1978; Ford et al., 1986; MacCallum, 1983; MacCallum, Widaman, Zhang and Hong, 1999; Velicer and Fava, 1998; Weiss, 1976) have also suggested that each of the above decisions can have important consequences for the results obtained.

Therefore, the challenge for the researcher is to ensure that the above methodological decisions are sound and rational.

3.6 Structural Equation Modeling (SEM)

SEM is used in this study to analyze the complex relationships between security effort, security performance, perceived collateral benefits and SCP. SEM is chosen as the technique of choice as opposed to multiple or logistic regressions because it allows the simultaneous analysis of more than one regression equation i.e. a complex network of relationships where are there more than one dependent variable and more than one independent variable.

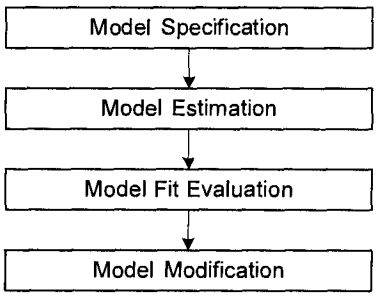
3.6.1 What is SEM?

SEM is a statistical methodology that tests a hypothesized model statistically to determine the extent the proposed model is consistent with the sample data (Wisner, 2003). It has been long known in marketing to be especially appropriate for theory testing (Savalei and Bentler, 2006).

3.6.2 Use of SEM in This Study

SEM is used in this study to test the a priori hypotheses of the relationships between security initiatives, security performance and traditional SCP. There are four key steps in the SEM modeling process: specification, estimation, evaluation and modification (see Figure 3.4).

Figure 3.4: Steps in SEM modeling process.



In the specification step, the model to be tested is developed and converted into a format that the SEM computer program – Analysis of Moment Structures (AMOS 7.0) can understand. In the estimation step, a fitting function is chosen and parameter estimates for the model are obtained. In the evaluation step, the test of model fit and other indices of fit are interpreted. In the modification step, the original model is modified in accordance with the information obtained in the previous step as well as theory. Steps 3 and 4 are usually conducted simultaneously.

Discussion of the steps taken can be found together with the results in Chapter 5.

3.6.3 Advantages and Challenges of Using SEM

Several aspects of SEM set it apart from the older generation of multivariate procedures. First, traditional multivariate procedures are incapable of assessing or correcting for measurement error, SEM provides explicit estimates of these error variance parameters. Second, whereas data analyses using the former methods are based on observed measurements only, those using SEM procedures can incorporate both unobserved (that is, latent) and observed variables (Savalei and Bentler, 2006). Finally, there are no widely and easily applied alternative methods for modelling multivariate relations or for estimating point and/or interval indirect effects.

However, when employing SEM, it is important that the researcher keep in mind the following potential pitfalls (Savalei and Bentler, 2006):

- Ignoring the test of model fit especially when your sample size is smaller than a few hundreds.
- Basing model acceptance or rejection on just one or two fit indices.
- Going wild with model modification and not ensuring that the modified model is consistent with some theory.
- Inferring causation and global truth. It is important not to simply draw causal conclusions from correlational data simply because SEM is used.
- Equating R2 and a well-fitting model. It is important not to assume that the constructs are strongly related simply when the model fits well.

CHAPTER 4 DATA

4.1 Profile of Field Interview Respondents

A total of 21 field interviews were conducted in Vancouver, Canada; Shanghai, China and Singapore from 14 January 2007 to 16 March 2007. Five, nine and eight companies were interviewed in Vancouver, Canada, Shanghai, China, and Singapore respectively. Table 4.1 displays the general profile of the organizations interviewed.

Table 4.1: General profile of organizations interviewed.

Stakeholder Type	Shipper (Importer + Exporter)	Logistics Service Provider	Ports + Terminals + Customs
Proportion of Total	**47.62% (10)**	**28.57% (6)**	**23.81% (5)**
Revenues (US$)*			
Large (>1 bil)	50.00% (5)	66.67% (4)	40.00% (2)
Medium (100 mil – 1 bil)	40.00% (4)	33.33% (2)	-
Small (< 100 mil)	10.00% (1)	-	20.00% (1)
Employee Count			
Large (> 5,000)	40.00% (4)	33.33% (2)	40.00% (2)
Medium (500 – 5,000)	40.00% (4)	50.00% (3)	20.00% (1)
Small (< 500)	20.00% (2)	16.67% (1)	40.00% (2)
Commodity Type			
FMCG	60.00% (6)	N.A.	N.A.
Automotive	10.00% (1)	N.A.	N.A.
Pharmaceuticals	10.00% (1)	N.A.	N.A.
Heavy Machinery	10.00% (1)	N.A.	N.A.
Others	10.00% (1)	N.A.	N.A.
Major Trade Routes^			
Intra Asia	40.00% (4)	66.67% (4)	80.00% (4)
Intra Americas	20.00% (2)	-	-
Asia ←→ N. America	80.00% (8)	83.33% (5)	80.00% (4)
Asia ←→ Europe	40.00% (4)	83.33% (5)	20.00% (1)
Europe ←→ N. America	10.00% (1)	-	-
Interviewee's Position Within Organization			
President/CEO	20.00% (2)	-	20.00% (1)
Supply Chain Director	10.00% (1)	16.67% (1)	20.00% (1)
Supply Chain Manager	50.00% (5)	50.00% (3)	-
Security Manager	10.00% (1)	33.33% (2)	60.00% (3)
Logistics Analyst	10.00% (1)	-	-

Notes to Table 4.1:
The number in brackets refers to the number of organizations that fall into that particular category.

* Two organizations interviewed under the category of Ports + Terminals + Customs were unable to disclose their annual revenues for 2005.
^ Interviewees are allowed to mention more than one major trade routes.

The different key stakeholders in the international maritime supply chain include shippers, and buyers (48%), customs brokers, freight forwarders and consolidators, third party logistics providers, trucking and inter-modal transportation companies (28%), ocean carriers, ports and terminals and customs authorities (24%).

The majority of the interviewees represent large organizations with annual revenues of more than US$1 billion (~52%). About 29% represent medium-sized organizations with annual revenues between US$100 million and US$1 billion. Another 10% represent smaller organizations with annual revenues of US$100 million or less. Two organizations (i.e. 9%) interviewed were unable to disclose their annual revenues for 2005.

Interviewees were asked to indicate their major trade routes and they are allowed to mention more than one. A significant majority of the organizations interviewed (~80%) have trade movements or handle trade movements between Asia and North America. The next most popular trade route is within Asia (~60% of respondents) followed by Asia-Europe (~48%).

The majority of the shipper organizations interviewed belong to the fast moving consumer goods (FMCG) industry (60%) with the rest from a varied mix of industries such as pharmaceuticals (10%), automotive (10%), and heavy machinery (10%). The rest of the 10% are classified as other industries such as forestry and chemicals.

The majority of the interviewees from these organizations are either managers or directors of their organization's supply chain operations. This was particularly true for shippers (80%) and logistics service providers (67%) than for the representatives from port and terminals and customs (40%). A good number of them are also managers for their company's supply chain security matters.

A summary of the responses gathered from these interviews can be found in Appendix E[28].

Since only one government organization was interviewed, it is deemed that its responses cannot be reliably generalized. As such, the field interview response from the government organization was not taken into consideration in the analyses discussed in Chapter 5.

[28] The names of the organizations and personnel interviewed are kept confidential as agreed with all field interview participants. A summary of their profile by industry type can be found in Table 4.2.

4.2 Profile of Web/Email Survey Respondents

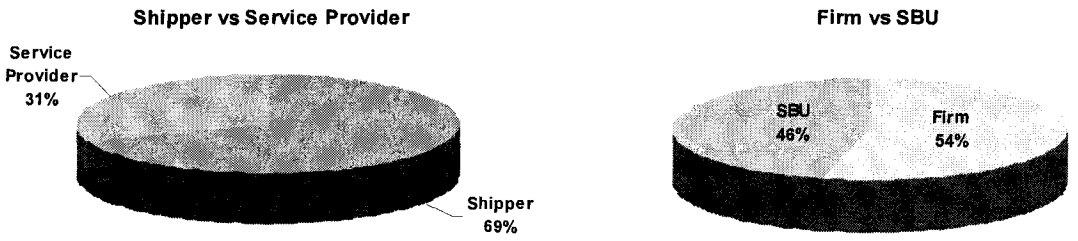
A total of 163 organizations from Asia and North America responded to the web/email survey. Of these 113 responded to the survey in entirety while 12 of the rest of the 50 omitted a few questions for the last section – Section D (Security Initiatives) and omitted Section E (Respondents' Information). The rest of the 38 only completed half of the survey, that is, only Section A (Self-Performance Appraisal) and Section B (Organization Profiling).[29] The omitted sections include Section C (KPIs), Section D (Security Initiatives) and Section E (Respondents' Information). On the web survey, respondents are only allowed to proceed upon completion of a question.

The profile of the web/email survey respondents is similar to that of the field interview interviewees. They represent a good mix of various stakeholders in the international marine supply chain. The paragraphs below discuss the profile of the web/email survey respondents.

Shipper vs. Service Provider

Figure 4.1 illustrate the proportion of service providers and shippers who responded to the survey and whether they represented only a single Strategic Business Unit (SBU) or the entire firm. Table 4.2 provides the detailed numbers. As can be seen, there is enough variation in respondent type to determine if being a shipper versus a service provider affects the pattern of responses. There is also enough variation in respondents' scope of responsibility to determine if scope of responsibility affects the pattern of responses.

Figure 4.1: Respondent profile in terms of type and representation.



[29] Possible reasons for a partially completed survey could be due to the sensitivity of the issues asked (i.e. security) and potential technical difficulties with some private organizations' firewall protection.

Table 4.2: Shipper vs. service providers.

	Firm	SBU	Total
Shipper	58	55	113
Service Provider	30	20	50
Total	88	75	163

Industry Sector

In terms of industry profile, shippers are classified as either importers (buyers) or exporters (sellers) or both (e.g. a trading company) (see Table 4.3 and Figure 4.2) and service providers are further classified into sub groups based on the logistics services they provide. The groupings used for service providers are 3rd party logistics service provider (3PL), trucking companies, customs brokerage firms, freight consolidators, freight forwarders, terminal operators, ocean carriers and port (see Table 4.4 and Figure 4.3).

Table 4.3: Shipper profile.

Shipper	Count	Percentage
Buyer (Importer)	81	50.63
Seller (Exporter)	74	46.25
Others	5	3.13

Table 4.4: Service provider profile.

Service Provider	Count
3rd Party Logistics	30
Trucker	17
Customs Broker	10
Freight Consolidator	10
Freight Forwarder	10
Terminal	5
Others	4
Ocean Carrier	2
Port	1

Note: Count totals in Table 4.4 and 4.5 do not add up to 113 or 50 for shippers and service providers respectively because respondents are allowed to select more than one industry type.

Figure 4.2: Industry profile of shippers.

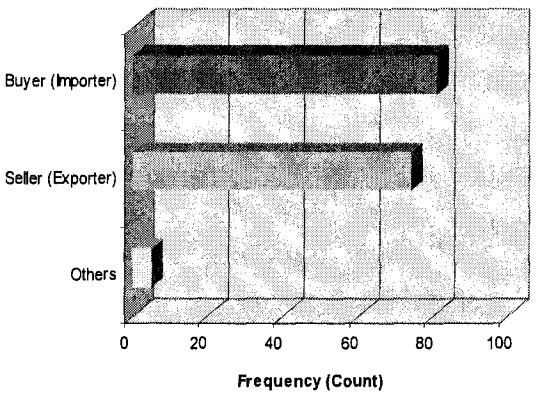
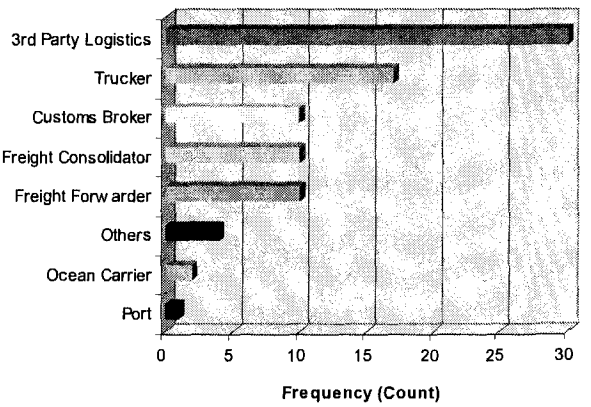


Figure 4.3: Industry profile of service providers.



Although it is regretful that no customs authorities responded to the web survey, the field interviews with a customs authority in Asia revealed that the key role of customs authority is in setting and implementing regulations. They have little impact or opinions in terms of determining or influencing the type of security initiatives adopted and also the kind of performance measurements used for security and supply chain management.

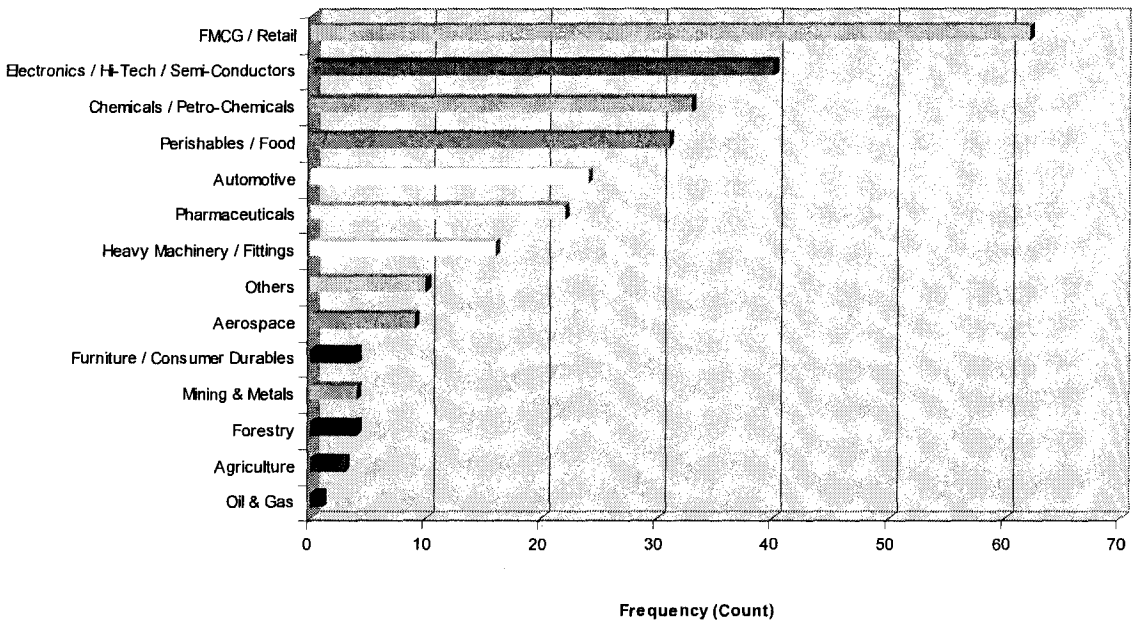
Supply Chain Types

Figure 4.4 and Table 4.5 shows that majority of the respondents come from the FMCG/Retail sector which can include respondents from both the FMCG/Retail and Electronics group. This makeup is ideal for our analysis because these supply chains more often than not dealing with container freight. The bulk and break bulk freight-dominant supply chains such as the agriculture, oil and gas and forestry make up the minority of the sample population.

Table 4.5: Respondents' supply chain types.

	Shipper	Service Provider	Total
FMCG / Retail	35	27	62
Electronics / Hi-Tech / Semi-Conductors	18	22	40
Chemicals / Petro-Chemicals	21	12	33
Perishables / Food	15	16	31
Automotive	5	19	24
Pharmaceuticals	9	13	22
Heavy Machinery / Fittings	6	10	16
Others	6	4	10
Aerospace	4	5	9
Furniture / Consumer Durables	4	0	4
Mining & Metals	4	0	4
Forestry	3	1	4
Agriculture	3	0	3
Oil & Gas	0	1	1

Figure 4.4: Illustration of respondents' supply chain type proportions.



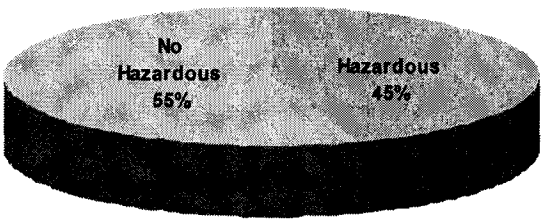
Hazardous Cargo Composition

Figure 4.5 and Table 4.6 show a balanced variation in the proportion of respondents carrying hazardous versus non-hazardous cargo is balanced.

Table 4.6: Cargo nature handled by respondents' organizations.

	Shipper	Service Provider	Total
Hazardous	45	28	73
No Hazardous	68	22	90

Figure 4.5: Variation in cargo nature handled by respondents' organizations.



FCL Cargo Composition

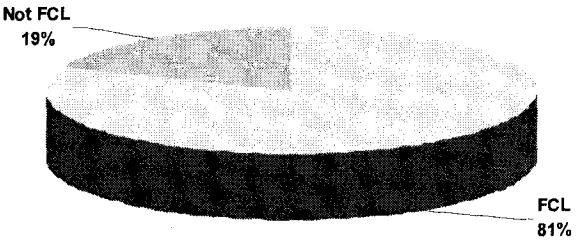
Figure 4.6 and Table 4.7 show that a significant majority of respondents carry primarily FCL cargo. This is perfect for our study because the assumption is that if the entire container

belongs to an organization, the organization will have greater incentives to ensure that the integrity of its international movement is not compromised. Therefore, the responses given by these companies can be seen as more credible in terms of perceptions and intentions.

Table 4.7: Shipment size nature of respondents.

	Shipper	Service Provider	Total
FCL	95	37	132
Not FCL	18	13	31

Figure 4.6: Variation in shipment size nature of respondents.



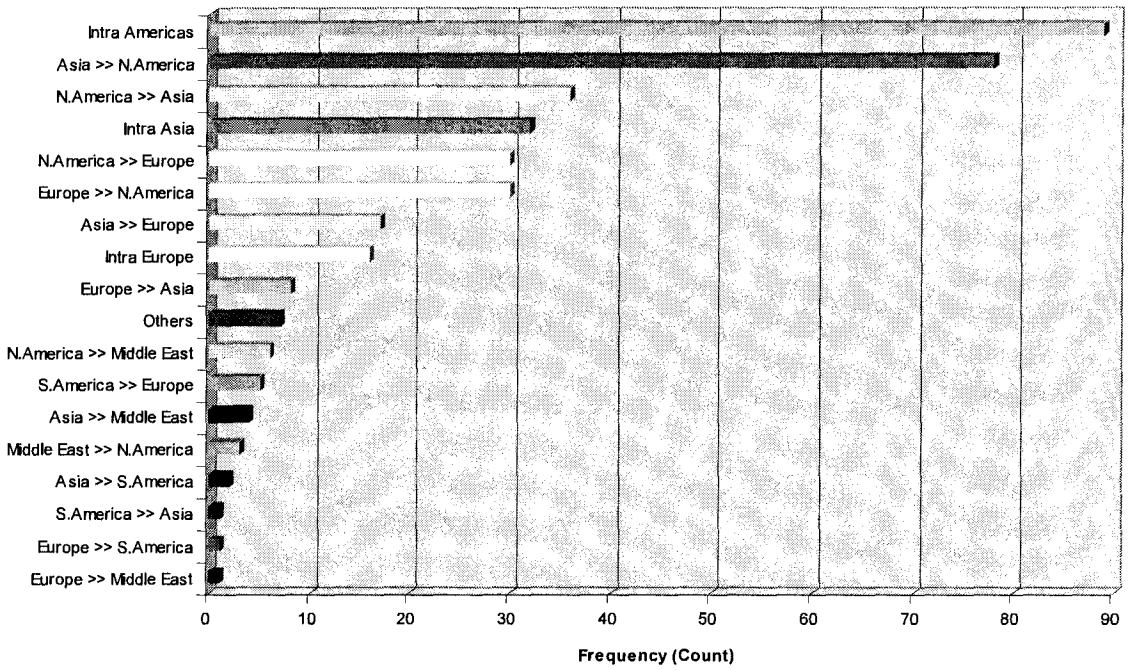
Trade Route Profile

Respondents are asked to indicate their three most frequently used trade routes. Figure 4.7 and Table 4.8 show that a significant majority of the respondents are moving cargo within North America and between North America and Asia.

Table 4.8: Respondents' trade route profile.

Trade Route	Shipper	Service Provider	Total
Intra Americas	67	22	89
Asia >> N.America	52	26	78
N.America >> Asia	28	8	36
Intra Asia	21	11	32
N.America >> Europe	23	7	30
Europe >> N.America	27	3	30
Asia >> Europe	8	9	17
Intra Europe	14	2	16
Europe >> Asia	6	2	8
Others	1	6	7
N.America >> Middle East	5	1	6
S.America >> Europe	3	2	5
Asia >> Middle East	2	2	4
Middle East >> N.America	3	0	3
Asia >> S.America	2	0	2
S.America >> Asia	0	1	1
Europe >> S.America	1	0	1
Europe >> Middle East	1	0	1
S.America >> Middle East	0	0	0
Middle East >> Asia	0	0	0
Middle East >> S.America	0	0	0
Middle East >> Europe	0	0	0

Figure 4.7: Variation in respondents' trade route profile.



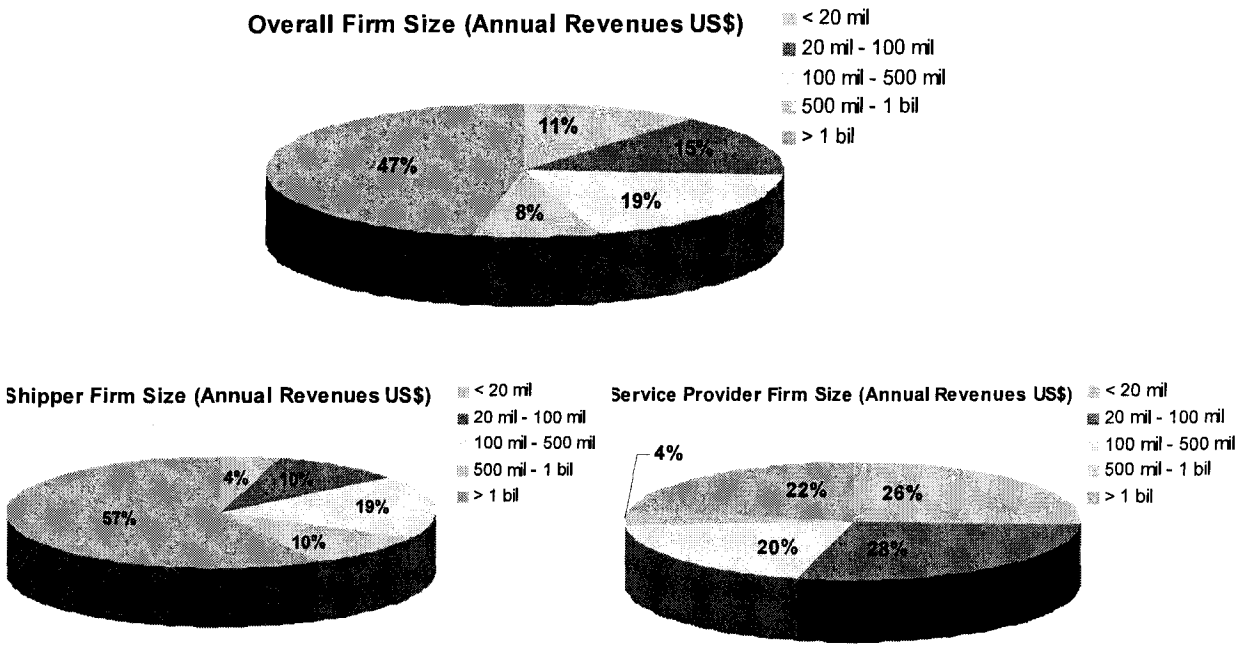
Organization Size

Respondents' organization size is reflected by their 2006 annual revenues in U.S. dollars. Figure 4.8 and Table 4.9 show that majority of the respondents belong to large organizations with annual revenues exceeding US$1 billion. More than two-thirds belong to organizations with annual revenues exceeding US$100 million. It is however interesting to note that most of the large organizations belong to the Shipper category. The organization size of surveyed service providers are more evenly distributed with most of them being relatively smaller organizations with annual revenues between US$20 million and US$500 million.

Table 4.9: Respondents' 2006 annual revenues profile.

Range	Shipper	Service Provider	Total
< 20 mil	5	13	18
20 mil - 100 mil	11	14	25
100 mil - 500 mil	21	10	31
500 mil - 1 bil	11	2	13
> 1 bil	65	11	76

Figure 4.8: Respondents' 2006 annual revenues profile.



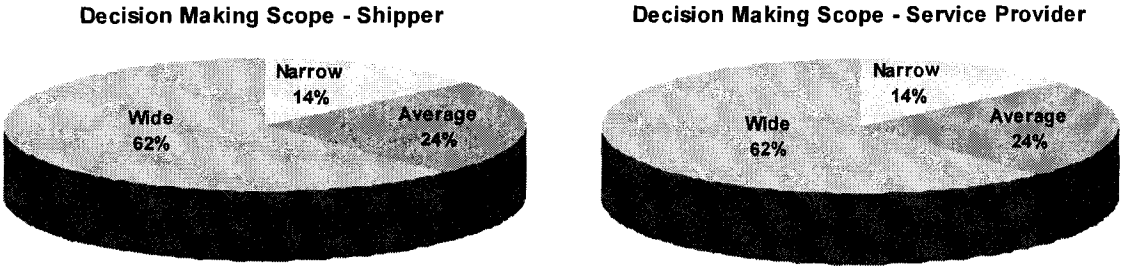
Decision Making Scope/Scope of Supply Chain Influence

Figure 4.9 and Table 4.10 show that majority of the respondents hold considerable influence and/or decision making authority over the operations of their supply chain. This profile demonstrates the credibility of the opinions gathered in the survey and is especially encouraging for the analysis and results of this study. Please refer to section 5.2.5 for a detailed discussion and definition of the various scopes of control.

Table 4.10: Respondents' scope of influence over their supply chain.

Decision Making Scope	Shipper	Service Provider
Narrow	16	7
Average	27	12
Wide	70	31

Figure 4.9: Respondents' scope of influence over their supply chain.



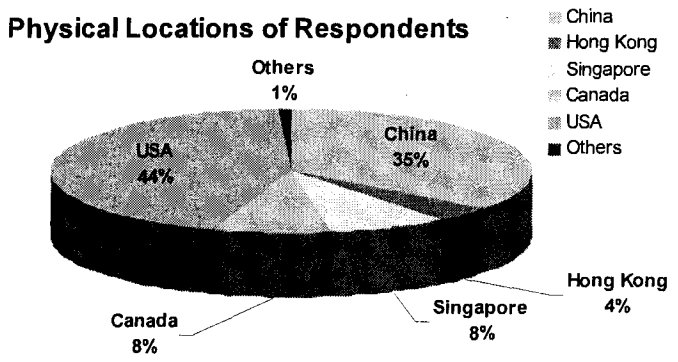
Respondents' Physical Locations

Figure 4.10 and Table 4.11 below show a balanced variation in the proportion of respondents from North America and Asia.

Table 4.11: Physical locations of respondents.

Location	Shipper	Service Provider	Total
China	28	16	44
Hong Kong	3	2	5
Singapore	6	4	10
Canada	3	7	10
USA	39	16	55
Others	1	0	1

Figure 4.10: Variation in physical locations of respondents.



Note: The country included in the "Others" category is United Kingdom.

Respondents' Dominate Culture in Business Management

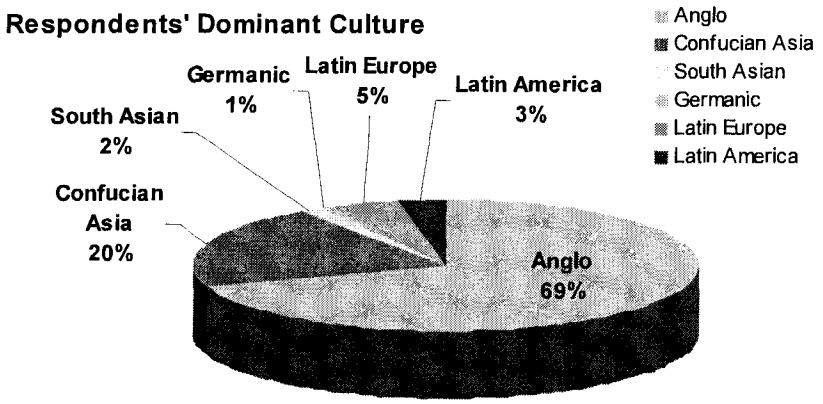
With globalization, we can reasonably expect respondents to be physically located in a country but be influenced by another country's culture in managing their business. The survey asked each respondent to indicate the culture that dominates their behaviour and attitude in the day to day management of their business. Figure 4.11 and Table 4.12 show that even though respondents are evenly located in North America and Asia, majority of them are influenced by the Anglo culture, which includes countries such as England, Australia, South Africa (White), Canada, New Zealand, Ireland and the U.S..[30] China, Singapore and Hong Kong all belong to the Confucian Asia cluster.

[30] The cultural clusters used in Figure 4.11 and Table 4.13 are from Gupta et al. (2002). Using data collected on cultural values and beliefs from 61 nations, Gupta et al. (2002) used discriminant analysis, split half sample and cross-validation to provide strong support to the existence of 10 cultural clusters: South Asia, Anglo, Arab, Germanic Europe, Latin Europe, Eastern Europe, Confucian Asia, Latin America, Sub Sahara Africa and Nordic Europe.

Table 4.12: Respondents' dominant culture in business management.

Cluster Group	Shipper	Service Provider	Total
Anglo	62	30	92
Confucian Asia	14	13	27
South Asian	2	0	2
Germanic	0	1	1
Latin Europe	4	2	6
Latin America	3	1	4
Arab	0	0	0
Eastern Europe	0	0	0
Nordic Europe	0	0	0
Sub-Sahara Africa	0	0	0

Figure 4.11: Variation in respondents' dominant culture in business management.



4.3 Types of Variables

The survey responses can be represented by two main types of variables – observed and latent. Observed variables are those variables that can be observed and directly measured. Latent variables, on the other hand are those variables that are not or cannot be directly observed but are rather inferred from observed variables.

Based on the research conceptual framework presented in Chapter 3, the types of variables required to answer the research questions of interests were identified and are listed in Table 4.13. How each variable is operationalized in the web/e-mail survey instrument is shown in the right hand column.

Table 4.13: Types of variables.

Variable	Observed/Latent	How Operationalized
A. Organization size	Observed	• Annual sales revenue (2005)
B. Supply chain characteristics	Observed	• Industrial sector • Commodity carried • Hazardous / Non-hazardous • Average shipment size • Major trade routes
C. Supply chain control	Latent	• # of aspects of supply chain operations that are performed in-house and outsourced versus not controlled
D. Supply chain drivers	Observed	• Self rate importance of five supply chain drivers* and security
E. Supply chain performance	Observed	• Self rate performance on five key aspects of supply chain performance* on 7-point Likert scale
F. Security performance	Observed	• Self rate performance on 7-point Likert scale
G. Supply chain KPIs	Observed	• Rate appropriateness on 32 KPIs
H. Supply chain security KPIs	Observed	• Respondent opinion on necessity for security KPIs • Rate appropriateness on 32 KPIs^

Notes to Table 4.1:

* the selection of the drivers and key performance indicators is based on the comprehensive review of 20 of the 116 studies in Keller et al. (2002), SCOR version 8.0 and several other recent studies on supply chain performance and results from the field interviews. Citations of these studies can be found in Appendix D.

^ the selection of the security KPIs is based on the results from the field interviews and recent literature on supply chain security.

Other observed variables in this study includes various supply chain characteristics/facts such as industrial sector, commodity and their hazardous nature, the average shipment sizes and key trade routes and the performance on various supply chain performance KPIs. It also includes organization size in terms of annual revenues and importance of various supply chain drivers.

There is only one latent variable – span of supply chain control/influence. The span of supply chain control variable is considered a latent variable because respondents are asked to indicate if they have decision influence over a set of 12 activities and the span of control variable is inferred by arbitrarily grouping respondents into three categories. Respondents in the first group have eight or more of the 12 activities managed in-house and therefore are considered to have a wide span of control. Respondents in the second group have four to seven activities managed in-house and are considered as having an average span of control. Lastly, the respondents in the third group have less than 4 activities managed in-house and are therefore considered as having a narrow span of control.

CHAPTER 5 ANALYSIS

This Chapter discusses the analyses performed on the data collected in this study.

5.1 General Attitude Towards Supply Chain Security

The opinions gathered from the field interviews revealed that many of the shipper and service provider organizations interviewed do not see advancement in security as a competitive advantage at this point in time. They see security threats as mainly thefts, pilferages and cargo damage. This opinion does not vary significantly among respondents from Asia and North America.

The majority of the organizations interviewed during the field interviews also pointed out that what are considered reasonable requirements for some businesses might not necessarily be reasonable for others. For instance, an organization trading low value items such as plastic household products for hyper-marts will definitely find GPS-equipped trucks a less reasonable security requirement as compared to an organization handling non-weaponry supply business for the U.S. army in Iraq. The majority of the organizations interviewed also have their principal physical operating activities in China and South East Asia and most do not perceive these geographic locations as imminent targets or breeding grounds for terrorism as compared to some other countries such as U.S. and U.K. The U.S. Customs and Border Protection (2006) publication has also explicitly mentioned that the adoption of certain best practices depends on the risks assessments on the operating environment. It writes that while the adoption of certain best practices in a low risk environment might be sufficient to mitigate the risks present and enable the importer to qualify for Tier Three standing under the C-TPAT program, the adoption of the same practices may be viewed as a necessary, minimum security measure in a high risk environment and therefore not elevate the overall security environment to the point at which the importer would be considered for Tier Three.

The majority of the service provider organizations interviewed also cite the fact that their customers are not currently demanding security requirements beyond what they are already receiving, as a key reason behind the lack of enthusiasm.

Supply chain security is more than just mitigating the risks of terrorism. However, many of the organizations interviewed, especially those in Shanghai, China, perceive incidents such as human smuggling, which they have experienced, as harmless incidents that do not cause devastating damages to human lives and public infrastructures. Hence they do not consider them as security threats. Moreover, they feel that the same means used for preventing such crimes can also be used against terrorism. This opinion is echoed by the participants in Wills and Ortiz's 2004 study which noted that terrorism can be prevented using many of the same means used for preventing theft and smuggling because each objective requires the system to be able to control the cargos enter and leave the system.

Many of the organizations interviewed also do not see an impending need to invest heavily in security improvement initiatives unless required by legislation in order to continue operations legally. These sentiments are shared by the respondents in Peleg-Gillai et al.'s 2006 study where many found it difficult to provide a business case to justify security investments and are therefore reluctant to invest in security beyond the minimum necessary.

However, the organizations interviewed in this study are cognizant that depending on how the market dynamics and public sector's legislations and regulations around security develop, their organizations need to be ready and willing to comply within their best ability. For example, a few of the larger companies are already investing in relatively more high-tech security solutions such as GPS and Biometrics. Most of these solutions were undertaken as a result of the need to comply with regulations or requirements from their business customers. These security requirements can range from basic items such as installing a minimum number of CCTVs within a warehouse to sophisticated ones such as being C-TPAT certified and/or having all trucks GPS-equipped.

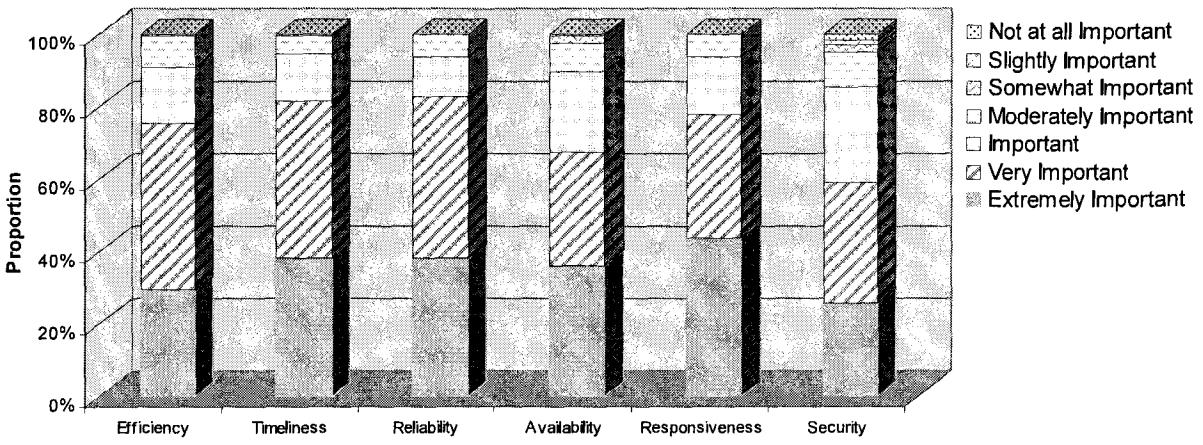
These same sentiments can be seen in the results from the web survey. Respondents to the web survey were asked to evaluate and rank the importance of security as a supply chain driver relative to five other traditional supply chain drivers – efficiency, reliability, responsiveness, availability and timeliness.

Figure 5.1 and Table 5.1 show that the security driver is ranked very differently (lower)[31] from the other traditional supply chain drivers. Within the "Extremely Important" ranking, a significant smaller proportion of respondents ranked security as such (26% for security vs an average of 37% for the rest of the drivers). Combining "Extremely Important" and "Very Important" categories, still a significantly smaller of proportion of respondents rank security as such (59% for security vs. an average of 77% for the rest of the drivers. A further cumulative combination of "Extremely Important", "Very Important" and "Important" categories, still a significantly smaller proportion of respondents rank security as such (85% for security vs. an average of 92.4% for the rest of the drivers).

Table 5.1: Respondents' view of security as a supply chain driver.

Importance	Efficiency	Timeliness	Reliability	Availability	Responsiveness	Security
Extremely Important	29%	38%	38%	36%	44%	26%
Very Important	46%	44%	45%	31%	34%	33%
Important	15%	13%	11%	22%	16%	26%
Moderately Important	9%	5%	6%	8%	6%	10%
Somewhat Important	0%	1%	0%	2%	0%	2%
Slightly Important	1%	0%	0%	0%	0%	1%
Not Important	0%	0%	0%	1%	0%	2%
Total	163	163	163	163	163	163
Average Rank	5.94	6.13	6.15	5.90	6.15	5.60
50th Percentile	6.00	6.00	6.00	6.00	6.00	6.00
90th Percentile	7.00	7.00	7.00	7.00	7.00	7.00

Figure 5.1: Respondents' view of security as a supply chain driver.



[31] Recall from Chapter 4 that only one out of the 163 web survey respondents come from a port authority. As such, the result in Figure 5.1 reflects only the sentiments from the shippers and service provider organizations.

The sample is also split into shippers and service providers to see if there are any attitude differences between the two groups. An initial visual analysis of the same charts for shippers and service providers (Figures 5.2 and 5.3 respectively) show that there are no apparent differences in attitudes towards security as a supply chain driver. Within the shipper and service provider groups separately, respondents rank security lower as a supply chain driver compared to the other five traditional aspects of SCP.

Figure 5.2: Shipper respondents' view of security as a supply chain driver.

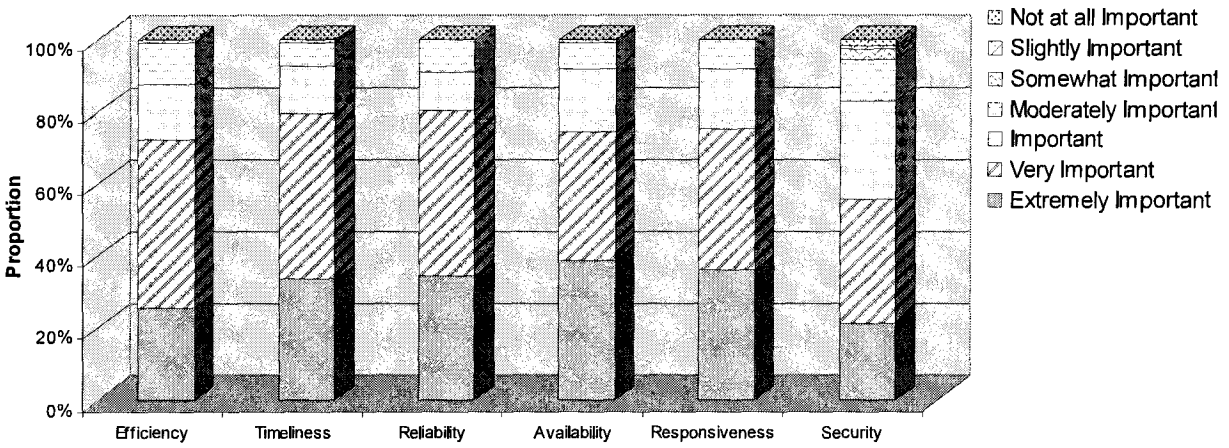
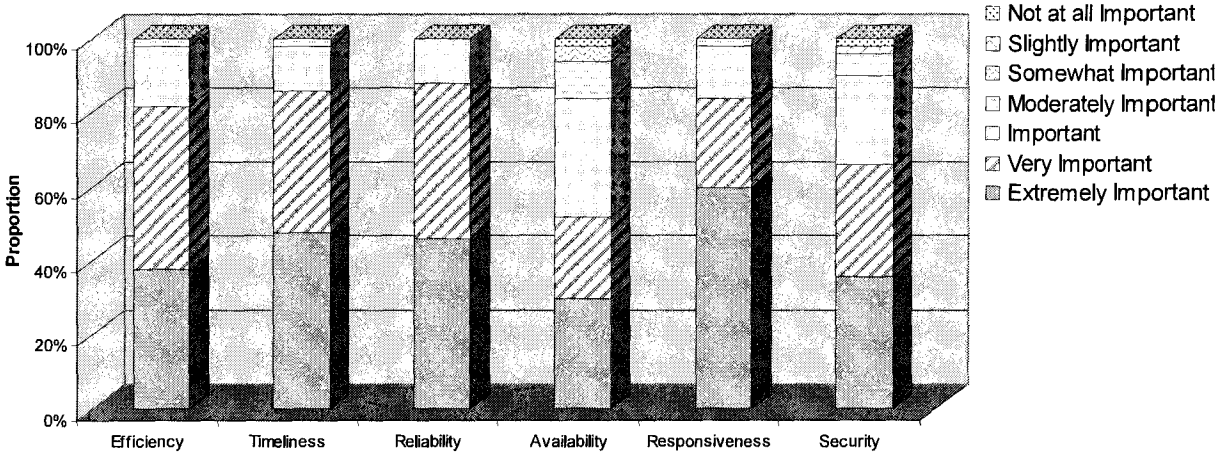


Figure 5.3: Service providers' view of security as a supply chain driver.



Since there are no apparent differences between shipper and service provider groups, the following statistical tests were carried out using a combined sample. These tests are performed to determine if the difference in ranking between security and other aspects of SCP are

statistically significant. The average ranking for security as a driver is 5.60 (Table 5.1), which is 0.55 points lower than the highest ranked drivers – Reliability and Responsiveness. Two-tailed[32] paired t-tests[33] were performed to determine if these differences are statistically significant (see Table 5.2).

Table 5.2 shows that the differences between all drivers paired with security driver are statistically significant (i.e. pairs 5, 9, 12, 14 and 15), where the Sig. (2-tailed) values are smaller than 0.025. These pairs are marked with an "*". The differences in mean for these pairs are positive, indicating that the security driver (being the latter variable in each pair), is ranked significantly lower than the former variable in the pair.

Table 5.2: Results for statistical tests for significance in differences in ranking of drivers.

		Paired Differences			t	df	Sig. (2-tailed)
		Mean	Std. Deviation	Std. Error Mean	Mean	Std. Deviation	Std. Error Mean
Pair 1*	Efficiency - Time	-0.1902	0.8281	0.0649	-2.9320	162	0.0039
Pair 2*	Efficiency - Reliability	-0.2025	0.7467	0.0585	-3.4617	162	0.0007
Pair 3	Efficiency - Availability	0.0491	1.0049	0.0787	0.6235	162	0.5338
Pair 4*	Efficiency - Responsiveness	-0.2086	0.8989	0.0704	-2.9625	162	0.0035
Pair 5*	Efficiency - Security	0.3436	1.0851	0.0850	4.0421	162	0.0001
Pair 6	Time - Reliability	-0.0123	0.6666	0.0522	-0.2350	162	0.8145
Pair 7*	Time - Availability	0.2393	0.9676	0.0758	3.1570	162	0.0019
Pair 8	Time - Responsiveness	-0.0184	0.6981	0.0547	-0.3366	162	0.7368
Pair 9*	Time - Security	0.5337	1.1401	0.0893	5.9771	162	0.0000
Pair 10*	Reliability - Availability	0.2515	0.9645	0.0755	3.3297	162	0.0011
Pair 11	Reliability - Responsiveness	-0.0061	0.7973	0.0625	-0.0982	162	0.9219
Pair 12*	Reliability - Security	0.5460	1.0316	0.0808	6.7574	162	0.0000
Pair 13*	Availability - Responsiveness	-0.2577	1.0691	0.0837	-3.0769	162	0.0025
Pair 14*	Availability - Security	0.2945	1.2469	0.0977	3.0152	162	0.0030
Pair 15*	Responsiveness - Security	0.5521	1.2676	0.0993	5.5611	162	0.0000

This result is consistent with the findings from the field interviews where the majority of the respondents from the shipper and service provider groups expressed that they do not see security as an apparent competitive advantage that is distinct from the other traditional drivers of supply chain. This result is also consistent with current literature that talks about the fact that

[32] Since there are no a priori theories supporting a higher ranking of one driver versus another driver, the null hypotheses being tested here are whether the difference between the mean rankings of two drivers are significantly different from 0. Therefore, two-tailed tests are used.

[33] Paired t-tests are used instead of Analysis of Variance (ANOVA). This is because the paired t-test procedure compares the means of two variables for a single group with no assumption made about the causal relationship between the two variables. ANOVA on the other hand, seeks to explain the variation in a variable (dependent variable) as a result of the treatment to another variable (independent variable). In this case, since a causal relationship is not logically expected among the ranking of the supply chain drivers, the paired t-test procedure is used.

most private organizations are reluctant to invest in security beyond the minimum necessary for compliance and reducing cargo theft and pilferages (Willis and Ortiz, 2004; Peleg-Gillai et al., 2006).

Although so, it is also important to share that some of the interviewees from the field interviews cited that regardless of what their specific business value propositions are, they either see or are beginning to see security as a potential disruptor to their ability to deliver their value proposition all the time. One of the main reasons cited by respondents is that their general consumer base in North America are very concerned about security and they do not want any breaches to impact their reputation as a preferred supplier. Some of them have also assisted their customers' in their C-TPAT applications.

For those organizations that also consider supply chain management as a competitive advantage and key driver to the fulfilment of their customer service value proposition, notwithstanding what the underlying supply chain driver(s) (e.g. efficiency, timeliness, responsiveness and agility, availability and reliability) are, they do see the potential of supply chain security as becoming an ultimate driver to supply chain excellence, although not immediately. This is because security breaches threaten the fundamental reliability of their operations and value delivery.

5.2 Factors that Affect Attitude Towards Security

From the results of the field interviews, several characteristics stood out as factors that affect an organization's attitude and the extensiveness of their efforts towards ensuring security in the supply chain that they are participating in. These factors are what these organizations look at when they evaluate the general level of risk in their trading environment.

Several hypotheses were derived based on the review of existing literature and the information gathered from the field interviews. The following analyses uses data collected from the web/email survey to validate these hypotheses. Cross-tabulation[34] analyses are performed where appropriate to validate some of these findings.

[34] The cross-tabulation technique is used because the variables used are categorical in nature (Hair et al., 1998). ANOVA is appropriate when variables are scaled.

5.2.1 Organization Size (Annual Revenue)

At the development stage of the field interview questionnaire, the author hypothesized that the size of an organization can have impacts on its attitude towards security improvements. Organization size is measured by the organization's 2006 annual revenues in US dollars.

Results from the field interviews supported this hypothesis. There is a general attitude difference between large and small organizations. Large organizations are characterised by higher annual revenues and/or greater employee count. Large organizations tend to place or have already placed considerably more emphasis on supply chain security. Most, if not all of them expressed that ensuring security in their supply chain is very to extremely important (though not a competitive advantage or supply chain driver). Many of them have also undertaken some form of security initiatives beyond the basic requirements for safe business operations. Eight of the 21 organizations interviewed are C-TPAT certified or in the process of getting their certification and all of them are large organizations with annual revenues greater than US$1 billion. These organizations also tend to be more proactive in employing more sophisticated security enhancement technology. For example, the number of employees within the organization may affect the degree of negative impacts of security breaches. As such, organizations with more employees especially those located in less secure environments, tend to place greater emphasis on personnel security and have more stringent security measures in place such as biometric access controls. With a larger volume of cargo movement and transactions, these larger organizations also have more to lose if a security breach impacts the flow of goods to their markets.

Results from the web/email survey are discussed next. Recall that respondents were asked to express their opinions about the importance of security as a supply chain driver using a 7-point Likert scale. These ratings have been consolidated into three categories – (1) Not important, (2) Moderately important and (3) Very important, for ease of evaluation (see Table 5.3).

An initial visual analysis of the data and bar charts comparing the security driver rating among different annual revenue groups (Table 5.3 and Figure 5.4) show that although there is a larger proportion of organizations in the larger revenue group ranking security as very important, there are no significantly large differences in attitudes between large and small organizations.

Table 5.3: Ranking of security driver by organizations of different sizes.

		Security_Driver			
		Very Important	Moderately Important	Not Important	Total
Annual Revenue	< 20 mil	78%	17%	6%	100%
	20 mil - 100	92%	4%	4%	100%
	100 mil - 500	87%	13%	0%	100%
	500 mil - 1 bil	85%	8%	8%	100%
	> 1 bil	84%	13%	3%	100%
Total		85%	12%	3%	100%

Figure 5.4: Ranking of security driver by organizations of different sizes.

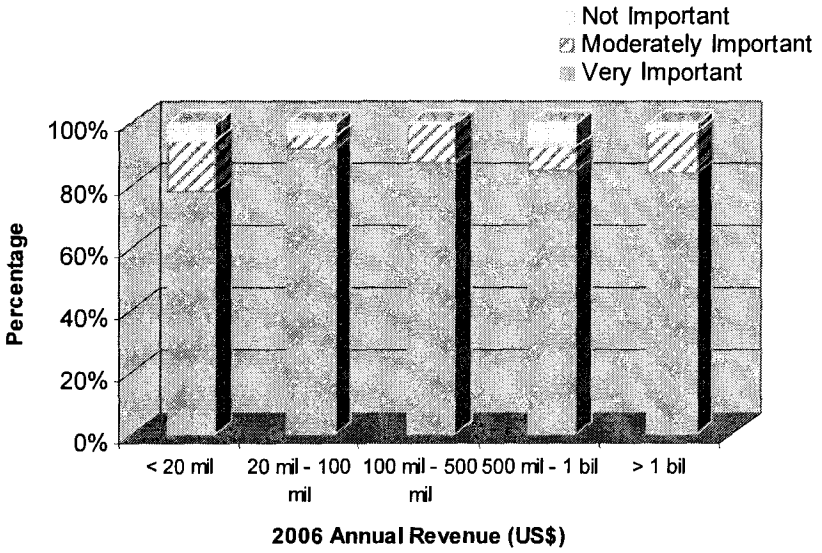


Table 5.4 shows that the difference in mean ranking of security as a supply chain driver between the largest and smallest revenue groups is 0.02. In fact, the results are reversed of our expectations, i.e. respondents in the smallest revenue group have a higher mean ranking compared to respondents in the largest revenue group.

Table 5.4: Mean ranking of security driver for different revenue groups.

Label	Annual_Revenue	Mean	N	Std. Deviation
AR1	< 20 mil	5.61	18	1.29
AR2	20 mil - 100 mil	5.36	25	1.11
AR3	100 mil - 500 mil	5.84	31	1.04
AR4	500 mil - 1 bil	5.54	13	1.66
AR5	> 1 bil	5.59	76	1.32
	Total	5.60	163	1.26

Further statistical tests were performed to determine if these slight differences are statistically significant. Paired sample t-tests were performed and results shown in Table 5.5 are inconclusive. There are only two pairs of revenue groups that have significant differences in their mean ranking of security as a supply chain driver. Pair 2 is between AR1 (< 20 mil) and AR3 (100 mil – 500 mil). Pair 5 is between AR2 (20 mil and 100 mil) and AR3 (100 mil – 500 mil). There are however no consistent patterns between these pairs for any meaningful conclusions to be drawn.

Table 5.5: Results for statistical tests for significance in differences in security driver ranking.

		Paired Differences					t	df	Sig. (2-tailed)
		Mean	Std. Deviation	Std. Error Mean	95% Confidence Upper	95% Confidence Lower			
Pair 1	AR1 - AR2	0.1111	1.3672	0.3223	-0.5688	0.7910	0.3448	17	0.7345
Pair 2*	AR1 - AR3	-0.6111	1.7536	0.4133	-1.4832	0.2609	-1.4785	17	0.1576
Pair 3	AR1 - AR4	0.0769	2.5646	0.7113	-1.4728	1.6267	0.1081	12	0.9157
Pair 4	AR1 - AR5	0.3333	2.2229	0.5239	-0.7721	1.4387	0.6362	17	0.5331
Pair 5*	AR2 - AR3	-0.6800	1.2490	0.2498	-1.1956	-0.1644	-2.7222	24	0.0119
Pair 6	AR2 - AR4	0.1538	1.7723	0.4915	-0.9171	1.2248	0.3130	12	0.7597
Pair 7	AR2 - AR5	-0.0400	2.0306	0.4061	-0.8782	0.7982	-0.0985	24	0.9224
Pair 8	AR3 - AR4	1.0769	1.7541	0.4865	0.0169	2.1369	2.2136	12	0.0470
Pair 9	AR3 - AR5	0.2581	2.0489	0.3680	-0.4935	1.0096	0.7013	30	0.4885
Pair 10	AR4 - AR5	0.1538	1.9936	0.5529	-1.0509	1.3586	0.2782	12	0.7856

Further cross-tabulation analyses were also conducted with the following control variables: (1) respondent type (i.e. shipper versus service provider), (2) entire firm versus SBU and (3) respondent physical location (i.e. Asia versus North America).

Table 5.6 shows one of the cross-tabulation results with respondent type as the control variable. The corresponding chi-square test is shown in Table 5.7 and results indicate no statistically significant differences in the mean ranking of security as a supply chain driver among the groups.

None of the other cross-tabulation results for control variables – firm versus SBU and respondent physical location, indicate statistically significant differences in the mean ranking of security as a supply chain driver among the groups. Detailed results for the other cross-tabulation analyses are not provided here because they are all statistically insignificant. They can however be found in Appendix F.

Table 5.6: Cross-tabulation results (respondent type).

Respondent_Type				Security_Driver			Total
				Not Important	Moderately Important	Very Important	
Shipper	Annual_Revenue	< 20 mil	Count	0	1	4	5
			% within Annual_Revenue	.0%	20.0%	80.0%	100.0%
		20 mil - 100 mil	Count	1	1	9	11
			% within Annual_Revenue	9.1%	9.1%	81.8%	100.0%
		100 mil - 500 mil	Count	0	4	17	21
			% within Annual_Revenue	.0%	19.0%	81.0%	100.0%
		500 mil - 1 bil	Count	1	1	9	11
			% within Annual_Revenue	9.1%	9.1%	81.8%	100.0%
		> 1 bil	Count	1	9	55	65
			% within Annual_Revenue	1.5%	13.8%	84.6%	100.0%
	Total		Count	3	16	94	113
			% within Annual_Revenue	2.7%	14.2%	83.2%	100.0%
Service Provider	Annual_Revenue	< 20 mil	Count	1	2	10	13
			% within Annual_Revenue	7.7%	15.4%	76.9%	100.0%
		20 mil - 100 mil	Count	0	0	14	14
			% within Annual_Revenue	.0%	.0%	100.0%	100.0%
		100 mil - 500 mil	Count	0	0	10	10
			% within Annual_Revenue	.0%	.0%	100.0%	100.0%
		500 mil - 1 bil	Count	0	0	2	2
			% within Annual_Revenue	.0%	.0%	100.0%	100.0%
		> 1 bil	Count	1	1	9	11
			% within Annual_Revenue	9.1%	9.1%	81.8%	100.0%
	Total		Count	2	3	45	50
			% within Annual_Revenue	4.0%	6.0%	90.0%	100.0%

Table 5.7: χ^2 test for cross-tabulation results with respondent type as control variable.

Respondent_Type		Value	df	Asymp. Sig. (2-sided)
Shipper	Pearson Chi-Square	5.346[a]	8	.720
	Likelihood Ratio	4.760	8	.783
	Linear-by-Linear Association	.306	1	.580
	N of Valid Cases	113		
Service Provider	Pearson Chi-Square	6.457[b]	8	.596
	Likelihood Ratio	8.170	8	.417
	Linear-by-Linear Association	.003	1	.959
	N of Valid Cases	50		

Therefore, we conclude that the survey data does not seem to support the hypothesis that larger organizations tend to place more importance on security improvements. This could be a reflection of a "need" to be "politically correct" when it comes to security issues.

5.2.2 Extent of Overseas Sourcing

An organization's key sourcing countries also affect the degree of their security efforts. Of the sample of organizations interviewed in Vancouver, Canada, organizations that do a lot of overseas sourcing especially from Asia and/or the Middle East, tend to place more efforts and emphasis on security issues and related legislative developments. Organizations that source the majority of their products from within Canada or just across the border from U.S. are less concerned about security breaches such as terrorism. This could be due to the confidence they have in the integrity of both the Canadian national transportation network and the U.S. customs authorities at the border-crossings between the two countries. Similarly for exporters in Asia, organizations that use a relatively larger percentage of raw material imports in their production of final products tend to see security as a more immediate operations element compared to organizations that source most of their raw materials locally.

Information regarding the respondent's organization's degree of overseas sourcing is not collected in the survey instrument.

5.2.3 Cargo Nature

Based on the findings from field interviews, it was hypothesized that the nature of an organization's products may also affect the extent and type of security measures an organization adopts.

Organizations that carry hazardous materials may be more willing to invest in security improvements compared to organizations that do not. Again, similar analyses are performed to determine if the data from the survey supported this hypothesis.

An initial visual analysis of the data and bar charts (Table 5.8 and Figure 5.5) shows that there are no significant differences in the ranking of security as a supply chain driver between organizations who carry hazardous cargo and those who do not.

Table 5.8: Ranking of security driver.
(Between hazardous and non-hazardous cargo carrying organizations)

		Security_Driver			
		Very Important	Moderately Important	Not Important	Total
Hazardous	No	84.44%	11.11%	4.44%	100%
	Yes	86.30%	12.33%	1.37%	100%
	Total	85.28%	11.66%	3.07%	100%

Figure 5.5: Ranking of security driver.
(Between hazardous and non-hazardous cargo carrying organizations)

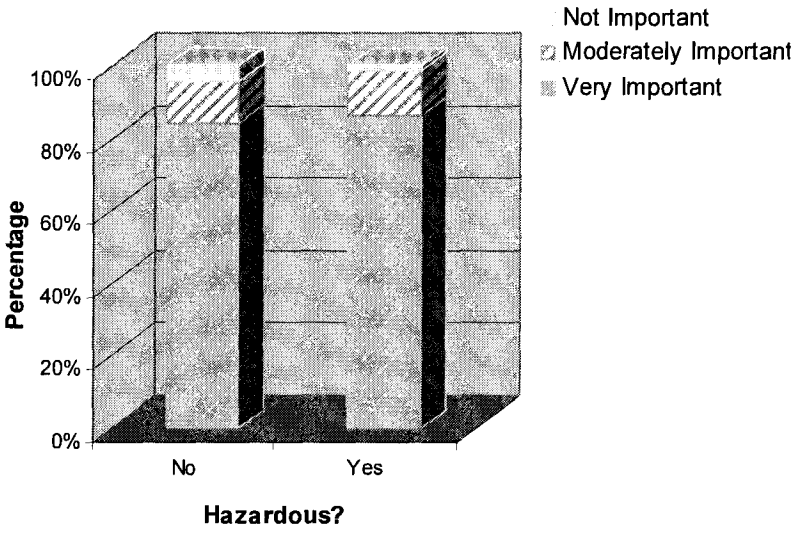


Table 5.9 shows that the difference in mean ranking of security as a supply chain driver between the two groups is 0.27. Further statistical tests were performed to determine if the difference in mean rankings between the two groups of respondents is statistically significant. Results of the paired sample t-tests show that this slight difference of 0.27 is statistically not significant (Table 5.10).

Table 5.9: Mean ranking of security driver.
(Between hazardous and non-hazardous cargo carrying organizations)

Hazardous	Mean	N	Std. Deviation
No	5.48	90	1.33
Yes	5.75	73	1.16
Total	5.60	163	1.26

Table 5.10: Results for statistical tests for significance in differences in security driver ranking.

		Paired Differences					t	df	Sig. (2-tailed)
		Mean	Std. Deviation	Std. Error Mean	95% Confidence Interval Upper	Lower			
Pair 1	No - Yes	-0.3151	1.9499	0.2282	-0.7700	0.1399	-1.3806	72	0.1717

Further cross-tabulation analyses were conducted with the following control variables: (1) respondent type (i.e. shipper versus service provider), (2) entire firm versus SBU and (3) respondent physical location (i.e. Asia versus North America). None of the cross-tabulation results indicate statistically significant differences in the mean ranking of security as a supply chain driver between the two groups. Detailed results of these cross-tabulations are not provided here because they are statistically insignificant but they can be found in Appendix F.

We therefore conclude that the results from the survey do not support the hypothesis that organizations carrying hazardous cargo have a greater tendency to view security as a supply chain driver compared to organizations that do not.

This observation could be due to the fact that the movement of hazardous cargo has had a long history of being under the governance of The Responsible Care ® ethic.[35] As such, for organizations that move hazardous materials, they do not see themselves as doing anything very differently. They have also always viewed safety and security of cargo movement as an important element in their customer fulfilment process. Organizations that do not move hazardous cargo, on the other hand, will now view security as more important than in the past because of the influx of international cargo movement security regulations and requirements.

5.2.4 Size of Shipment

The typical size of an organization's shipments also speaks of the amount of risk and potential losses an organization will suffer in the event of a security breach. All else being equal, organizations with typically smaller shipments are exposed to considerably lesser potential losses from security breaches, although they experience a greater number of hand-offs in their cargo movement process.

[35] The Responsible Care ® ethic is the chemical industry's global voluntary initiative under which companies, through their national associations, work together to continuously improve their health, safety and environmental performance, and to communicate with stakeholders about their products and processes. http://www.responsiblecare.org

Organizations interviewed that tend to have relatively smaller shipments (that is, less-than-container loads), are less worried about security breaches compared to those who typically ship full container loads and in large quantities. For example, one of the organizations interviewed uses mainly air freight because of the very small size of their shipments and relatively high retail value of their products. The supply chain manager interviewed cited his confidence in airfreight movement as one of the reasons why his organization has yet to invest heavily in security initiatives.

Again, data collected from the web survey is analysed to determine if this hypothesis is valid. An initial visual analysis of the data and bar charts (Table 5.11 and Figure 5.6) show that there are no significant differences in the ranking of security as a driver between the two groups.

Table 5.11: Ranking of security driver between FCL and no-FCL cargo carrying organizations.

		Security_Driver			
		Very Important	Moderately Important	Not Important	Total
FCL	No	90.32%	6.45%	3.23%	100%
	Yes	84.09%	12.88%	3.03%	100%
	Total	85.28%	11.66%	3.07%	100%

Figure 5.6: Ranking of security driver.
(Between FCL and No-FCL cargo carrying organizations)

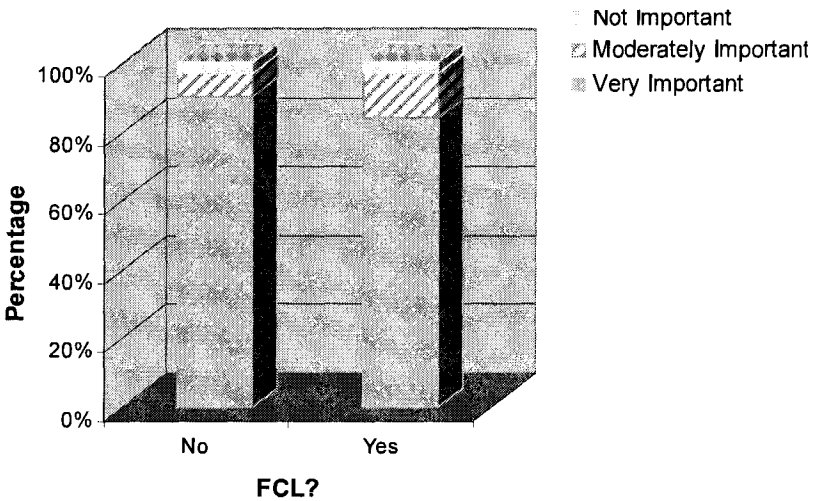


Table 5.12 shows that the difference in mean ranking of security as a supply chain driver between the two groups is 0.13. In fact, these mean values are reversed of our expectations. Respondents in the No-FCL group have a greater mean ranking than respondents in the Yes-FCL group. Reasons for this observation include:

- Respondents in the no-FCL group may perceive non-FCL shipments as more vulnerable compared to FCL shipments as a result of more number of hand-offs and re-handling of cargo.
- A closer look at the supply chain types of the respondents in the non-FCL group and FCL group reveals a wider mix of respondents in the FCL group. Respondents in the non-FCL group consist of organizations handling FMCG, food and pharmaceuticals and electronics. The FCL group on the other hand consist of organizations handling anything from FMCG to heavy machinery, chemicals, forestry and aerospace. This wide mix may have even-out any strong opinions some respondents might have regarding the importance of security as a business driver.

Further statistical tests were however performed to determine if the difference in mean rankings between the two groups of respondents is statistically significant. Results of the paired sample t-tests show that this slight difference of 0.13 is statistically not significant (Table 5.13).

Table 5.12: Mean ranking of security driver.
(Between organizations who ship FCL and those who do not)

FCL	Mean	N	Std. Deviation
No	5.71	31	1.13
Yes	5.58	132	1.29
Total	5.60	163	1.26

Table 5.13: Results of statistical tests for significance in differences in security driver ranking.

		Paired Differences					t	df	Sig. (2-tailed)
		Mean	Std. Deviation	Std. Error Mean	95% Confidence Interval Upper	Lower			
Pair 1	No - Yes	0.2258	1.8567	0.3335	-0.4552	0.9068	0.6771	30	0.5035

Further cross-tabulation analyses were conducted with same control variables: (1) respondent type (i.e. shipper versus service provider), (2) entire firm versus SBU and (3) respondent physical location (i.e. Asia versus North America). None of the cross-tabulation results indicate statistically significant differences in the mean ranking of security as a supply chain driver between the two groups. Detailed results for these cross-tabulation analyses are not provided because they are all statistically insignificant but can be found in Appendix F.

We therefore conclude that the results from the survey do not support the hypothesis that organizations carrying FCL cargo have a greater tendency to view security as a supply chain driver compared to organizations that do not. Again this could be due to the "need" to be "politically correct" on a sensitive issue such as security.

5.2.5 Scope of Supply Chain Control/Influence

In the field interviews, interviewees were also asked to give an assessment of the span of control and influence their organization has over the supply chain that they are participating in. Although most of the organizations interviewed consider supply chain security to be very to extremely important and recognize the importance of the role of market dynamics in their onward efforts in supply chain security, organizations with different scope of control over their supply chain can take quite a different stance as to of who should lead the security initiatives in the supply chain.

Organizations with a narrower span of control/influence (such as terminals and suppliers selling mainly Ex-works) tend to feel that the ultimate customer (i.e. the buyer) should take the lead in initiating supply chain wide security improvements and also assume the costs of such initiatives. Organizations that has a wider span of control or influence over their supply chain, on the other hand, tends to view supply chain management as one of their organization's competitive advantage. These organizations tend to be shippers (either exporters or importers) but can also be large service providers. These organizations tend to take a more proactive approach towards ensuring security in the supply chain that they are participating in. Organizations in this group also can afford more high-tech security solutions such as biometrics access controls but most of the initiatives taken by this group of organizations are more internal in nature and seeks to protect the safety and interests of their company's personnel only.

Based on a list of 16 supply chain activities (Table 5.14), interviewees and survey respondents were asked to indicate whether an activity is controlled in-house, outsourced and managed through contractual obligations and performance measurements or not controlled at all.

Table 5.14: List of supply chain activities.

Activity	Aspects of Supply Chain
A	Choice of suppliers (e.g. manufacturers)
B	Trucking or other inter-modal transportation from factory to origin port
C	Warehousing at origin
D	Freight consolidation at origin
E	Customs clearance at origin
F	Cross-border trucking to origin port or final destination (if required)
G	Choice of port of loading
H	Choice of terminal at origin
I	Choice of carriers (i.e. freight contracts)
J	Choice of port of destination
K	Choice of terminal at destination
L	Customs clearance at destination
M	Cross-border trucking from destination port to final destination (if required)
N	Warehousing at destination
O	Freight deconsolidation / break bulk at destination
P	Trucking or other inter-modal transportation to final location at destination

For shippers, these activities are grouped into two clusters based on where these activities take place (i.e. where the control is exerted). This is because the origin operations and destination operations are usually handled or overseen by different business entities (i.e. sellers for origin and buyers for destination). The origin cluster for shippers includes seven activities B to H. The destination cluster for shippers includes nine activities A, I to P. Activity A is included in the destination cluster because the decision as to which suppliers to use is made by the buyer at destination. Activity I – choice of carriers is included in the destination cluster because sellers/suppliers usually sell free-on-board (FOB) and buyers are more often than not the ones who determine which carrier to use based on either pre-negotiated contracts (for volume discount) or sailing schedules that meet their cargo required date. Even when buyers themselves do not command the volumes for full-container-load shipping, they are usually the ones who engage freight forwarders.

For service providers, there are also two clusters – one for origin and one for destination. These clusters are appropriate because service providers always have a physical presence in the geographical locations that they serve and operations decisions are always made locally. However, activity A is not applicable. Therefore, the eight activities in the origin cluster include activities B to I and destination cluster includes seven activities J to P. In the case of service providers, Activity 7 – choice of carriers, is included in the origin cluster because in the rare event that the service provider gets to decide which carrier to use, it is the office at the origin location that makes that decision and triggers the booking with the ocean carrier.

An organization's span of control is represented as wide, average or narrow (see Table 5.15).

For shippers, wide span of control refer to sellers with at least some destination control or buyers with at least some origin control. Average span of control refer to sellers with only destination control or buyers with only origin control. Narrow span of control refers to sellers with less than total origin control and buyers with less than total destination control.

For service providers, those with wide control include (1) primarily origin service providers[36] (such as origin port, terminals, customs broker, 3PL, trucker, freight forwarder and consolidator) with at least some destination control, (2) primarily destination service providers (such as destination port, terminal, customs broker, 3PL, trucker, freight forwarder and consolidator) with at least some origin control and (3) global service providers with control over at least 70% of the activities. Those with average control include (1) primarily origin service providers with only origin control, (2) primarily destination service providers with only destination control and (3) global service providers with control of 40% to 70% of the activities. Those with narrow control include (1) primarily origin service providers with control over less than 100% of origin activities, (2) primarily destination service providers with control over less than 100% of destination activities and (3) global service providers with control over less than 30% of the activities.

Table 5.15: Definitions of span-of-control.

Span-of-Control	**Definition**
Wide	Sellers with at least some destination control. Buyers with at least some origin control. Primarily origin service providers with at least some destination control. Primarily destination service providers with at least some origin control. Global service providers with control over > 70% of activities.
Average	Sellers with only destination control. Buyers with only origin control. Primarily origin service providers with only origin control. Primarily destination service providers with only destination control. Global service providers with control over 40% to 70% of activities.
Narrow	Sellers with less than total origin control. Buyers with less than total destination control. Primarily origin service providers with less than total origin control. Primarily destination service providers with less than total destination control. Global service providers with control over <30% of activities.

[36] Determined based on a combination of characteristics: (1) the physical location of the respondent, (2) the industry type and (3) the major trade routes or simply the name of the organization. Origins are in Asia and destinations are in North America.

So does an organization's span of control over their supply chain affect the amount of importance they place on security as a supply chain driver? The data and bar charts in Table 5.16 and Figure 5.7 show that there are no significant differences among organizations with different span of supply chain control.

Table 5.16: Ranking of security driver among organizations with different span of control.

		Security_Driver			
		Very Important	Moderately Important	Not Important	Total
Control Span	Wide	86.25%	12.50%	1.25%	100%
	Average	80.00%	15.00%	5.00%	100%
	Narrow	88.37%	6.98%	4.65%	100%
Total		85.28%	11.66%	3.07%	100%

Figure 5.7: Ranking of security driver among organizations with different span of control.

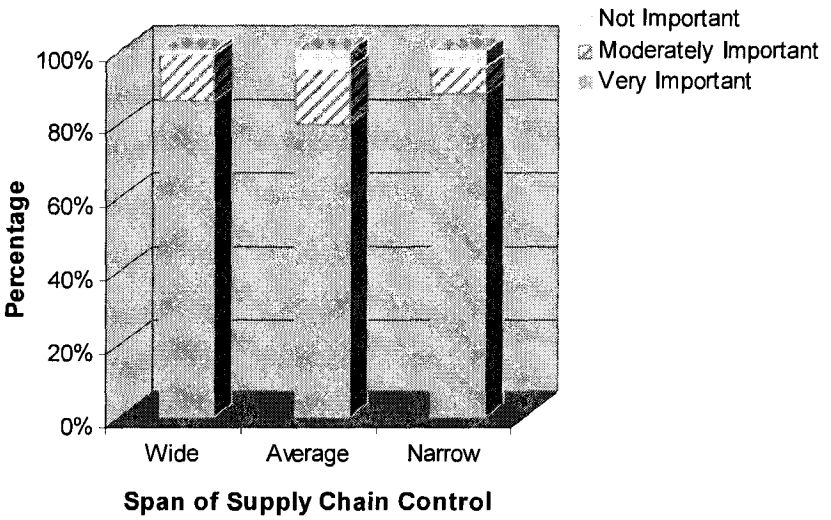


Table 5.17 shows that the difference in the mean ranking between the wide and the narrow group is 0.01 and that between the wide group and the average group is 0.1. In order to determine if these very slight differences are significant, paired sample t-tests are performed.

Table 5.17: Mean ranking of security driver among organizations with different control span.

Control Span	Mean	N	Std. Deviation
Wide	2.85	80	0.39
Average	2.75	40	0.54
Narrow	2.84	43	0.48
Total	2.82	163	0.46

Table 5.18 shows that none of the differences between any two groups are statistically significant. Therefore, the data does not support the hypothesis that an organization's span of supply chain control affects the amount of importance they place on security. The reason why this was otherwise in the field interviews could be due to the "need" for the interviewee to say the "right thing" in the presence of an interviewer (i.e. lack of anonymity).

Table 5.18: Results for statistical tests for significance in differences in security driver ranking.

		Paired Differences					t	df	Sig. (2-tailed)
		Mean	Std. Deviation	Std. Error Mean	95% Confidence Interval Upper	Lower			
Pair 1	Wide - Average	0.3250	2.1648	0.3423	-0.3673	1.0173	0.9495	39	0.3482
Pair 2	Wide - Narrow	0.3953	1.8276	0.2787	-0.1671	0.9578	1.4185	42	0.1634
Pair 3	Average - Narrow	0.0750	1.8171	0.2873	-0.5061	0.6561	0.2610	39	0.7954

5.2.6 Summary of Attitude Analyses

In summary, hypotheses 6 to 9 below are not supported when the web/email survey data are analysed in isolation. Even when control variables such as respondent type, physical location and firm/SBU responsibility scope are introduced separately, the results are not statistically significant.

Hypothesis 6: Organization size affects attitude towards security.

Hypothesis 7: The nature of cargo handled (hazardous or lack thereof) affects attitude towards security.

Hypothesis 8: Typical shipment size (FCL or LCL) affects attitude towards security.

Hypothesis 9: Scope of supply chain decision control/influence affects attitude towards security.

This may mean that an organization's attitude towards security is impacted by a simultaneous existence of one or more of the above variables – organization size, nature of cargo, shipment size and scope of supply chain control. It is possible in principle to cross-tabulate many variables with the possibility of obtaining further insights into lower order associations. However, the need to maintain an adequate cell size for all categories presents a practical limitation.

Ordinal regression is used to validate this conjecture[37] because the dependent and independent variables in this case are non-metric. For details of this technique, please refer to McCullagh (1980). Results of the ordinal regression[38] are shown in Table 5.19.

Table 5.19: Ordinal regression results – model-fitting information.

Model Fitting Information

Model	-2 Log Likelihood	Chi-Square	df	Sig.
Intercept Only	283.587			
Final	276.149	7.438	8	.490

The significance level for the chi-square statistic as shown in Table 5.19 is greater than 0.05, indicating that the model is only as good as simple guessing. This statistically insignificant result shows a divergence in the security attitudes found in the field interviews and web/email survey. This could be a reflection of the need for respondents to give "politically correct" answers during an interview. But when given the opportunity to remain anonymous on a web/email survey, respondents can be more candid about their opinions. For instance, larger organizations especially those with global operations, may be more concern about their corporate image compared to smaller local organizations. As such during a face-to-face interview, they can be more likely to give "politically correct" responses. Organizations who carry hazardous cargo certainly do not want to be perceived as not placing enough importance on security and thus during a face-to-face interview may "overstate" their efforts and positive attitudes towards security. Organizations who has a greater span of control certainly also do not want to be perceived as not doing much when especially when they have the ability to do so and thus may also "overstate" their enthusiasm towards security.

5.3 Supply Chain Security a Holistic Effort

Although the majority of the organizations interviewed during the field interviews have not assumed a lead role in driving security initiatives within the supply chain that they are

[37] Multiple regression and multiple discriminant analyses are not appropriate techniques because they require the independent variables to be metric. Multiple-way ANOVA is also not appropriate because the dependent variables are required to be metric.

[38] The complementary log-log function is chosen as the link function because the bulk of the responses for security driver is found in the higher categories.

participating in, they recognize that security within a supply chain can only be achieved through a holistic effort from all stakeholders. This is consistent with the findings from Langhoff et al. (2005) where it is noted that although a wide variety of organizations have put forth proposals and solutions for increasing security, each has fallen short of addressing the needs of the integrated supply chain. Supply chain participants are also found to protect their financial interests without regard to other parties in the integrated chain.

Responses from the organizations interviewed during the field interviews suggest that there are generally two ways in which organizations can influence their supply chain partners' efforts in security – the hard approach and the soft approach.

The hard approach includes measures such as instituting the desired security requirements as pre-requisites to business negotiations or making them legal obligations in business contracts. These measures are more popular with buyer organizations than with service provider organizations. However, there is one buyer organization that commented that unless it can be proven that security initiatives have tangible benefits to their bottom-line or top-line, it will be tough to convince his organization and probably other companies in his industry to adopt any security efforts out of self-interests, not to even mention about driving their other partners in the same direction.

The soft approach includes proactive engagement measures such as communications, education and training to create awareness about security among the other stakeholders in their supply chain. A few of the organizations interviewed have already conducted security training with their suppliers/vendors. These training efforts can come in the form of formalised security manuals, online training modules and/or security seminars.

5.4 KPIs for Supply Chain Performance and Security Performance

In this section, we want to find out what KPIs are appropriate for security performance of an international maritime supply chain from industry's practitioners' point of view. From there, we seek to understand how security KPIs are related to traditional supply chain KPIs.

5.4.1 Determining the Appropriate KPIs for Factor Analysis

First, the frequency statistics for the appropriateness of the KPI variables were computed to identify those KPI variables that are deemed to be inappropriate for measuring Supply Chain Performance (SCP) or Security Performance (SP). KPI variables that are deemed inappropriate will not be included in the initial factor analysis. Table 5.20 shows that for each KPI variable, the percentage (%) of respondents who thinks that it is an appropriate or inappropriate measurement for SCP and SP. The total number of respondents (N) = 125. The total number of KPI variables = 32.

A full description of the KPIs can be found in Appendix C.

Table 5.20: KPIs and their appropriateness frequencies.

		SCP			Security		
S/N	KPI	App	Indiff	Not app	App	Indiff	Not app
1	AssetUtilize	89.6	9.6	0.8	41.6	31.2	27.2
2	SecurityAudit	68	26.4	5.6	87.2	11.2	1.6
3	OpsEfficiency	90.4	8	1.6	31.2	33.6	35.2
4	PolicyViolations	70.4	20.8	8.8	91.2	7.2	1.6
5	InsurancePremiums	56	34.4	9.6	57.6	34.4	8
6	InventoryLevel	84.8	13.6	1.6	42.4	34.4	23.2
7	InspectionCost	60	29.6	10.4	67.2	24	8.8
8	LogCostSavings	83.2	12	4.8	24	36.8	39.2
9	ShipmentInfo	88	12	0	54.4	26.4	19.2
10	UnauthorizedEntry	56.8	30.4	12.8	85.6	10.4	4
11	FulfillmentLT	90.4	8	1.6	27.2	34.4	38.4
12	OTDelivery	96	4	0	38.4	31.2	30.4
13	ExpeditedOrders	93.6	5.6	0.8	29.6	37.6	32.8
14	CustomsLT	75.2	18.4	6.4	54.4	31.2	14.4
15	InfoAccuracy	88.8	11.2	0	63.2	20	16.8
16	ServiceErrors	88.8	10.4	0.8	50.4	28.8	20.8
17	SafetyAudit	68	28	4	69.6	18.4	12
18	InventoryAccuracy	88.8	8.8	2.4	55.2	24.8	20
19	InvoiceAccuracy	85.6	12	2.4	37.6	31.2	31.2
20	Pilferage	79.2	15.2	5.6	90.4	6.4	3.2
21	FreightClaims	84.8	13.6	1.6	74.4	15.2	10.4
22	SafetyAccidents	78.4	19.2	2.4	53.6	24	22.4
23	OSD	88	8.8	3.2	72.8	14.4	12.8
24	OpsDeviation	81.6	16	2.4	36	34.4	29.6
25	BackOrders	80.8	14.4	4.8	22.4	35.2	42.4
26	Cancellations	72	21.6	6.4	20.8	39.2	40
27	ProblemResponse	88.8	10.4	0.8	26.4	35.2	38.4
28	ProblemResolution	85.6	12.8	1.6	24.8	35.2	40
29	FeedbackSurvey	91.2	8	0.8	32.8	37.6	29.6
30	FillRate	85.6	13.6	0.8	19.2	36.8	44
31	SpecialRequests	73.6	20.8	5.6	24	39.2	36.8
32	Complaints	84	13.6	2.4	28.8	42.4	28.8

Legend: App = Appropriate Indiff = Indifferent Not app = Inappropriate

Table 5.20 shows that all the KPI variables are deemed appropriate for SCP by majority of the respondents (i.e. greater than two-thirds or greater than 66.7%) of the respondents except for:

- Insurance premiums 56%
- Inspection costs 60%
- Unauthorized entry 57%

With regards to SP, less than 50% of the respondents deemed 17 of the 32 KPI variables as appropriate measurements for security performance (Table 5.20). These KPI variables are highlighted and boxed in Table 5.20 and will not be included in the SP factor analysis.

5.4.2 Factor Analysis for SCP KPIs

Since all the KPI variables are deemed appropriate by more than half the respondents, all were included in the initial factor analysis for SCP.

Appropriateness of Factor Analysis

The data for SCP KPI appropriateness is considered categorical (ordinal data). To determine whether factor analysis is appropriate, the Bartlett's Test and Measure of Sampling Adequacy were calculated.

The Bartlett's Test is a statistical test for the presence of correlations among the variables. If there is insufficient correlation among variables, then factor analysis may not be appropriate. The Bartlett's Test provides the statistical probability that the correlation matrix has significant correlations among at least some of the variables. In this case, when taken overall, the correlations among the KPI variables are significant at 0.000.

However, as the sample size increases, the Bartlett's Test becomes more sensitive to detecting correlations among the variables. Moreover, the Bartlett's Test only indicates the presence of non-zero correlations, not the pattern of these correlations.

Another measure to quantify the degree of inter-correlations among the variables and the appropriateness of factor analysis is the MSA index, which can range from 0 to 1. Therefore, the larger the MSA index, the more appropriate is factor analysis for the data set. The general

guidelines are 0.80 and above, meritorious; 0.70 or above, middling; 0.60 or above, mediocre; 0.50 or above, miserable; and below 0.50, unacceptable.

Table 5.21: KMO-MSA index and Bartlett's test results.

Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		.724
Bartlett's Test of Sphericity	Approx. Chi-Square	2031.196
	df	496
	Sig.	.000

Both the MSA index and Bartlett's Test indicates the appropriateness and support the use of Factor Analysis for data reduction for SCP KPIs (see Table 5.21).

Choice of Extraction Method

There are two basic models to obtain factor solutions (Hair et al., 1998) – Principal Component Analysis and Common Factor Analysis (also known as Principal Factor Analysis or Principal Axis Factoring).

The principal component factor model is appropriate when the primary concern is about prediction or the minimum number of factors needed to account for the maximum portion of the variance. Wilkinson, Blank and Gruber, 1996) notes that for most datasets, principal component method and common factor method will lead to similar substantive conclusions, though principal component method is generally preferred for purposes of data reduction (translating variable space into optimal factor space), while common factor method is generally preferred when the research purpose is detecting data structure or causal modeling. Since data reduction is the objective over here, the Principal Component method shall be used.

The Principal Axis method and Image Factoring methods are also conducted for comparison purposes and comprehensiveness of the analysis. Image factoring is a factor analysis method based on the correlation matrix of predicted variables rather than actual variables, where each variable is predicted from the others using multiple regression.

The factor pattern matrices were compared[39]. Although the factors generated are similar, the total amount of variance explained is larger when the principal component method is used.

Choice of Rotation Methods

An important tool in interpreting factors is factor rotation. There are two major rotation options – orthogonal or oblique. Orthogonal rotational approach includes approaches such as Quartimax, Varimax and Equimax. Orthogonal rotational approaches assume independence between factors whereas oblique rotational approaches allow factors to be correlated. Oblique rotational approach includes Direct Oblimin and Promax.

The oblique rotational approach should be chosen for this case because a KPI used to measure one aspect of SCP is likely and expected to be correlated with another KPI used to measure another aspect of SCP. This is because the different aspects of SCP are known to be inter-dependent in fulfilling a supply chain objective. A comparison study by Costello and Osborne (2005) also argues and supports the use of a true factor analysis extraction method with oblique rotation for optimal results. Costello and Osborne (2005) adds that while principal components with Varimax rotation and the Kaiser criterion are the norm, they are not optimal particularly when data do not meet assumptions, which are often the case in the social sciences.

However, for the purpose of a comprehensive analysis again, three rotation methods, namely, Direct Oblimin, Promax and Varimax were used on all three methods of extraction mentioned above (i.e. Principal Component, Principal Axis and Image Factoring), and the one that generates the most interpretable factors is chosen as the final factor analysis result.

Table 5.22 summarizes the comparison of factor analysis results among the different combination of extraction and rotation methods. A "tick" indicates that the factor matrix generated by the combination of rotation method and extraction method is the most easily interpretable.

Under different scenarios of extraction criteria (i.e. eigenvalues > 1 and number of factors extracted = 6) and variables used (i.e. all variables are used versus three variables removed), the Promax rotation method generates factors that have variables loading more distinctively on

[39] Factor pattern matrices generated using the Principal Axia, Image Factoring and Principal Component methods are similar.

any one factor, thus making the factor more interpretable. On the other hand, Direct Oblimin and Varimax rotation methods, tend to generate factors that have variables loading significantly on more than one factor.

Table 5.22: Comparison of rotation methods.

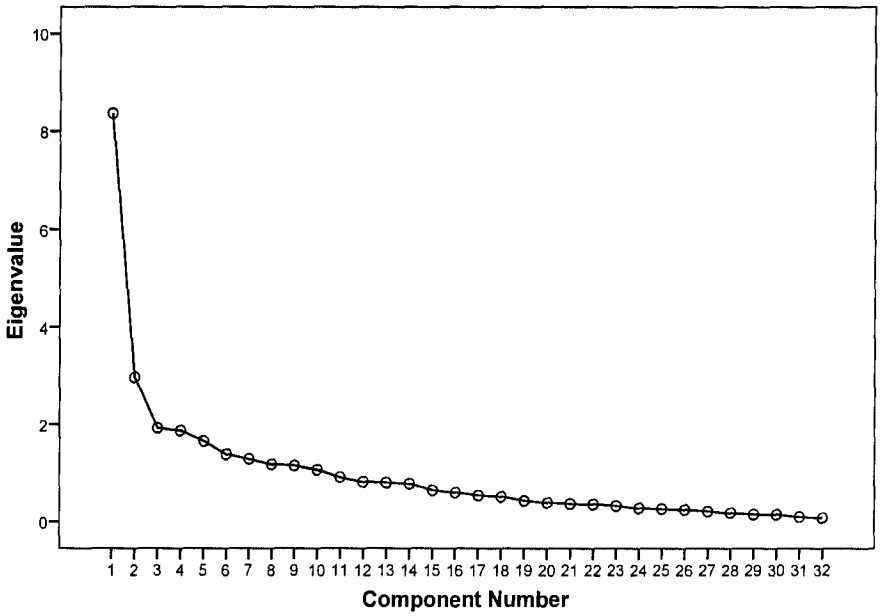
Extraction Methods	Rotation Methods		
	Promax	Oblimin	Varimax
Principal Component	✓	x	x
Principal Axis	x	x	x
Image Factoring	x	x	x

Therefore, overall, the Principal Component extraction method with Promax rotation yielded the most interpretable factors with reasonable total variance explained. The following sections will explain the rationale and logic behind the final selection of the factor matrix.

Interpreting the Factor Matrix

With a total of 32 variables, using the Principal Component extraction method with Promax rotation, the total variance explained by the initial solution of 10 factors (where extraction is based on eigenvalues > 1) is 72%. However, the scree plot suggests the retention of six factors instead (see Figure 5.8 where the "leveling-off" occurs).

Figure 5.8: Scree plot for initial solution.
(Principal component with promax rotation – eigenvalues > 1)



Therefore the extraction criteria used is changed from eigenvalues > 1 to six factors to be extracted. With the extraction criteria of six factors, the total variance explained using all 32 variables is 57%. The generated factors are shown in Table 5.23 and they are not straightforwardly interpretable.

Table 5.23: Pattern matrix.
(Principal component with promax rotation – 6 factors)

	Component					
	1	2	3	4	5	6
SCP_AssetUtilize	.406	-.054	-.076	.238	-.101	.461
SCP_SecurityAudit	-.066	.043	.683	.033	-.325	.188
SCP_OpsEfficiency	.661	.011	-.076	.165	.061	.113
SCP_PolicyViolations	.006	-.053	.785	.049	-.063	-.027
SCP_InsurancePremiums	.012	.225	.387	.317	.010	-.230
SCP_InventoryLevel	.214	-.109	-.109	.050	.671	.044
SCP_InspectionCost	-.127	.203	.273	.175	.310	-.264
SCP_LogCostSavings	-.169	-.210	-.123	.500	.526	.104
SCP_ShipmentInfo	.225	.073	.081	.227	.074	.266
SCP_UnauthorizedEntry	-.004	.284	.717	.037	-.148	-.085
SCP_FulfillmentLT	-.117	.016	.156	-.009	.103	.593
SCP_OTDelivery	.004	.261	.133	.164	-.233	.645
SCP_ExpeditedOrders	-.026	.905	-.102	-.239	.002	.130
SCP_CustomsLT	-.366	.390	.247	.022	.308	.290
SCP_InfoAccuracy	.061	.612	.080	.169	-.043	-.083
SCP_ServiceErrors	.531	.149	-.124	-.121	.122	.221
SCP_SafetyAudit	.209	-.267	.697	-.111	.011	.265
SCP_InventoryAccuracy	.569	-.028	.107	.377	.090	-.171
SCP_InvoiceAccuracy	.502	.655	-.136	-.167	-.095	-.132
SCP_Pilferage	-.087	-.147	.621	-.037	.281	.124
SCP_FreightClaims	.167	.561	.085	-.136	.101	.226
SCP_SafetyAccidents	.670	-.158	.527	-.271	.109	-.050
SCP_OSD	-.029	.672	-.113	.224	.059	.142
SCP_OpsDeviation	-.022	-.044	.015	.840	-.030	-.027
SCP_BackOrders	.122	-.027	-.048	.746	-.017	.140
SCP_Cancellations	.154	-.043	.105	.651	.043	.039
SCP_ProblemResponse	.129	.117	-.016	-.066	.787	.070
SCP_ProblemResolution	.159	.095	-.094	-.051	.810	-.063
SCP_FeedbackSurvey	.200	.036	-.031	-.047	.159	.604
SCP_FillRate	.571	.011	-.061	.462	-.101	.049
SCP_SpecialRequests	.248	.308	.067	.052	.367	-.056
SCP_Complaints	.589	.055	-.031	.023	.349	-.097

As seen from Table 5.23, based on the significant loading(s)[40] each variable has on a particular factor, the factors generated are not immediately interpretable (see values boxed in Table 5.23) because there are three variables (Logistics Cost Savings, Invoice Accuracy and Safety Accidents) with significant loadings (i.e. greater than or equal to 0.40 or at least 0.30 to be acceptable) on more than one factor and there are three variables (Shipment Information, Customs Lead-time and Special Requests) with no significant loadings on any factor.

In order to obtain better loadings, the correlation and communalities tables are reviewed. Variables with small communalities (i.e. < 0.40) and high correlation (i.e. > 0.50) with one or more other variables are deleted. Variable SCP_ShipmentInfo is the only variable with a communality value that is less than 0.40 at 0.333 and is therefore a candidate for removal. There are two variables with very high correlations with more than one other variables – SCP_ProblemResponse and SCP_InventoryAccuracy. SCP_ProblemResponse has a large correlation of 0.821 with SCP_ProblemResolution and 0.527 with SCP_SpecialRequests. It is therefore an ideal candidate for removal to minimize duplication of variable representation. SCP_InventoryAccuracy also has a large correlation of 0.641 with SCP_FillRate, 0.524 with SCP_Complaints and 0.501 with SCP_Cancellations. It is therefore also a good candidate for removal to improve the factor loadings.

The factor analysis is re-run with the rest of the 29 variables and the resulting factor matrix is shown in Table 5.24. The factors are interpretable based on each variables highest loading (boxed in Table 5.24) or their alternative significant loadings (circled in Table 5.24).

As seen from Table 5.24, based on their other significant loading values, two variables were loaded on an alternative factor that makes the most sense (see values circled). With this new interpretation, the factors can be named in order from 1 to 6 as, (1) Accuracy of Operations, (2) Security, (3) Efficiency, (4) Availability, (5) Responsiveness/Customer Service and (6) Reliability.

This factor analysis result explains ~58% of total variance. In social sciences or situations where information is less precise, it is not uncommon to consider a solution that accounts for ~60% (and in some instances even less) as satisfactory (Hair et al., 1998).

[40] Generally accepted guidelines for determining whether a loading is significant or not can be found in Hair et al. (1998).

Table 5.24: Pattern matrix.
(Principal component with promax rotation – 29 variables)

	Component					
	Accuracy	Security	Efficiency	Availability	Responsiveness	Reliability
SCP_AssetUtilize	-.055	-.034	.575	.304	-.168	.328
SCP_SecurityAudit	-.016	.676	-.061	.027	-.289	.187
SCP_OpsEfficiency	.016	-.050	.685	.181	.151	-.014
SCP_PolicyViolations	-.042	.790	-.045	.039	-.083	-.031
SCP_InsurancePremiums	.243	.420	-.026	.311	-.033	-.242
SCP_InventoryLevel	-.043	-.134	.149	.052	.753	.094
SCP_InspectionCost	.231	.285	-.180	.178	.301	-.224
SCP_LogCostSavings	-.149	-.122	.531	-.105	.500	.088
SCP_UnauthorizedEntry	.287	.747	-.021	.043	-.228	-.074
SCP_FulfillmentLT	.032	.093	-.069	-.042	.184	.659
SCP_OTDelivery	.264	.108	.111	.143	-.241	.629
SCP_ExpeditedOrders	.899	-.125	-.040	-.262	.021	.197
SCP_CustomsLT	.450	.215	-.342	.012	.228	.385
SCP_InfoAccuracy	.632	.086	.026	.132	-.037	-.076
SCP_ServiceErrors	.101	-.142	.531	-.102	.321	.140
SCP_SafetyAudit	-.293	.679	.183	-.109	.107	.301
SCP_InvoiceAccuracy	.662	-.091	.489	-.157	-.128	-.156
SCP_Pilferage	-.091	.624	-.067	.004	.181	.103
SCP_FreightClaims	.550	.052	.151	-.151	.210	.205
SCP_SafetyAccidents	-.149	.546	.593	-.251	.182	-.086
SCP_OSD	.694	-.115	.007	.209	.046	.139
SCP_OpsDeviation	-.048	.036	-.002	.811	.025	-.032
SCP_BackOrders	-.028	-.013	.223	.759	-.001	.040
SCP_Cancellations	-.052	.117	.151	.618	.157	.066
SCP_ProblemResolution	.226	-.043	.215	.053	.572	-.115
SCP_FeedbackSurvey	.090	-.010	.382	.029	-.003	.514
SCP_FillRate	-.013	-.036	.558	.437	.042	.027
SCP_SpecialRequests	.347	.077	.201	.053	.392	-.003
SCP_Complaints	.055	-.032	.505	.021	.533	-.124

The Bartlett's Test and MSA index were re-calculated and both still indicate the appropriateness of the use of factor analysis. In fact the MSA index is now higher than when the two variables were included (see Table 5.25).

Table 5.25: KMO-MSA index and Bartlett's test results.

Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		.715
Bartlett's Test of Sphericity	Approx. Chi-Square	1619.503
	df	406
	Sig.	.000

As seen from Table 5.26, all the factors (also known as scales) have satisfactory Cronbach's Alpha values. These scales are similar to the key dimensions of SCP discussed in Section 2.5

in Chapter 2. These key dimensions were identified from a rigorous review of 20 of the 116 relevant research studies summarized in Keller et al. (2002), SCOR version 8.0, other current literature on supply chain security and information gathered from the field interviews.

Table 5.26: Cronbach's alpha values for generated factors.

Scale	Cronbach's Alpha	N of Items
Accuracy	0.761	6
Security	0.769	7
Efficiency	0.700	5
Availability	0.748	4
Responsiveness	0.802	4
Reliability	0.792	3

However, instead of having a factor named Timeliness, we have one that's named Accuracy. The time element is instead found in the Reliability and Accuracy factors. For instance, the KPIs for fulfillment lead-time and on-time delivery are found in the Reliability factor and this could be because respondents interpreted the word "Reliability" to mean delivery reliability, a commonly held definition of this term in the logistics industry, despite the definition provided in the survey questionnaire.

The paragraphs below explain the rationale for each scale's labeling.

Factor 1: Accuracy

Factor 1 is made up of six variables – (1) Expedited Orders, (2) Customs Lead-time, (3) Info Accuracy, (4) Invoice Accuracy, (5) Freight Claims and (6) OSD. Info Accuracy and Invoice Accuracy are straightforward indicators of operations accuracy. Freight Claims and OSD are consequences of inaccurate operations such as stuffing and order preparation. Expedited Orders can also be interpreted as a result of errors made in order fulfillment operations because when there are errors in fulfilling the orders, customers usually need to have a re-order expedited in order to meet their business needs. Customs clearance lead-time can be affected if there are inaccuracies between shipment documentation and the physical shipment itself. This is especially relevant in today's global maritime logistics regulatory environment.

Factor 2: Security

Security refers to an organization's state of being secure. And secure refers to the likelihood of an organization's supply chain being compromised in terms of pilferages, thefts, damages,

terrorism and other crimes such as smuggling and contraband etc. The KPI variables in this factor therefore include custom inspection cost, security audit, policy violations, insurance premiums, unauthorized entry, pilferage and safety audit.

Factor 3: Efficiency

Efficiency refers to an organization's accomplishment of or ability to accomplish a job with a minimum expenditure of time, effort and resources. The KPI variables in this factor therefore include asset utilization, operations efficiency and logistics cost savings. The Service Error and Safety Accident variables are also included because it represents wastes in the system and wastes negatively impact an organization's bottom-line.

Factor 4: Availability

Availability refers to an organization's ability to ensure undisrupted supply of products and/or services and/or information. This could be achieved through the provision of shipment information, ensuring supply of special equipment or products, ensuring that sales force is readily available to respond to customers' inquiries and needs. As such, the KPI variables in this factor include order fill rate, amount of backorders and order cancellations. Operations Deviation refers to the deviation in production capacity or capacity to service a client. This variable is included here because without the required operations capacity, an organization is unable to make available her products or services to her customers.

Factor 4: Responsiveness

Responsiveness refers to an organization's accomplishment of or ability to react to changes and/or requests from demand or supply side. This capability includes flexibility and agility and could be enhanced by the use of information technology in terms of greater visibility and/or configuration of business operations to allow operations scaling flexibility and agility. Therefore the KPI variables in this factor include problem resolution lead-time, number of and ability to handle special requests and customer complaints. The KPI variable Inventory Level is included in this factor because without an adequate and appropriate level of inventory, an organization will not be able to respond effectively and reliably to customer demand.

Factor 5: Reliability

Reliability refers to an organization's dependability of product/service delivery operations. KPI variables in this factor therefore include delivery related measures such as on-time delivery and

fulfillment lead-time. The KPI variable Feedback Survey is also included in this factor because the customer feedback survey usually asks about the areas where an organization comes into contact with the customer and a large part of the contact happens downstream during the product/service delivery stage.

What is really important here is that it can also be seen from the resulting factors that there is indeed a component for Security. This means that organizations have all along been measuring an aspect of their operations that relates to security. As such, organizations should not perceive the current change in intensity of interests in security as throwing them off-balance.

The KPI variables for security are looked at next to identify what the KPIs are for security performance from the industry practitioners' point of view.

5.4.3 Factor Analysis for SP KPIs

Recall that less than 50% of the respondents deemed 17 of the 32 KPI variables as appropriate measurements for security performance (see Table 5.20 on page 104). These KPI variables are boxed in Table 5.20 and will not be included in the factor analysis. The remaining 15 KPI variables are ranked below in a descending order (in Table 5.27) based on the appropriate percentage.

Table 5.27: KPIs deemed appropriate for security performance.

S/N	KPI Name	% of Respondents	Corresponding SCP Factor
1	Policy violations	91.2	Security Factor
2	Pilferage	90.4	Security Factor
3	Security audit	87.2	Security Factor
4	Unauthorized entry	85.6	Security Factor
5	Freight claims	74.4	Accuracy Factor
6	OSD	72.8	Accuracy Factor
7	Safety audit	69.6	Security Factor
8	Inspection cost	67.2	Security Factor
9	Information accuracy	63.2	Accuracy Factor
10	Insurance premiums	57.6	Security Factor
11	Inventory accuracy	55.2	Not included in SCP Analysis
12	On-time shipment information	54.4	Not included in SCP Analysis
13	Customs lead time	54.4	Accuracy Factor
14	Safety accidents	53.6	Efficiency Factor
15	Service errors	50.4	Efficiency Factor

As expected, eight of these 15 KPI variables that are deemed appropriate measures of SP by majority of the respondents are also loaded in the Security Factor of SCP.

For the other KPI variables in Table 5.27, three coincide with those that load in the Reliability factor of SCP, two in the Timeliness factor, one in the Efficiency factor and one in the Availability factor respectively.

This set of results shows that respondents feel that security performance will have an impact on not just one but many aspects of SCP. This is consistent with current literature on the collateral benefits of security efforts and this is logical for the following reasons:

- security issues create uncertainties in the supply chain and uncertainties affects the reliability of supply chain operations. As noted by Rice and Spayd (2005), some firms have estimated the cost of trade discontinuity to be as high as US$50-100 million/day.

- unreliable supply chain operations in turn jeopardize the ability of the organization to make available their products and services to their customers.

- customs regulations such as advanced shipment information has lengthened supply chains in terms of overall time required to move cargo.

- the overall increase in fulfillment lead time in turn brings about negative impacts to the efficiency of an organization's supply chain operations.

- the mushrooming of security regulations now present more opportunities for non-compliance (either deliberate or due to ignorance) and therefore presenting more windows for service errors and inefficiencies in the supply chain.

Factor Analysis Results

Since only these 15 KPI variables are deemed appropriate, the data reduction effort for SP is based only on these 15 variables.

The same extraction method and rotation methods are employed – Principal Components and Promax. The Bartlett's Test and MSA index both indicate the appropriateness of the use of factor analysis (see Table 5.28).

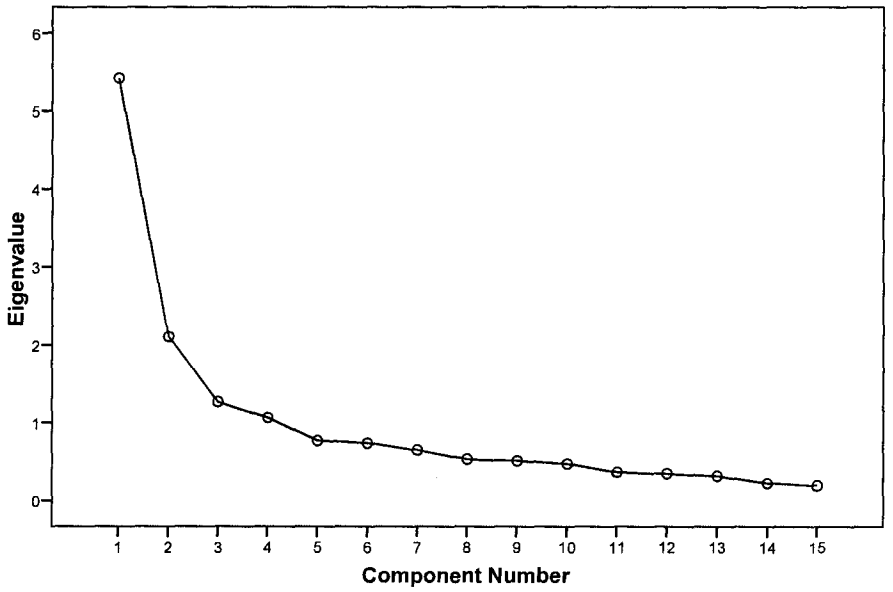
The total variance explained is 65% and four factors have been extracted in the initial solution with extraction criteria as eigenvalues > 1.

Table 5.28: KMO-MSA index and Bartlett's test results.

Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		.814
Bartlett's Test of Sphericity	Approx. Chi-Square	742.130
	df	105
	Sig.	.000

The scree plot in Figure 5.9 also supports the extraction of four factors. The last dip is between four and five factors.

Figure 5.9: Scree plot for SP factor analysis (eigenvalues > 1).



The resulting factor pattern matrix is shown in Table 5.29.

Table 5.29: Pattern matrix for SP factors.
(Principal component with promax rotation)

	Component			
	Information	Breaches	Cost	Safety
SP_SecurityAudit	-.008	.922	-.083	-.068
SP_PolicyViolations	.101	.810	-.232	.039
SP_InsurancePremiums	-.111	-.042	.866	.120
SP_InspectionCost	.090	.002	.797	-.132
SP_ShipmentInfo	.643	-.115	.015	.158
SP_UnauthorizedEntry	-.095	.797	.141	.005
SP_CustomsLT	.830	-.071	.081	-.195
SP_InfoAccuracy	.952	.012	-.002	-.215
SP_ServiceErrors	.639	-.021	-.211	.395
SP_SafetyAudit	-.147	.099	.028	.881
SP_InventoryAccuracy	.565	.212	-.004	.122
SP_Pilferage	-.068	.632	.282	.024
SP_FreightClaims	.303	-.083	.514	.120
SP_SafetyAccidents	.022	-.107	.045	.883
SP_OSD	.457	.214	.254	.083

All the four factors generated are interpretable. In fact, they are consistent with the concept of supply chain flows – information flow (information), physical flow (breaches), financial flow (cost) and people (safety). The Cronbach's Alphas for each of these factors are also higher than or at least very close to the recommended 0.70, which means that these scales are reliable (see Table 5.30).

Table 5.30: Cronbach's alpha values for SP factors.

Scale	Cronbach's Alpha	N of Items
Information	0.806	5
Physical Breaches	0.815	4
Cost	0.684	3
Safety	0.747	3

The Insights

In conclusion, the above analyses show that the KPIs for security performance (SP) are indeed a subset of traditional SCP from the industry practitioners' point of view. This means that organizations have all along been measuring an aspect of their operations that relates to

security. As such, organizations should not perceive the current change in intensity of interests in security as throwing them off-balance.

Specifically, security performance measurements can be classified into four key components:

- those measuring the accuracy and reliability of information
- those measuring the effectiveness of physical breaches prevention
- those measuring the cost of security initiatives
- those measuring the safety of operations and personnel

This means that when evaluating security performance, organizations should select key performance indicators (KPIs) that comprehensively represent each of the four areas of information, cargo, people and cost.

In addition, the information presented seems to indicate that industry practitioners feel that security performance has implications on not only one but many aspects of traditional SCP, especially in terms of timeliness, reliability, availability and efficiency.

To better identify and understand these relationships and those among security initiatives, security performance and traditional SCP, we employ the Structural Equation Modeling (SEM) technique and the analyses are discussed in the sections that follow.

5.5 Security Initiatives, SCP and Security Performance

As a first step to understanding the relationships between security initiatives and security performance, we take a look at the descriptive statistics of the data collected.

5.5.1 Perceptions of Security Initiatives and their Popularity

Supply chain security has been redefined as preventing terrorists from targeting the maritime supply chain or transporting a weapon in a shipping container. This change in focus raises questions about the effectiveness of proposed security efforts and the consequences they may have for supply chain performance (Willis and Ortiz, 2004). As a first step to understanding the

relationships among security initiatives, SCP and security performance, we take a look at the descriptive statistics of the data collected.

Perceived Impact of Security Initiatives on SCP

Respondents to the web/email survey were asked directly the degree of negative or positive impact they perceived a particular initiative has on various aspects of SCP. Respondents used a 7-point Likert scale where 1=Extremely Negative and 7=Extremely Positive. Figure 5.10 shows the mean value of the perceived impact of a particular initiative on the six different aspects of SCP. The data is sorted in descending magnitude of the mean value.

Figure 5.10: Respondents' perceived impact of security initiatives on SCP.[41]

Initiatives	Efficiency
Tracking & Monitoring	5.43
Business Partner Requirements	5.26
Management Support & Sponsorship	5.20
Physical Security & Access Control	5.17
Security Training and Outreach Programs	5.16
Advanced Data	5.05
Container Security	5.02
Procedural Security	5.00
Personnel Security	4.99
Security Certification	4.75
Overall Average	**5.10**

Initiatives	Time
Tracking & Monitoring	5.38
Business Partner Requirements	5.21
Physical Security & Access Control	5.09
Management Support & Sponsorship	5.08
Container Security	5.01
Security Training and Outreach Programs	4.98
Advanced Data	4.94
Procedural Security	4.83
Personnel Security	4.76
Security Certification	4.74
Overall Average	**5.00**

Initiatives	Availability
Tracking & Monitoring	5.18
Physical Security & Access Control	5.10
Management Support & Sponsorship	5.05
Business Partner Requirements	4.99
Personnel Security	4.98
Procedural Security	4.97
Security Training and Outreach Programs	4.96
Container Security	4.86
Advanced Data	4.86
Security Certification	4.69
Overall Average	**4.97**

Initiatives	Responsiveness
Tracking & Monitoring	5.47
Management Support & Sponsorship	5.36
Physical Security & Access Control	5.19
Security Training and Outreach Programs	5.16
Business Partner Requirements	5.11
Procedural Security	5.10
Advanced Data	5.09
Container Security	5.07
Personnel Security	4.98
Security Certification	4.68
Overall Average	**5.12**

Initiatives	Reliability
Tracking & Monitoring	5.48
Security Training and Outreach Programs	5.39
Physical Security & Access Control	5.34
Management Support & Sponsorship	5.34
Personnel Security	5.30
Business Partner Requirements	5.29
Procedural Security	5.24
Container Security	5.19
Advanced Data	5.14
Security Certification	5.04
Overall Average	**5.28**

Initiatives	Security
Tracking & Monitoring	5.92
Procedural Security	5.91
Management Support & Sponsorship	5.88
Personnel Security	5.79
Physical Security & Access Control	5.78
Security Training and Outreach Programs	5.75
Advanced Data	5.62
Security Certification	5.61
Container Security	5.43
Business Partner Requirements	5.37
Overall Average	**5.71**

Note: The standard deviations of these mean values range from 0.91 to 1.25.

[41] Paired t-tests are not performed on these means because the sample size of each selected pair is not consistent. This is because respondents are only required to indicate their perception on impact on supply chain performance if they have implemented that initiative or is planning to implement that initiative.

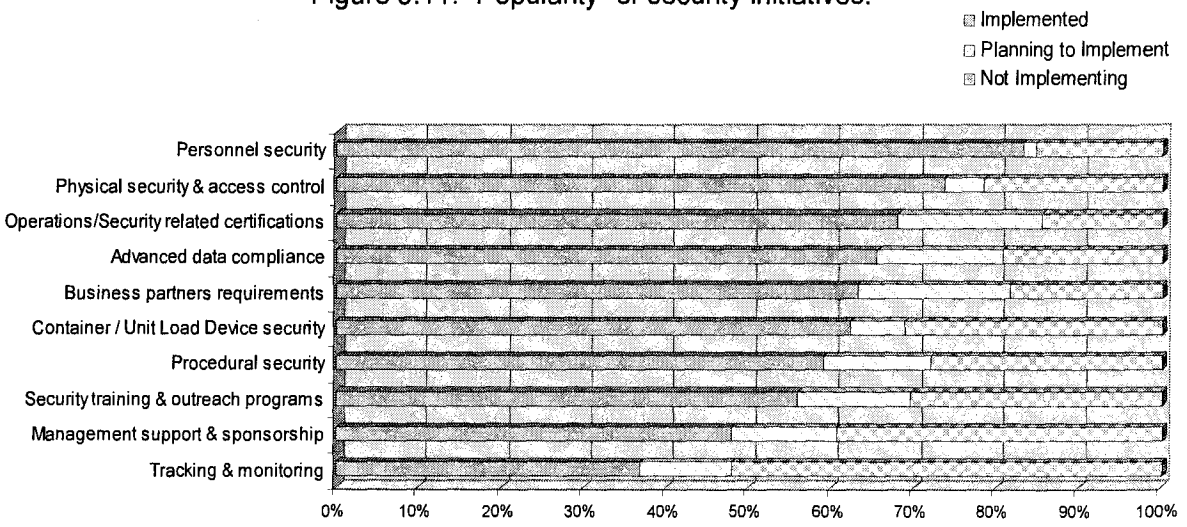
Although the differences in these mean values are not huge, it does reflect a general trend among these respondents that they perceive all of these initiatives as a whole to have a greater positive impact on security performance compared to other aspects of traditional SCP (see Figure 5.10 where the overall mean value for security is 5.71, which is 0.73 points higher than a mean of 4.97 for availability aspect of SCP and 5.00 for time aspect of SCP).

As can be seen from Table 5.10, security initiatives under the Tracking and Monitoring group are consistently ranked the best in terms of their perceived impact on traditional aspects of SCP. In addition, management support and sponsorship is ranked in the top three groups of initiatives with the most impact for three out of six aspects of SCP. This indicates that respondents also view security efforts as strategic endeavors where success in their implementation requires management support and sponsorship. Externally oriented initiatives such as instituting business partner requirements are also perceived to have a relatively greater impact on SCP's efficiency and time performance compared to other groups of initiatives.

Types of Security Initiatives Implemented

Respondents to the web/email survey were also asked to indicate which group of initiatives their organization has implemented or is planning to implement or has no intention to implement in the near future. Figure 5.11 shows the "popularity" of the ten groups of security initiatives among the respondents. Popularity of an initiative is determined by the number of respondents' whose organizations have implemented or planning to implement that initiative.

Figure 5.11: "Popularity" of security initiatives.



As seen from Figure 5.11, the groups of initiatives that most organizations have implemented or are planning to implement include personnel security, physical security and access control and obtaining security related certifications. The groups of initiatives that the least number of organizations have chosen to implement include tracking and monitoring of cargo conveyance and clear management support and sponsorship.

The Insights

It is especially interesting to note that although Tracking and Monitoring is the least implemented security initiative, it is perceived by respondents to be the one with the greatest positive impact on supply chain performance (see Figure 5.10).[42] Similarly, for some of the more widely implemented security initiatives such as Personnel Security, Security Related Certifications, Container Security and Advanced Data Compliance, respondents are either neutral or unsure of the positive impacts they have on SCP (See Figure 5.10).

This initial analysis suggests that the current motivations behind security initiatives implementation in the private sector are very much that of a pressure to comply with public sector regulations and/or simply the ease of implementation. This is consistent with current literature on security such as Willis and Ortiz (2004). Wolfe (2004), Langhoff et al. (2005), Rice and Spayd (2005), Peleg-Gillai et al. (2006). Organizations are not yet motivated by their perceptions to implement initiatives that they think will have positive impacts on traditional SCP. And to the extent that security is a consideration, it is focused on reducing cargo theft and protecting proprietary data from competition (Smart and Secure Tradelanes, 2003).

5.6 Structural Equation Modeling (SEM) Analysis

To understand the relationship between security initiatives, security performance and traditional SCP, SEM is employed. SEM provides a test of the overall model as opposed to performing a series of multiple regressions and takes into account the reliability of observed variables by representing each construct as a latent variable (as opposed to simple path analysis) (Savalei and Bentler, 2006). The relationships among these constructs constitute the structural part of the model. The measurement part of the model consists of the relationships between the latent variables and their indicators.

[42] 4 on the Likert scale = Neutral/Unsure. 5 on the Likert scale = Moderately Positive. 6 on the Likert scale = Very Positive.

There are three measurement models and one structural model in the model used for this study. The steps in a SEM modeling process will be described together with the results in the sections that follow.

5.6.1 Data Considerations

Sample Size Required

Although there are several recommendations for a minimum sample size of at least 200 or 5 or 10 times the number of variables or estimated parameters (Garver and Mentzer, 1999 and Savalei and Bentler, 2006), McQuitty (2004) notes that these recommendations may be outdated.

Hair et. al (1998) provides an argument that the absolute minimum sample size must be at least greater than the number of covariances or correlations in the input data matrix. The sample size used in this SEM model is 113 and there are 112 correlations in the input data matrix.

Moreover, according to Hair et. al (1998), using the Maximum Likelihood method, the generally accepted minimum sample size can be between 100 to 150. In fact, Hair et. al (1998) wrote that as the sample size becomes large, the Maximum Likelihood method can become "too sensitive" and almost any difference is detected, making all goodness-of-fit measures to indicate poor fit.

Therefore it is decided that it is appropriate to proceed with the SEM analysis.

Departures from Normality

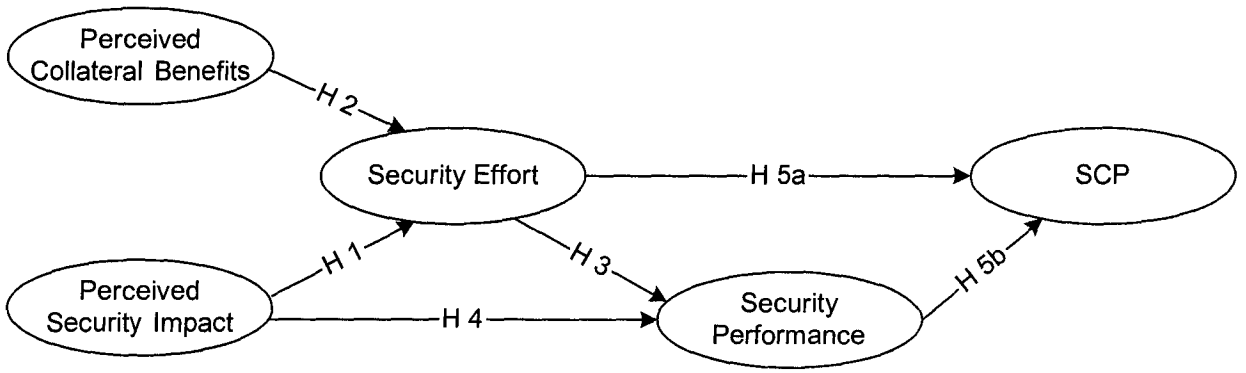
The skewness and kurtosis statistics for the variables used in the Supply Chain Security model are evaluated and the variables used are mostly non-normal. It is therefore necessary to employ appropriate model estimation techniques that compensates for the non-normality of the data used. Further discussion can be found in the model estimation section.

5.6.2 Model Specification

Figure 5.12 shows the Supply Chain Security model to be tested. Based on the extensive review of existing literature (see Chapter 2) and field interviews conducted (see Chapter 4 and

Appendix E), it is hypothesized that the amount of security effort undertaken by an organization is dependent on the amount of collateral benefits perceived from undertaking that security effort (H2) and the resulting impact on security itself (H1). An organization's security effort is expected to have an impact on the security performance of its business operations (H3 and H4). The changes and/or improvements made to an organization's business operations as a result of undertaking such security efforts are expected to have impact on the other traditional aspects of SCP such as efficiency, availability, responsiveness, reliability and timeliness (H5). This impact could be a direct result of security effort (H5a) or it could be an indirect result from an improvement in security (H5b) or it could be both.

Figure 5.12: Structural model for Supply Chain Security.



5.6.3 Model Estimation

The model estimation process is an iterative process and there are many techniques available depending on the computer program used. Although the Maximum Likelihood (ML) technique is by far the most widely used, this technique is sensitive to non-normal data.

There are some estimation procedures specifically designed to deal with non-normal data (Hair et al., 1998). Examples include Weighted Least Squares (WLS), Generalized Least Squares (GLS) and Asymptotically Distribution Free (ADF). The ADF technique has received particular attention due to its insensitivity to non-normality of the data but its primary drawback is the increased samples size required (Hair et al., 1998; Savalei and Bentler, 2003). As the WLS technique is not available in AMOS 7.0, the GLS estimation technique will be used to compensate the non-normality of the data used.

However, Savalei and Bentler (2006) conclude that despite the restrictive normality assumption, the ML parameter estimates are actually fairly robust to the violation of this assumption, and ML is the preferred method of estimation even if this assumption is violated.

The ML method is therefore also performed on the same model with the same data set. The ML and GLS results are compared on eleven aspects of model explanation and fit (see Table 5.31).

Table 5.31: Comparison of ML and GLS estimation techniques.

Model Explanation Statistics	**GLS**	**ML**
R^2 – SCP	0.557	0.500
Standardized Residuals*	7	0
Modification Indices**	1	2
Insignificant Parameters	16	13

Model Fit Statistics	**GLS**	**ML**
Chi-Square (χ^2) (p-value)	90.920 (0.338)	99.816 (0.146)
GFI	0.899	0.909
RMSEA	0.023	0.038
TLI/NNFI	0.943	0.988
CFI	0.959	0.991
IFI	0.968	0.992

* number of standardized residuals greater than 2.0[43].
** number of modification indices greater than 7.88[44].

Both techniques generated significant χ^2 values and other model fit statistics. Their explanation powers are also comparable with similar R^2 values for SCP at 0.500 for ML and 0.557 for GLS. Although GLS has a larger R^2 value, it has a significantly larger number of standardized residuals that are considered large; seven compared to none for ML. There are also a greater number of insignificant parameter estimates for GLS than ML. Taking all ten indices together, the ML technique is selected as the model estimation technique used in this study.

There are also several estimation processes available, ranging from direct estimation of the model, which is common in most multivariate techniques, to methods that generate thousands of model estimations from which the final model results are obtained such as bootstrapping and jackknife. Detailed discussions of these methods can be found in standard multivariate statistics

[43] Garver and Mentzer (1999) recommended that standardized residuals > 2.0 are considered large.

[44] Garver and Mentzer (1999) recommended that modification indices > 7.88 are considered large.

books such as Hair et al. (1998). Because the bootstrapping estimation process estimates the final parameters and their confidence estimates directly from multiple model estimations across separate samples, they do not rely on assumptions as to the statistical distribution of the parameters (Hair et al., 1998). Therefore the bootstrapping estimation process is employed in this study. The results in Table 5.31 were generated using bootstrapping estimation.

Next to determine whether the effects of security effort on SCP are direct or indirect, a comparison was conducted between a model that has H5a and a model that does not. The results are shown in Table 5.32. Path H5a was found to be statistically insignificant and its inclusion in the model reduces the R^2 value of SCP. The inclusion of path H5a also renders path H5b statistically insignificant. Since the elimination of path H5a did not affect the model fit indices significantly, the decision was made to exclude path H5a in the model.

Table 5.32: Comparison of model having path H5a and model not having H5a.

Model Explanation Statistics	**H5a**	**No H5a**
R^2 – SCP	0.500	0.530
Standardized Residuals*	0	0
Modification Indices**	2	2
Insignificant Parameters	13	11

Model Fit Statistics	**H5a**	**No H5a**
Chi-Square (χ^2) (p-value)	99.816 (0.146)	99.949 (0.162)
GFI	0.909	0.909
RMSEA	0.038	0.036
TLI/NNFI	0.988	0.989
CFI	0.991	0.992
IFI	0.992	0.992

* number of standardized residuals greater than 2.0[45].
** number of modification indices greater than 7.88[46].

5.6.4 Model Evaluation

The overall SEM model consists of two key components – the measurement model(s) and the structural equation model. There are usually one or more measurement models and the final model is the structural equation model. The measurement models specify how the latent

[45] Garver and Mentzer (1999) recommended that standardized residuals > 2.0 are considered large.

[46] Garver and Mentzer (1999) recommended that modification indices > 7.88 are considered large.

variables are measured in terms of the indicator variables as well as address the reliability and validity of the indicator variables in measuring the latent variables or hypothetical constructs (Wisner, 2003). The structural equation model provides an assessment of predictive validity, specifies the direct and indirect relations among the latent variables, and describes the amount of explained and unexplained variance in the model (Wisner, 2003).

5.6.4.1 Measurement Model Evaluation

The evaluation of the measurement models is performed in two key stages. The first stage evaluates each measurement model that makes up the structural model.

There are three measurement models in this model. One measurement model measures the Perceived Collateral Benefits (Figure 5.13), one other measures the SCP (Figure 5.14) and the last one measures the Security Effort (Figure 5.15).

Figure 5.13: Perceived Collateral Benefits measurement model.

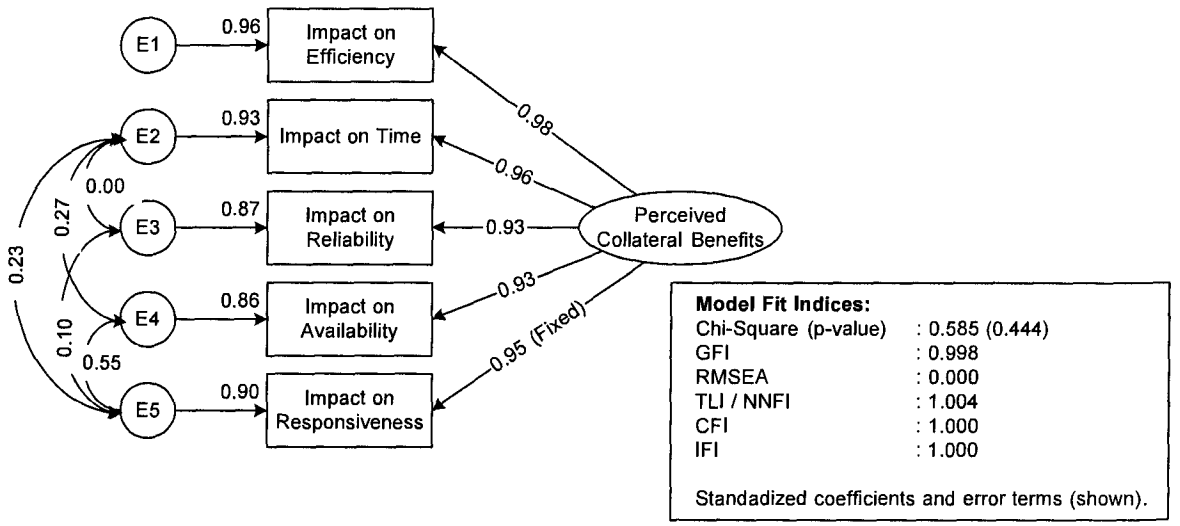


Figure 5.14: SCP measurement model.

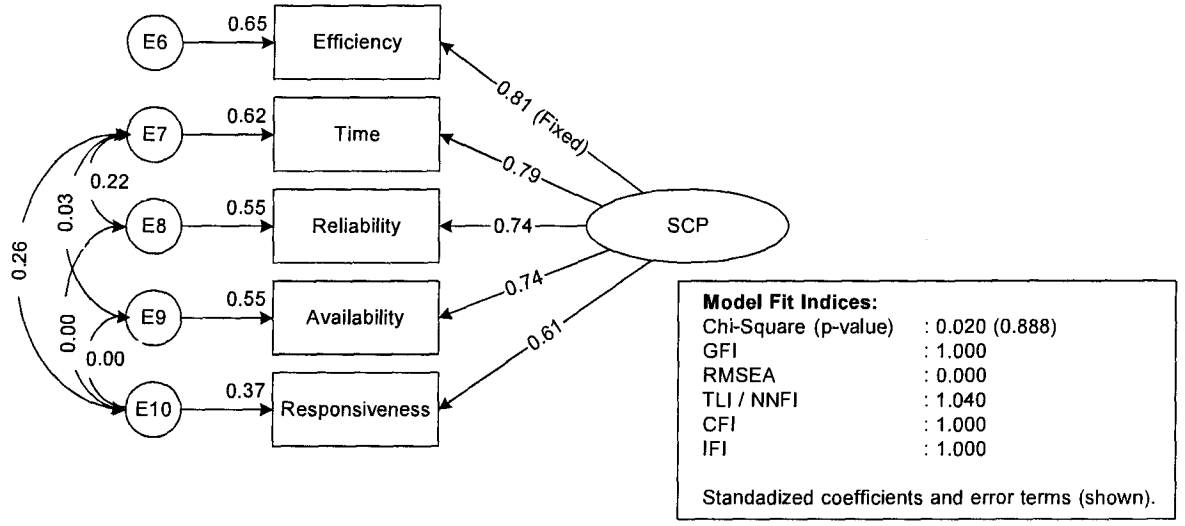
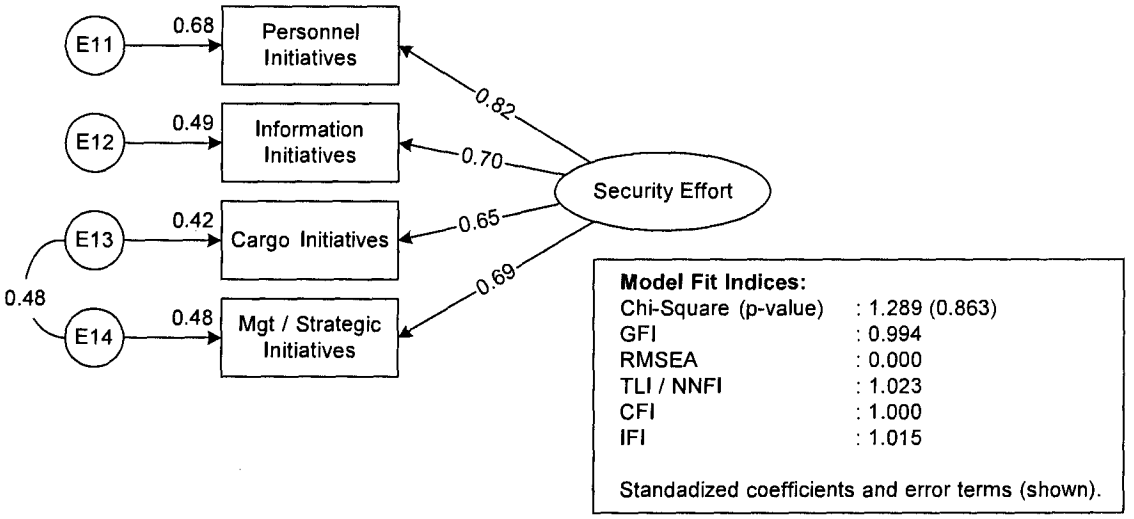


Figure 5.15: Security Effort measurement model.



Each measurement model is assessed for unidimensionality, reliability and validity. For a latent construct to possess construct validity, it must first be unidimensional and reliable (Garver and Mentzer, 1999).

Unidimensionality

Unidimensionality is an assumption underlying the calculation of reliability and is demonstrated when the indicators of a construct have acceptable fit on a single factor (one-dimensional)

model. An acceptable measurement of unidimensional constructs should reveal relatively small standardized residuals and modification indices. A large residual will be over 2.00 (Garver and Mentzer, 1999). A substantial modification index value is considered 7.88 (Garver and Mentzer, 1999). For all three measurement models, there are no standardized residual values larger than 2.00. The largest standardized residual values are 0.019, 0.031 and 0.366 for the Perceived Collateral Benefits, SCP and Security Effort model respectively. Similarly, there are no modification indices that are larger than 7.88. In fact, there are no modification indices for all three measurement models.

In addition, the direction/sign (+, -), magnitude and statistical significance of the parameter estimates between indicators and latent variables are inspected and evaluated. The directions of all the parameter estimates are consistent with theory and existing literature. All estimated parameters are also statistically significant at the 0.05 level of significance.

Next, Garver and Mentzer (1999) suggests that the magnitude of the standardized parameter estimates should be at least 0.70 to ensure construct unidimensionality. As can be seen from Figures 5.13, 5.14 and 5.15, all the standardized parameter estimates are greater than 0.70 except for three parameters: (1) Responsiveness for SCP, (2) Cargo Initiatives for Security Effort and (3) Management/Strategic Initiatives for Security Effort. Although less than 0.70, all these three parameters are marginally close enough to 0.70 to be accepted. Moreover, Savalei and Bentler (2006) suggested that a parameter value greater than 0.60 is a rather good estimate especially for exploratory studies such as this.

Reliability

Cronbach's alpha is still the most commonly used index of scale reliability and in general scales that receive alpha scores over 0.70 that are considered to be reliable. Table 5.33 shows the Cronbach's alpha values for each of the three latent constructs.

Table 5.33: Cronbach's alpha values for each measurement model.

Measurement Model	Cronbach's Alpha
Perceived Collateral Benefits	0.908
SCP	0.865
Security Effort	0.827

Although commonly used, Cronbach's alpha has three limitations (Garver and Mentzer, 1999). Firstly, Cronbach's alpha tends to underestimate scale reliability or become artificially inflated if there is a large number of items in the scale. Secondly, it does not measure consistency. Thirdly, it assumes that all items have equal reliabilities.

In order to overcome these limitations, Baumgarter and Homburg (1996) and Garver and Mentzer (1999) propose two additional SEM construct reliability measures:

Construct Reliability $= (\Sigma\lambda)^2 / [(\Sigma\lambda)^2 + \Sigma(1 - \lambda_j^2)]$

Variance Extracted $= \Sigma\lambda^2 / [\Sigma\lambda^2 + \Sigma(1 - \lambda_j^2)]$

Where:

λ is the standardized parameter estimate between a latent construct and each of its indicators.

$(1 - \lambda_j^2)$ is the measurement error for each indicator.

The construct reliability index does not assume that individual items have equal reliabilities and the acceptable reliability value is 0.70 or greater (Garver and Mentzer, 1999). Complementary to the Construct Reliability, the Variance Extracted measure measures the total amount of variance in the indicators accounted for by the latent variable (Garver and Mentzer, 1999). An acceptable reliability value for variance extraction is 0.50 or greater.

The construct reliability and variance extracted measures are calculated for all three measurement models and all of them have construct validity values greater than 0.80 and variance extracted values greater than 0.50 (see Table 5.34).

Table 5.34: SEM construct reliability measures for each measurement model.

Measurement Model	**Construct Validity**	**Variance Extracted**
Perceived Collateral Benefits	0.981	0.914
SCP	0.868	0.636
Security Effort	0.808	0.596

Validity

There are three key aspects of validity: convergent, discriminant and predictive.

Convergent Validity:

Convergent validity is tested by determining whether the items in a scale converge or load together on a single construct in the measurement model. A reasonable benchmark value of substantial magnitude of the parameter estimate indicating convergent validity is 0.70. As mentioned above, majority of the standardized parameter estimates (i.e. loadings) in the measurement models are greater than 0.70. For those parameter estimates that are not, they are at least greater than 0.60. As mentioned earlier, Savalei and Bentler (2006) concluded loading values greater than 0.60 as good loadings. This therefore also implies convergent validity in the three constructs (Dunn et al., 1994). Moreover, Table 5.35 shows that the correlations values among observed variables measuring the same latent construct are significantly higher than the correlation values with other observed variables measuring another latent construct. These results provide clear support for convergent validity for all the measurement models.

Table 5.35: Observed variables item-to-item correlation matrix.

	Impact on Efficiency	Impact on Availability	Impact on Responsiveness	Impact on Time	Impact on Reliability	Responsiveness	Availability	Reliability	Time	Efficiency	Mgt/Strategic Initiatives	Cargo Initiatives	Personnel Initiatives	Information Initiatives
Impact on Efficiency	1													
Impact on Availability	0.909	1												
Impact on Responsiveness	0.929	0.945	1											
Impact on Time	0.941	0.92	0.933	1										
Impact on Reliability	0.914	0.86	0.896	0.902	1									
Responsiveness	0.212	0.195	0.214	0.198	0.22	1								
Availability	0.27	0.248	0.273	0.252	0.279	0.443	1							
Reliability	0.282	0.26	0.285	0.264	0.292	0.447	0.547	1						
Time	0.296	0.273	0.299	0.277	0.307	0.603	0.593	0.675	1					
Efficiency	0.301	0.277	0.304	0.281	0.312	0.459	0.584	0.61	0.641	1				
Mgt/Strategic Initiatives	0.321	0.297	0.322	0.302	0.328	0.195	0.248	0.259	0.272	0.277	1			
Cargo Initiatives	0.301	0.278	0.301	0.283	0.307	0.183	0.232	0.243	0.255	0.259	0.71	1		
Personnel Initiatives	0.375	0.347	0.376	0.353	0.383	0.228	0.29	0.303	0.318	0.323	0.564	0.529	1	
Information Initiatives	0.325	0.301	0.326	0.306	0.332	0.198	0.251	0.263	0.276	0.28	0.489	0.458	0.572	1

Discriminant Validity:

Discriminant validity verifies that scales developed to measure different constructs are indeed measuring different constructs. In contrast to convergent validity, discriminant validity is the

extent to which the items representing a latent construct discriminate that construct from the other items representing other constructs (Garver and Mentzer, 1999). Table 5.36 shows the correlations between each observable variable and each latent construct. It can be seen that the highest correlation value each observable variable has with a latent construct is with the latent construct that it is suppose to be measuring. This provides clear support for discriminant validity.

Table 5.36: Variables (Items) to latent constructs correlation matrix.

	Perceived Collateral Benefits	Security Effort	SCP
Impact on Efficiency	0.983	0.462	0.373
Impact on Availability	0.925	0.427	0.344
Impact on Responsibility	0.946	0.463	0.377
Impact on Time	0.957	0.434	0.349
Impact on Reliability	0.93	0.472	0.386
Mgt/Strategic Initiatives	0.34	0.695	0.343
Cargo Initiatives	0.319	0.651	0.321
Personnel Initiatives	0.398	0.812	0.401
Information Initiatives	0.345	0.704	0.347
Responsiveness	0.227	0.281	0.569
Availability	0.288	0.357	0.723
Reliability	0.302	0.373	0.756
Time	0.316	0.392	0.794
Efficiency	0.322	0.398	0.807

Predictive Validity:

Predictive validity estimates whether or not the construct of interest predicts or covaries with constructs that it is supposed to predict or covary. This can be assessed by correlating constructs to other constructs that they should predict. The correlations between these two constructs should be substantial in magnitude and statistically significant (Garver and Mentzer, 1999). The correlations between the following pairs of latent constructs were performed and they are all statistically significant at the 0.05 level (see Table 5.37). This shows that the measurement models all satisfy the predictive validity requirement.

Table 5.37: Correlations between measurement models.

Measurement Model Pairs	Correlation	Significance
Perceived Collateral Benefits – Security Effort	0.477	< 0.001
Perceived Collateral Benefits – SCP	0.249	0.023
Security Effort – SCP	0.508	< 0.001

Model Fit

The individual measurement models are lastly evaluated for their model fit indices. There are three types of goodness-of-fit measures: (1) absolute fit measures which assess only the overall model fit (both structural and measurement models collectively) without adjustment for the degree of "overfitting" that might occur, (2) incremental fit measures which compare the proposed model to another model specified by the researcher, or (3) parsimonious fit measures which "adjust" the measures of fit to provide a comparison between models with differing numbers of estimated coefficients.

Assessing the goodness-of-fit of a model is more a relative process than one with absolute criteria. Multiple fit indices should be examined and reported when evaluating practical fit of a model (Savalei and Bentler, 2006). Garver and Mentzer (1999) recommended using the (1) Tucker-Lewis index or Non-normed fit index (TLI or NNFI), (2) the comparative fit index (CFI) and (3) the root mean squared approximation of error (RMSEA). These indices are all scaled to a pre-set continuum (0 to 1) for easy interpretation and are all relatively independent of sample size effects. Wisner (2003) used the (1) χ^2 statistic, (2) Goodness-of-fit Index (GFI), (3) Normed fit index (NFI), (4) CFI, (5) Incremental fit index (IFI) and (6) Hoelter's N (CN). Savalei and Bentler (2006) recommends the use of CFI and RMSEA.

However, Arbuckle and Wothke (1998) are not convinced by Hoelter's arguments in favor of the 200 cutoff for Hoelter's N. And Savalei and Bentler (2006) highlighted the NFI's dependence on sample size and the fact that NFI tends to be too small for models based on fewer observations. Therefore, in evaluating the model fit for each of the measurement models in the Supply Chain Security structural model, the six model fit statistics shown in Table 5.38 are used.

Table 5.38: Supply Chain Security measurement models fit evaluation.

			Measurement Models		
Type	**Indices**	**Acceptable Level**	**Perceived Collateral Benefits**	**SCP**	**Security Effort**
Absolute fit	RMSEA	< 0.08 (preferably < 0.05)	0.000	0.000	0.000
	χ^2 (p-value)	Small χ^2 Large p-values (> 0.2)	0.585 (0.444)	0.020 (0.888)	1.289 (0.863)
	GFI	> 0.90	0.998	1.000	0.994
Incremental fit	TLI / NNFI	> 0.90	1.004	1.040	1.023
	CFI	> 0.90	1.000	1.000	1.000
	IFI	> 0.90	1.000	1.000	1.015

Chi-Square (χ^2):

It is important to note that although the χ^2 statistic is the most common method of evaluating fit, this fit index is highly sensitive to sample size and significance tests can be misleading (Garver and Mentzer, 1999; Arbuckle and Wothke, 1995). Hair et al. (1998) recommends that the use of χ^2 statistic is appropriate for sample sizes between 100 and 200 and that a minimum value of 0.1 or 0.2 for the significance level should be exceeded before non-significance is confirmed. The sample size for this study is 111 and the p-values for all the χ^2 statistics for all three measurement models are greater than 0.20. The use of χ^2 statistic is therefore appropriate.

The χ^2 statistics for all three measurement models have corresponding p-values greater than 0.05, indicating good fit. They are also greater than the 0.2 level recommended by Hair et al. (1998).

GFI:

This index represents the overall degree of fit but does not adjust for the degrees of freedom. The higher the value of GFI, the better the fit and Wisner (2003) recommends a greater than 0.90 GFI value as acceptable. The GFI for all three measurement models are greater than 0.90, indicating good fits.

RMSEA:

This index measures the discrepancy between observed and estimated input matrices per degree of freedom. The value is representative of the goodness-of-fit that could be expected if the model were estimated in the population. A value of the RMSEA of about 0.05 or less would indicate a close fit of the model in relation to the degrees of freedom (Arbuckle and Wothe, 1995). The RMSEA values for all three measurement models are less than 0.05, indicating very good fits.

TLI (NNFI):

This index combines a measure of parsimony into a comparative index between the proposed and null models, resulting in typical values ranging from 0 to 1.0 but it is not limited to this range. A value greater than 0.90 and close to 1.0 indicates a very good fit (Arbuckle and Wothe, 1995). The TLI values for all three measurement models are greater than 0.90 and close to 1.0, indicating very good fits.

CFI and IFI:

Both the CFI and IFI indices represent comparison between the estimated model and a null or independence model. The values lie between 0 and 1.0 with larger values indicating higher levels of goodness-of-fit. Values close to 1.0 indicate very good fit. The CFI has been found to be more appropriate in a model development strategy or when a smaller sample is available. The CFI values for all three measurement models are greater than 0.90, indicating very good fits. And the IFI values for all three measurement models are greater than 0.90, also indicating very good fits.

In summary, all six model fit indices achieve their recommended thresholds or benchmarks thus indicating good if not very good fits of the data to all the three proposed measurement models.

5.6.4.2 Structural Model Evaluation

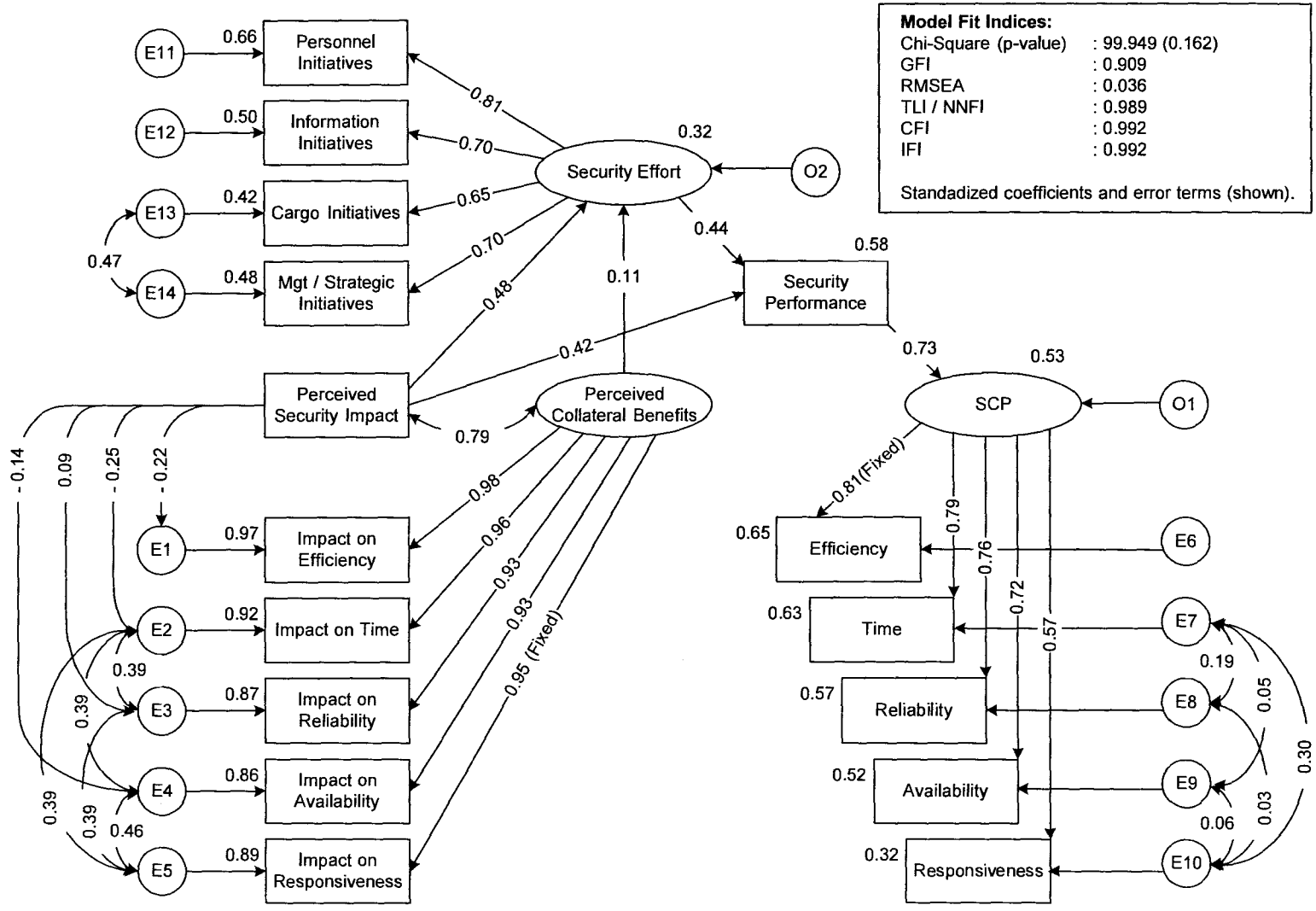
The structural model for supply chain security is now put together, and the parameters estimated and assessed for goodness-of-fit (see Figure 5.16).

The first step in evaluating the results of the Supply Chain Security model is an initial inspection for "offending estimates". Once the model is established as providing acceptable estimates, the standardized residuals and modification indices can be evaluated and thereafter the indices for goodness-of-fit must then be assessed. Offending estimates refer to (1) negative error variances or non-significant error variances for any construct, (2) standardized coefficients exceeding 1.0 or (3) very large standard errors associated with any estimated coefficient.

Standardized Coefficients

The AMOS output for Supply Chain Security model contains no negative error variances or non-significant error variances for any construct. There are also no standardized coefficients larger than 1.0. All standard errors are also small with the largest value being only 0.198.

Figure 5.16: Supply Chain Security SEM model.



Note: E's and O's are "error" variables that represent factors that affect the variable that it is pointing to, that are not captured in the survey.

Table 5.39: Standardized residuals matrix for Supply Chain Security model.

	Security_Impact	SCP_Resp	Security_Perf	Eff_Impact	Available_Impact	Resp_Impact	Time_Impact	SCP_Available	SCP_Reliable	SCP_Time	SCP_Eff	Mgt/Strat_Init	Cargo_Init	Personnel_Init	Info_Init	Reliable_Impact
Security_Impact	-0.003															
SCP_Resp	-0.571	0														
Security_Perf	0.089	-1.021	0													
Eff_Impact	0.002	-1.713	0.285	0												
Available_Impact	-0.001	-0.872	0.357	-0.001	0.001											
Resp_Impact	-0.004	-0.931	-0.011	0	0	0										
Time_Impact	-0.001	-1.297	0.23	0	0	0.001	0									
SCP_Available	-0.443	0	-0.039	-0.923	-0.762	-1.211	-1.296	0								
SCP_Reliable	0.4	0.001	0.133	-0.123	0.22	-0.011	-0.203	0.017	0							
SCP_Time	-0.025	0	-0.116	-1.569	-1.043	-1.117	-1.569	0.003	0	0						
SCP_Eff	-0.051	0.322	0.179	-1.082	-1.03	-0.921	-1.541	0.113	-0.145	-0.049	0					
Mgt/Strat_Init	-0.315	-1.837	0.26	0.089	0.568	0.343	0.457	-0.56	-0.062	0.657	0.501	-0.309				
Cargo_Init	0.339	0.116	-0.167	0.713	1.337	1.085	1.289	-0.362	0.135	0.657	0.192	-0.045	0.198			
Personnel_Init	-0.225	-0.844	-0.189	-0.097	0.548	0.193	-0.064	-0.739	-0.239	-0.205	-0.741	-0.494	0.061	-0.259		
Info_Init	0.451	0.872	-0.213	-0.321	0.262	0	-0.279	0.696	1.691	1.495	0.737	0.055	0.355	0.332	0.504	
Reliable_Impact	-0.003	-1.428	0.169	0.002	-0.003	-0.002	-0.001	-1.271	0.593	-0.994	-1.088	-0.111	0.787	-0.708	-0.421	0

Table 5.40: Modification indices for Supply Chain Security model.

Covariances: (Security Model - Default model)

			M.I.	Par Change
E10	<-->	E14	13.379	-0.141
E13	<-->	E10	4.675	0.075
E12	<-->	O1	4.258	0.07
E3	<-->	E8	6.975	0.06

Variances: (Security Model - Default model)

	M.I.	Par Change

Regression Weights: (Security Model - Default model)

			M.I.	Par Change
SCP_Responsiveness	<---	E14	9.795	-0.349
SCP_Responsiveness	<---	Support_Initiatives_I	7.465	-0.164
SCP_Reliability	<---	Avg_Reliable_Impact	4.658	0.152
SCP_Time	<---	E14	4.323	0.207
SCP_Time	<---	Support_Initiatives_I	4.009	0.107
Support_Initiatives_I	<---	SCP_Responsiveness	7.46	-0.21
Info_Initiatives_I	<---	SCP_Responsiveness	4.036	0.121
Info_Initiatives_I	<---	SCP_Reliability	5.2	0.116

Standardized Residuals

The standardized residuals are examined next. From the standardized residuals matrix (see Table 5.39), it can be seen that half of the residuals are negative and half are positive, indicating a good degree of randomness. The majority of their values are also small with the largest standardized residual value being 1.691 which is lower than the cutoff of 2.00 recommended by Garver and Mentzer (1999) and makes this model acceptable in terms of explaining the covariances and correlations among the variables very well.

Modification Indices

The modification indices are examined next (see Table 5.40). They are helpful in determining whether and how a model can or should be modified because they point specifically to paths whose addition to the model would result in the biggest improvement in the overall χ^2 value. Table 5.40 shows that there are two modification indices that are greater than the recommended cutoff level of 7.88 suggested by Garver and Mentzer (1999). These modification indices suggest that the corresponding pairs of variables should be allowed to correlate.

The first value is 13.379, between the error term for responsiveness performance (E10) and the error term for management/strategic initiatives (E14). Theoretically, the factors that affect an organization's motivation to implement support type initiatives such as the amount of upstream and downstream control (i.e. how integrated) it has, the nature of its operating environment and business partners can be expected to be the same as those that affect the organization's performance in terms of responsiveness. Therefore E10 and E14 should correlate. But when these two variables are allowed to correlate, their covariance value is negative, which does not make theoretical sense. As such, this modification to the model is not made.

The second value is 9.795, between responsiveness performance and the error term for management/strategic initiatives (E14). E14 represents those factors that affect an organization's adoption of management/strategic initiatives. These factors can include the management's attitude towards security, general trends in its industry and extent of government regulations. These factors cannot be directly related to an organization's responsiveness performance because an organization can and would have appropriate strategies in place to ensure that they are able to respond to customers' deliveries and requirements effectively and efficiently given these operation constraints/challenges and hence, this modification to the model is also not made.

Goodness-of-fit Indices

Next, we assess the overall goodness-of-fit for the Supply Chain Security model. The goodness-of-fit indices used are the same as those used for evaluating the goodness-of-fit of the measurement models (see Table 5.41).

Table 5.41: Supply Chain Security model fit evaluation.

Type	Indices	Acceptable Level / Cutoff	Security Model Values
Absolute fit	RMSEA	< 0.08 (preferably < 0.05)	0.036
	χ^2 (p-value)	Small χ^2 Large p-values (> 0.2)	99.949 (0.162)
	GFI	> 0.90	0.909
Incremental fit	TLI / NNFI	> 0.90	0.989
	CFI	> 0.90	0.992
	IFI	> 0.90	0.992

The absolute fit indices all indicate good fit for the Supply Chain Security model. The RMSEA is 0.036, indicating good fit as it is smaller than 0.05. The p-value for χ^2 is 0.162, larger than the significance level of 0.05. This means that the departure of the data from the model is insignificant at the 0.05 α level, indicating good fit. The GFI is 0.909, greater than the acceptable level of 0.90, indicating good fit.

The incremental fit indices also indicate good fit for the Supply Chain Security model. The values for all the three indices – TLI/NNFI, CFI and IFI, are greater than the acceptable level of 0.90, at 0.989, 0.992 and 0.992 respectively, indicating very good fit.

Structural Model Statistical Power

Statistical power is defined as the probability of correctly rejecting the null hypothesis when it is false and this can be affected by factors such as the significance criterion (α), sample size, number of groups or levels, effect size and number of dependent variables (McQuitty, 2004).

McQuitty (2004) notes that if one is concerned about the validity of measures contained in structural equation models and the interpretation of model fit, then one should evaluate the associated statistical power in order to place fit indices in an appropriate context.

Using the method proposed by MacCallum et al. (1996) for estimating the power associated with the test of an entire structural equation model with known sample size (N) and degrees of

freedom (*df*), McQuitty (2004) provides a table of the minimum sample size required to achieve a desired level of power for a range of *df*. The statistical power for the Supply Chain Security Model is assessed using the McQuitty (2004) table (Table 5.42).

Table 5.42: Minimum sample size required to achieve specified power (test of close fit).

df	Power = 0.60, N ≥	Power = 0.70, N ≥	Power = 0.80, N ≥	Power = 0.90, N ≥
5	885	1132	1463	1994
10	486	613	782	1050
15	350	436	550	732
20	280	346	435	572
30	207	254	314	410
40	168	205	252	325
50	145	175	214	274
75	111	133	168	204
100	92	110	132	165
125	80	95	114	142
150	72	85	101	125
200	61	71	84	104
250	53	62	74	90
300	48	56	66	81
400	41	48	56	68

Source: McQuitty (2004).

The N and *df* values for the Supply Chain Security model are 113 and 87 respectively. From Table 5.42, the power of the Supply Chain Security model is approximately 0.70. This is a desirable level of statistical power. And we can reasonably and safely conclude that the Supply Chain Security model is adequate in shining light on the concepts it seeks to explain.

5.6.5 Interpreting Parameters

Now that we have a model that fits the data well, we proceed to assess the statistical significance of the parameter estimates and interpret them. Table 5.43 shows the standardized estimates for the final parameters in the Supply Chain Security model. Significant estimates are marked "***" beside their respective p-values.

Table 5.43: Parameter estimates for Supply Chain Security model.

Standardized Regression Weights: (Security Model - Default model)

			Estimate	S.E.	C.R.	P
Security Effort	<---	Avg_Security_Impact	0.478	0.080	3.162	0.002***
Security Effort	<---	Perceived_Collateral Benefits	0.112	0.083	0.734	0.463
Performance in_Security	<---	Avg_Security_Impact	0.419	0.097	2.789	0.005***
Performance in_Security	<---	Security Effort	0.440	0.196	2.744	0.006***
SCP	<---	Performance in_Security	0.728	0.198	4.162	***
Info_Initiatives_I	<---	Security Effort	0.704			
Personnel_Initiatives_I	<---	Security Effort	0.812			
Cargo_Initiatives_I	<---	Security Effort	0.651			
Support_Initiatives_I	<---	Security Effort	0.695			
Personnel_Initiatives_I	<---	E11	0.584			
Support_Initiatives_I	<---	E14	0.719			
Avg_Time_Impact	<---	Perceived_Collateral Benefits	0.957	0.039	26.967	***
Avg_Reliable_Impact	<---	Perceived_Collateral Benefits	0.930	0.045	21.328	***
Avg_Available_Impact	<---	Perceived_Collateral Benefits	0.925	0.034	29.199	***
Avg_Resp_Impact	<---	Perceived_Collateral Benefits	0.946			
Avg_Eff_Impact	<---	Perceived_Collateral Benefits	0.983	0.044	24.381	***
SCP_Reliability	<---	SCP	0.756	0.156	7.235	***
SCP_Availability	<---	SCP	0.723	0.129	7.274	***
SCP_Time	<---	SCP	0.794	0.161	7.214	***
SCP_Efficiency	<---	SCP	0.807			
SCP_Responsiveness	<---	SCP	0.569	0.136	5.266	***

Correlations: (Security Model - Default model)

			Estimate	S.E.	C.R.	P
Avg_Security_Impact	<-->	Perceived_Collateral Benefits	0.791	0.111	6.342	***
E13	<-->	E14	0.472	0.049	3.65	***
E3	<-->	Avg_Security_Impact	0.093	0.027	1.169	0.242
E4	<-->	Avg_Security_Impact	-0.144	0.021	-2.503	0.012***
E7	<-->	E8	0.187	0.071	1.105	0.269
E7	<-->	E10	0.304	0.068	1.99	0.047***
E9	<-->	E10	0.057	0.056	0.456	0.648
E8	<-->	E10	0.031	0.064	0.24	0.810
E5	<-->	E4	0.567	0.019	3.602	***
E2	<-->	Avg_Security_Impact	-0.247	0.024	-2.907	0.004***
E3	<-->	E5	0.133	0.012	1.228	0.219
E2	<-->	E4	0.312	0.018	1.896	0.058
E2	<-->	E5	0.295	0.018	1.533	0.125
E3	<-->	E2	0.112	0.015	0.76	0.448
E7	<-->	E9	0.046	0.055	0.331	0.741
E1	<-->	Avg_Security_Impact	-0.219	0.025	-1.536	0.124

All parameter estimates are significant except:

1. Security Effort ← Perceived Collateral Benefits
2. E3 ←→ Average Security Impact
3. E7 ←→ E8
4. E9 ←→ E10
5. E8 ←→ E10
6. E3 ←→ E5

7. E2 ←→ E4
8. E2 ←→ E5
9. E3 ←→ E2
10. E7 ←→ E9
11. E1 ←→ Average Security Impact

When a non-significant path exists in an otherwise well fitting model, we ask whether the model would fit the data equally well or about as well if we were to omit this path entirely. We can answer this question by means of a χ^2 difference test (Table 5.44).

Table 5.44: Goodness-of-fit indices for χ^2 difference tests.

Path Eliminated	RMSEA	χ^2 (p-value)	GFI	TLI / NNFI	CFI	IFI	R^2 – SCP
Original	0.036	99.949 (0.162)	0.909	0.989	0.992	0.992	0.530
Security Effort ← Collateral Benefits	0.036	100.489 (0.171)	0.909	0.989	0.992	0.992	0.533
E3 ←→ Average Security Impact	0.037	101.333 (0.157)	0.908	0.989	0.992	0.992	0.530
E7 ←→ E8	0.037	101.184 (0.159)	0.907	0.989	0.992	0.992	0.514
E9 ←→ E10	0.035	100.159 (0.177)	0.908	0.990	0.992	0.993	0.521
E8 ←→ E10	0.035	100.007 (0.180)	0.908	0.990	0.993	0.993	0.526
E3 ←→ E5	0.037	101.479 (0.154)	0.907	0.989	0.992	0.992	0.530
E2 ←→ E4	0.040	103.675 (0.122)	0.905	0.987	0.990	0.990	0.529
E2 ←→ E5	0.038	102.256 (0.142)	0.906	0.988	0.991	0.991	0.530
E3 ←→ E2	0.036	100.528 (0.170)	0.908	0.989	0.992	0.992	0.530
E7 ←→ E9	0.035	100.059 (0.179)	0.909	0.990	0.992	0.993	0.525
E1 ←→ Average Security Impact	0.038	102.409 (0.140)	0.906	0.988	0.991	0.991	0.530

Table 5.44 shows that the elimination of each of the non-significant paths does not alter the goodness-of-fit of the model by much. The χ^2 differences range between 0.11 and 3.726 with 1 degree of freedom. The path that yields the largest χ^2 difference is E2 ←→ E4. E2 is the error term for average time impact and E4 is the error term for the average availability impact. The resulting modified model still fits the data well but we note that the squared multiple correlation value (R^2) has decreased very slightly from 0.530 to 0.529. However, as there is strong

theoretical and logical support for this relationship between the unaccounted factors that affects the perceived impact on time and the perceived impact on availability performance, this path is retained in the final model.

The rest of the non-significant paths yielded relatively smaller χ^2 differences. Although the elimination of these paths does not significantly alter the model's goodness-of-fits, their corresponding R^2 values either remain the same or decreased. However, this is with the exception of the path - Security Effort ← Perceived Collateral Benefits. The R^2 value has increased very slightly from 0.530 to 0.533. However, as there is strong theoretical support for the relationship between perceived collateral benefits and security effort (i.e. the extent of adoption of security initiatives), this path is also retained in the final model.

Note also that Garver and Mentzer (1999) pointed out that the χ^2 test is highly sensitive to sample size and significance testing can be misleading. As such, even though these parameters or paths are not statistically significant, they are retained in the model because their directions (i.e. sign) and magnitudes demonstrate some of the interesting existing hypotheses around supply chain security. A bigger sample size might be able to detect this relationship (Savalei and Bentler, 2006).

5.6.6 Analysis of Structural Model

The sections that follow will discuss the findings from the SEM model results. However, first and foremost, it is important to highlight the concept of nonidentifiability and how it has been addressed in the SEM model.

It is essential to note that the Std Errors, Critical Ratios and P-Values are blank for those regression weights that are pre-specified with a value (typically "1") to fix the problem of model nonidentifiablility (Arbuckle and Wothke, 1995), Model nonidentifiability refers to the situation where the number of parameters to be estimated exceeds the number of distinct sample moments (i.e. negative degrees of freedom). To illustrate with an example, there is simply not enough information to determine both the price of each button and the number purchased by only knowing that one bought $10 worth of buttons.

According to Arbuckle and Wothke (1995), any one single-headed arrow leading away from each unobserved variable can be chosen and its regression weight fixed to "1". The regression weights that are fixed at "1" are:

- Impact on Responsiveness ← Perceived Collateral Benefits (for the unobserved variable "Perceived Collateral Benefits)
- SCP_Efficiency ← SCP (for the unobserved variable "SCP")

In addition, specifically for the measurement model Security Effort, there is a need to compensate for the assumption that the four groups of initiatives predicting Security Effort are parallel with same-sized common variance components and equal-sized error variances. This is because the number of groups of initiatives included under each of the four headings is different. "Info Initiatives" and "Cargo Initiatives" each consists of two of the ten groups whereas "Personnel Initiatives" and "Mgt/Strategic Initiatives" each consists of three of the ten groups. As such the regression weights for all four observed variables that predict Security Effort are specified. Since "Personnel Initiatives" and "Mgt/Strategic Initiatives" have 50% more items in their group than the other two, the weight for regressing these observed variables on the unobserved variable Security Effort is 1.5 times the weight for regressing "Info Initiatives" and "Cargo Initiatives" on Security Effort. Similarly, given equal variances for each of these observed variables, the (fixed) regression weight for the error terms for "Personnel Initiatives" and "Mgt/Strategic Initiatives" is $\sqrt{1.5} = 1.22$ times as large as the (fixed) regression weights for the error terms for "Info Initiatives" and "Cargo Initiatives".

Since these regression weights are pre-specified, AMOS does not calculate their corresponding Std Errors, Critical Ratios and P-Values.

Security Effort

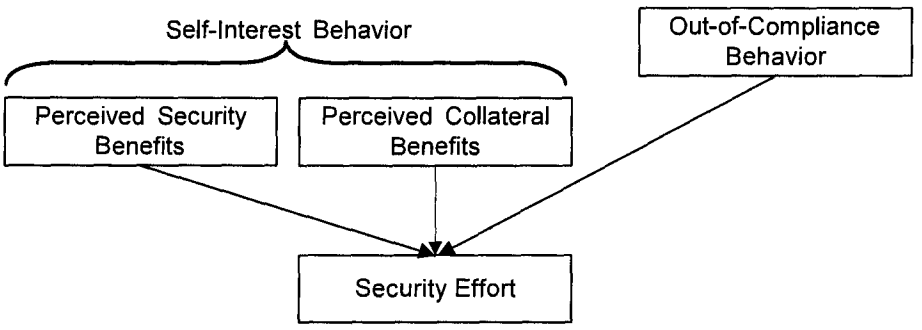
The statistical relationship between perceived security impact and security effort is significant with a standardized parameter estimate of 0.478 (see Table 5.41). This statistically significant relationship (p-value < 0.001) supports the hypothesis (H1) that an organization will undertake a security effort that is perceived to have a positive impact on the security performance of its supply chain operations.

The statistical relationship between perceived collateral benefits and security effort is however not significant with a standardized parameter estimate of 0.112 (see Table 5.41). Although this statistical relationship is not significant (p-value > 0.05) in this model, the positive sign between the two latent constructs supports the common viewpoint that the more collateral benefits a security investment is perceived to bring, the more motivated an organization will be to undertake the security investment.

Next, it is interesting to note the large difference in the magnitudes of these two standardized parameter estimates. The parameter value between perceived collateral benefits and security effort is 0.366 (i.e. ~ 77%) smaller than the parameter value between perceived security impact and security effort. This illustrates that currently, organizations place more emphasis on the actual resulting security performance improvements rather than traditional SCP improvements when deciding whether or not to undertake security improvement initiatives. Both the perceived security impact and perceived collateral benefits speaks to an organization's self-interest behavior.

However, recall from Figures 5.10 and 5.11 that there is also a strong indication of an out-of-compliance behavior from the private sector. This means that the private sector is undertaking security efforts as a result of the need to comply with public regulations rather than self-interests. These findings are consistent with that from the field interviews where interviewees indicated that they see their current efforts in security improvements as a result of complying with regulations and trade movement requirements such as C-TPAT and FAST. Figure 5.17 illustrates the structure of these motivators for security efforts.

Figure 5.17: The motivators of security efforts.



Security Effort and Security Performance

The statistical relationship between security effort and security performance is also significant with a standardized parameter estimate value of 0.440 (see Table 5.41). This significant statistical relationship (p-value < 0.05) answers the third research question of interest and also supports the hypothesis (H3) that undertaking security efforts will improve security performance.

This result reflects that despite a lack of objective KPIs for security performance, responding organizations are confident that whatever they are doing towards improving security performance are indeed doing what they are supposed to. This is consistent with the findings from the field interviews and this observation could be due to a simply logical expectation of a positive outcome from security effort since security performance is a paradoxical concept where an improved outcome can only be measured when something bad happens.

To understand specifically how each type of initiative affects security performance between respondent types, each initiative is cross-tabulated against the self-rated performance in security. The results show statistically significant positive relationships between seven of the ten groups of security initiatives and security performance (see Table 5.45). Significance is determined using the Pearson χ^2 statistic where a p-value smaller than 0.05 is considered significant. Detailed results of the cross-tabulation analyses can be found in Appendix G.

Table 5.45: Cross-tabulation results for security initiatives and security performance.

Security Initiatives	P-Value		
	Entire Sample	Shipper	Service Provider
Security/Operations related certifications	0.005***	0.027***	0.055***
Business Partner Requirements	0.020***	0.028***	0.448
Container/Trailer/ULD Security	0.061	0.086	0.322
Advanced Data	0.000***	0.007***	0.002***
Physical Security and Access Control	0.002***	0.028***	0.027***
Procedural Security	0.129	0.108	0.858
Tracking and Monitoring	0.109	0.125	0.536
Security Training	0.049***	0.093	0.172
Personnel Security	0.001***	0.001***	0.210
Management Support	0.008***	0.066	0.058

*** Significant p-values at the 0.05 level of significance.

Taken as a whole, these results show that the organizations that have implemented one or more of the seven groups of security initiatives below perceive their security performance to be significantly better than organizations that have not. These seven groups of initiatives are (1)

security/operations related certifications, (2) business partner requirements, (3) advanced data, (4) physical security and access control, (5) security training, (6) personnel security and (7) management support and sponsorship.

It is also important to recall that advanced data, personnel security, physical security and security/operations related certifications are the four most popularly implemented security initiatives to date. Therefore, like an effort justification behavior[47], organizations that have implemented these initiatives due to compliance actually see these initiatives as having a significant positive effect on their security.

However, when the sample is split into shipper and service provider clusters, we can see that shippers and service providers differ in their opinions on two of these seven groups of significant initiatives. These two groups of initiatives are (1) business partner requirements and (2) personnel security. The significant difference in opinions about their impact on security performance comes mainly from the shipper cluster. The service providers in the sample are somewhat neutral about the effectiveness of instituting business partner requirements and personnel security on security performance.

The division on opinions on business partner requirements is consistent with findings gathered from field interviews. During the field interviews, service provider organizations such as the 3PLs, port operators and ocean carriers expressed that although they see security improvement as a holistic effort among different stakeholders in the supply chain, shippers (i.e. ultimate owners of the cargo) should be taking the lead in these efforts.

The division on opinions on personnel security training could be due to the fact that service providers typically employ more temporary workers compared to shippers as a result of the nature of their operations. As such, some of the examples of personnel security efforts such as background checks and security awareness training may be seen as being less effective to service providers.

The statistical relationship between perceived security impact and security performance is also significant with a standardized parameter estimate value of 0.419 (see Table 5.41). The

[47] Effort justification behavior refers to the tendency to reduce dissonance by finding reasons for why a person has devoted time, effort, or money for something turned out to be unpleasant or disappointing to the person (Gilovich et al., (2005).

statistically significant relationship (p-value < 0.05) between perceived security impact and security performance supports the fourth hypothesis (H4) that in the absence of objective security performance KPIs, organizations who perceive a security initiative (be it a mandatory one or voluntary one) as having strong impact on security performance will also perceive their performance in security to have improved after implementing the initiative (i.e. again an effort justification behavior).

At this point, it is important to recall that the data supported that current private sector security efforts are made primarily out-of-compliance rather than self-interests. Thus, it follows that in view of the positive relationships among perceived security impact, security effort and self-rated security performance, if there is no objective way of evaluating the effectiveness of security efforts, we can expect the effects of effort justification behaviour to kick-in.

It is also important of note that neither the shipper nor the service provider groups perceive any significant impact container/trailer/ULD security measures has on security performance. This is consistent with the findings from Langhoff et al. (2005), which found that most technologies for container security are not commercially viable in the near future because they do not function properly (i.e. they have less then 99.9% reliability), do not improve security or are too expensive. The study tested every major technology group that could possible be applied to a container: eSeals, container security devices (CSDs), cellular devices, GPS, and sensors (radiation, biological, chemical, etc.). International jurisdiction and frequency ranges also remain an issue especially for remote sensors and monitoring devices such as CSDs.

Security Effort and SCP

Via the impact on security performance, security effort also has a positive effect on traditional SCP. The statistical relationship between security performance and traditional SCP is significant with a very large standardized parameter estimate value of 0.728. This supports the fifth hypothesis (H5) and reflects the sentiments that organizations support the notion that in today's environment, an improvement in security performance will bring about a net positive improvement in traditional SCP.

To understand if there are specific groups of security initiatives that are contributing to these effects on traditional SCP, we conducted cross-tabulation analyses to identify any significant relationships between each group of security initiative and their corresponding impact on

various aspects of SCP[48]. Statistical significance is determined using the χ^2 test with p-values smaller than 0.05 considered as significant. Table 5.46 shows the p-values with the significant ones marked with "***".

Table 5.46: Cross-tabulation results for security initiatives and traditional SCP.

	Security/Operations Related Certification (P-Value)		
Aspects of SCP	**Entire Sample**	**Shipper**	**Service Provider**
Efficiency	0.255	0.087	0.277
Time	0.218	0.111	0.650
Reliability	0.208	0.161	0.950
Availability	0.159	0.111	0.906
Responsiveness	0.293	0.264	0.950
	Business Partner Requirements (P-Value)		
Aspects of SCP	**Entire Sample**	**Shipper**	**Service Provider**
Efficiency	0.126	0.025***	0.153
Time	0.004***	0.004***	0.662
Reliability	0.121	0.058	0.376
Availability	0.062	0.171	0.236
Responsiveness	0.001***	0.005***	0.376
	Container/Trailer/ULD Security (P-Value)		
Aspects of SCP	**Entire Sample**	**Shipper**	**Service Provider**
Efficiency	0.226	0.310	0.386
Time	0.045***	0.124	0.151
Reliability	0.121	0.100	0.872
Availability	0.023***	0.046***	0.257
Responsiveness	0.088	0.193	0.139
	Advanced Data (P-Value)		
Aspects of SCP	**Entire Sample**	**Shipper**	**Service Provider**
Efficiency	0.067	0.279	0.075
Time	0.010***	0.040***	0.151
Reliability	0.154	0.530	0.005***
Availability	0.222	0.266	0.762
Responsiveness	0.024***	0.035***	0.872
	Physical Security & Access Control (P-Value)		
Aspects of SCP	**Entire Sample**	**Shipper**	**Service Provider**
Efficiency	0.211	0.028***	0.047***
Time	0.004***	0.068	0.011***
Reliability	0.182	0.403	0.106
Availability	0.022***	0.068	0.177
Responsiveness	0.019***	0.090	0.106

[48] Respondents' answers on impact on various aspects of SCP are used instead of their self rating on SCP in Section A of the survey because SCP performance was self-rated at the very beginning of the survey which means that the respondents' answer could have been influenced by many other things other than security efforts.

Table 5.46 (continued): Cross-tabulation results for security initiatives and traditional SCP.

Aspects of SCP	Procedural Security (P-Value)		
	Entire Sample	Shipper	Service Provider
Efficiency	0.100	0.128	0.977
Time	0.101	0.125	0.849
Reliability	0.026***	0.059	0.341
Availability	0.069	0.060	0.735
Responsiveness	0.060	0.128	0.341
Aspects of SCP	**Tracking & Monitoring (P-Value)**		
	Entire Sample	**Shipper**	**Service Provider**
Efficiency	0.064	0.212	0.144
Time	0.002***	0.064	0.009***
Reliability	0.282	0.439	0.463
Availability	0.065	0.200	0.166
Responsiveness	0.024***	0.212	0.053
Aspects of SCP	**Security Training (P-Value)**		
	Entire Sample	**Shipper**	**Service Provider**
Efficiency	0.003***	0.004***	0.437
Time	0.001***	0.001***	0.530
Reliability	0.001***	0.003***	0.072
Availability	0.002***	0.001***	0.340
Responsiveness	0.001***	0.000***	0.613
Aspects of SCP	**Personnel Security (P-Value)**		
	Entire Sample	**Shipper**	**Service Provider**
Efficiency	0.069	0.278	0.212
Time	0.006***	0.047***	0.060
Reliability	0.280	0.370	0.708
Availability	0.010***	0.130	0.014***
Responsiveness	0.010***	0.178	0.002***
Aspects of SCP	**Management Support & Sponsorship (P-Value)**		
	Entire Sample	**Shipper**	**Service Provider**
Efficiency	0.006***	0.041	0.054
Time	0.016***	0.018***	0.478
Reliability	0.009***	0.092	0.025***
Availability	0.030***	0.066	0.250
Responsiveness	0.015***	0.041***	0.308

Which security initiatives have significant impacts?

As seen from Table 5.46, it is interesting to note that probably one of the most widely implemented security initiatives – security/operations related certification, is not perceived to have statistically significant impacts on any aspects of SCP. None of the p-values are statistically significant and the conclusion does not change when the respondent type (i.e. Shipper vs Service Provider) variable is added as a control variable. This clearly reflects the out-of-compliance nature of getting paper certifications such as C-TPAT and FAST.

Of the other four more popularly implemented initiatives (i.e. Business Partner Requirements, Advanced Data, Physical Access and Control and Personnel Security), all of them are perceived to have significant impact on time and responsiveness but only two of them (i.e. Physical Access and Control and Personnel Security) are perceived to have significant impacts on availability.

Security initiatives that seek to enhance supply chain visibility (i.e. Tracking and Monitoring) are perceived to have significant impacts on the time and responsiveness aspect of SCP. This is logically since the increased in ability to get information about the whereabouts of an organization's cargoes enables the organization to respond rapidly and effectively to chances in demand or routing. However, recall from Figure 5.11 that this is the least popularly implemented group of security initiatives. The majority of the other less popularly implemented initiatives such as procedural security, security training and management support and sponsorship, are also perceived to have significant impact on reliability. Two of these initiatives (Security Training and Management Support) are in fact perceived to have significant impact all aspects of SCP. Considering that these groups of security initiatives are relatively more complex to implement compared to the popular/mandatory ones such as Physical Access and Control, Business Partner Requirements and Security Certification, it is evident why they are less widely adopted despite their perceived collateral benefits. It is because security is yet viewed as a strategic driver for supply chain management and again, this result alludes to the fact that security initiatives are currently implemented out of compliance instead of self-interest.

What are the aspects of SCP that are impacted?

As can be seen from Table 5.46, the aspect of SCP that is impacted by the most number of groups of security initiatives is Time and Responsiveness, followed by Availability, then Reliability and finally Efficiency.

It is evident why respondents perceive Time and Responsiveness to be the most impacted aspect of SCP. Most of the security initiatives commonly implemented today including those that are mandatory (such as advanced manifest rule) requires additional operation times to be spent on inspecting and checking, thus lengthening processing time. It follows that as a result of a "longer" supply chain and the increased risk of cargo being held at customs check points for inspections, organizations may opt to hold more inventories in order to remain responsive to their customers and ensure that their products and/or services are always available when

demanded. Those who do not or cannot will perceive security efforts as having a negative impact on their responsiveness and availability performance.

Reliability and Efficiency are two aspects of SCP that are perceived to be the least impacted by security efforts. Recall that many of the security technologies are "promoted" as being able to make one's supply chain more reliable and efficient. If this is not what the users (i.e. Shippers and Service Providers) perceive, then the marketing message may not have been the most appropriate.

Next notice from Figure 5.16 that respondents perceive that the impact security efforts have on security performance has unfavorable impacts on the efficiency, time and availability aspect of SCP. The regression weights between Perceived Security Impact and Impact on Efficiency, Time and Availability are negative with values of -0.22, -0.25 and -0.14 respectively. The relationship between Perceived Security Impact and Time and Availability are statistically significant meaning that security efforts that are perceived to bring about an improvement in security are perceived to bring about deteriorations in an organization's supply chain's on-time performance and ability to ensure availability of their products and services. This is consistent with the sentiments gathered from the field interviews. Theoretically, we can also see why this is so. Physical access and control and other procedural security initiatives that add checkpoints and inspections along the cargo movement process also add non-value adding delays to the supply chain, causing organizations to perceive a negative impact on their time performance. A lengthened supply chain brings about additional operations uncertainties. Additional checks and balances, more thorough and lengthy cargo handling procedures and inspections can also affect an organization's ability in ensuring that their products and services will always be available to their customers. As such it is not surprising organizations perceive a negative impact of enhanced security on their availability performance. These observations are very logical considering that the most popular security improvement initiatives currently are personnel security, physical security and access control and obtaining security related certifications which typically add additional checks and balances along the cargo movement process.

Although the relationship between Perceived Security Impact and Efficiency Impact is not statistically significant, the direction of the relationship does serve to illustrate a common sentiment found during the field interviews – security improvement initiatives are cost items.

Security initiatives such as physical access and control and C-TPAT certifications, costs money and do not have an immediate ROI. As such, organizations adopting these measures will perceive a negative impact on their supply chain efficiency.

It is often claimed that enhanced supply chain visibility can lead to other collateral benefits such as allowing an organization to be more responsive to changing business environment and enabling an organization to use of limited resources more effectively and efficiently in order fulfilment. Since security initiatives such as Tracking and Monitoring, which have the potential to improve an organization's visibility of its supply chain operations, is the least implemented group of security initiatives, it is small wonder again why respondents feel that the security efforts taken have a negative impact on their time, availability and efficiency performance.

And in light of Figure 5.10 where respondents consistently rank Tracking and Monitoring as the group of security initiatives with the greatest impact on all aspects of SCP, it is very evident that the private sector is currently adopting security initiatives only when mandated. The concept of collateral benefits is not enough to entice private organizations to adopt particular security improvements just yet.

However, notice from Figure 5.16 that organizations do perceive that security efforts that bring about an increase in security will bring about improvements in the reliability performance aspect of SCP. The regression weight between the Perceived Security Impact and Impact on Reliability is positive with a value of 0.093. Again, although this relationship is not statistically significant, it serves to illustrate a logical theory that a secured supply chain is also a more reliable[49] supply chain.

Are there any differences between Shippers and Service Providers?

The significant differences for the more popular security initiatives such as Advanced Data, Physical Access and Control, Personnel Security and Management Sponsorship and Support, come from the service provider cluster of respondents. Business Partner Requirements on the other hand, has significant differences accounted for by respondents in the shipper cluster. This is consistent with findings from field interviews where interviewees especially service provider organizations such as 3PLs, ocean carriers and port operators expressed that the ultimate

[49] "Reliable" being defined as consistency and dependability of supply chain operations.

cargo owners (i.e. Shippers) should take the lead in the holistic effort towards improving security.

The Insights

In conclusion, security efforts are perceived to have positive impacts on supply chain security performance and opinions between the shipper and service provider cluster are similar. Specifically, the five most popularly implemented security initiatives – personnel security, physical security and access control, security/operations related certification, advanced data and business partner requirements, are perceived to have the greatest impact on security performance. This could be a genuine feedback or an effort justification behavior or a combination of both.

But these same initiatives are not perceived to have significant impacts on SCP. This is especially the case for security/operations related certification. This group of initiatives is not perceived to have significant impact on any of the aspects of SCP.

Two of the ten groups of initiatives – security training and management support are also perceived to have significant impacts on security performance. They are also perceived to have significant impacts on all aspects of SCP, but they are currently two of the three least implemented initiatives; the other being tracking and monitoring. Tracking and Monitoring type of security initiatives are also perceived to have relatively wider impacts on SCP but is similarly not widely implemented. The fact that organizations are not implementing initiatives that they perceive to have positive impacts on their SCP reflects very strongly the reality that the private sector is currently adopting security initiatives out of compliance instead of self-interest.

The overall net perceived impact on traditional SCP is also positive. Results support Willis and Ortiz (2004) preliminary conclusions that supply chain efficiency and security are distinct but interconnected. However, the private sector does perceive that security efforts will bring about unfavorable impacts to the time, availability and efficiency aspects of SCP. The longer cycle time of the supply chain due to longer delays in getting goods through the global supply chain threatens supply chain practices such as Just-in-Time and lean inventory processes (Lee, 2004); Just-in-Time and lean inventory processes are proven supply chain strategies for improving supply chain performance especially operations efficiency and product availability.

Additional checks and inspections along the cargo movement process also add delays which are not necessarily value-adding.

Those security initiatives that are touted to bring about collateral benefits (e.g. enhanced availability of products and on-time performance of deliveries) as a result of improved supply chain visibility, such as Tracking and Monitoring, are however least widely implemented. As such, it is little wonder that organizations responding to this study perceive these negative effects of security efforts on their SCP.

Taking all operating factors into consideration, security efforts and improvements are perceived to have a net positive impact on SCP. Specifically, instituting the right procedures, training personnel appropriately and ensuring higher level management support, are the ways to go in ensuring reliability in an organization's supply chain operations in this increasingly uncertain environment. It is also apparent that these initiatives are much more long-term in nature and affects a more fundamental level of business operations than physical security and access control, personnel security, obtaining security certifications and transmitting shipment information in advance.

Results from this study also clearly illustrate the industry's opinions about the need for security efforts to be holistic. Instituting business partner requirements is not only perceived to have a significant impact on security performance, it is also perceived to be beneficial to the overall responsiveness of the supply chain. And the community expects the ultimate cargo owner (i.e. the shipper) to take the lead on this.

CHAPTER 6 CONCLUSION

This Chapter concludes the study and addresses the contributions and limitations of the study, final thoughts and potential future research directions.

This study attempted to increase the understanding of supply chain security management and provide useful insights to managers seeking to improve security performance of their supply chain. While the data in this study should not be considered as any type of industry average, the findings do demonstrate the key ideas and concepts in managing security in supply chain operations as described in the rest of this chapter. This study provides a major step and springboard for further research in the area of supply chain security management and performance evaluation.

6.1 Undertaking Security Effort

The results from this study clearly show the positive effects that security improvements have on overall supply chain performance. As such, undertaking security investments should not be omitted from an organization's overall supply chain strategic plan, if the organization endeavours to improve their overall supply chain operations performance.

The Motivation/Drivers

The field interview and empirical results from this study show that security is not yet a strategic driver in supply chain management. These sentiments do not differ significantly between the Shipper and Service Provider community. They also do not differ among organizations with different cargo nature, typical shipment sizes, organization size and scope of supply chain control/influence.

The current motivation/drivers behind the private sector's implementation of security initiatives are found to be very much due to a pressure to comply with public sector regulations and/or simply the ease of implementation. This is consistent with current literature on security such as Willis and Ortiz (2004), Wolfe (2004), Langhoff et al. (2005), Rice and Spayd (2005), Peleg-Gillai et al. (2006).

Support for this observation comes from the fact that respondents in this study place more weight on perceived security impact compared to perceived collateral benefits when determining the extent or amount of security efforts to undertake. The empirical results of this study also show that the most widely implemented security initiatives are not the ones perceived to have the greatest positive impact on SCP (i.e. collateral benefits). In fact, on the contrary, those security initiatives that are widely implemented are the ones perceived to have little or no collateral benefits.

To entice private organizations to undertake security investments out of self-interests, it is then logical for one to look to the concept of collateral benefits. That is, using collateral benefits as a catalyst to entice private sector investments in security improvements. The results from this study shows that although private organizations are cognizant of the collateral benefits that can come along with investments in security, they are not really basing their security investment decisions on collateral benefits right now. Their out-of-compliance behaviour in this context clearly shows the relative importance they see security in managing their supply chain.

These observations together mean that there is much work required to market the concept of collateral benefits. It also means that it is equally important to sell the idea of security as a potential competitive advantage in supply chain management in the future.

Types of Effort and Their Effectiveness on Security Improvement

Not all security initiatives are viewed equal however. Based on the ten groups of security initiatives outlined in the CBP's (2006) catalog of supply chain security best practices, the initiatives that are perceived to have significant impacts on security performance are (not in order of importance) [50]:

- Obtain security/operations related certifications
- Institute business partner requirements
- Comply with advanced data requirements
- Establish physical security and access controls
- Conduct security training for personnel

[50] However, it is important to be cognizant that these are also some of the most popularly implemented security initiatives. As such this could either be a genuine feedback or an effort justification behavior or a combination of both.

- Implement personnel security measures
- Garner management support

Empirical results show that the Service Provider group tends to place more importance in the effectiveness of initiatives such as obtaining certifications, complying with advanced data requirements and instituting physical security and access controls. This observation is not surprising considering the widespread outsourcing environment today, where service providers are the ones handling the physical cargo storage and movement and the associated shipping documentation for their clients.

The Shipper group on the other hand, also places more importance on externally oriented initiatives such as establishing business partner requirements. This observation is encouraging for the holistic approach to improving supply chain security. Many of the service providers interviewed during the field interviews have expressed the appropriateness for customers to lead the holistic effort in improving supply chain security.

It is also interesting to note that neither the shipper nor the service provider groups perceive container/trailer/ULD security measures to have any significant impacts have on security performance. This is consistent with the findings from current literature which found that most technologies for container security are not commercially viable in the near future because they do not function properly (i.e. they have less then 99.9% reliability), they do not improve security or they are too expensive. The study tested every major technology group that could possible be applied to a container: eSeals, container security devices (CSDs), cellular devices, GPS, and sensors (radiation, biological, chemical, etc.).

Types of Efforts and Their Collateral Benefits

In terms of collateral benefits, security efforts in general are perceived to have significant impacts on time and availability and the perceived impacts are negative. Efficiency is also found to be negatively impact by a tightening of security within the supply chain but the empirical results of this study for this is not statistically significant. These observations are not surprising considering there are widespread theoretical and logical support for the negative effects that security initiatives such as additional inspections and checkpoints have on lengthening the supply chain and increase the amount of uncertainties in cargo movement.

The reliability aspect of SCP on the other hand, is found to be positively impacted by a tightening of security within the supply chain. This is what security improvements are supposed to do anyways and it is encouraging that the private sector holds this same view.

However, again not all security initiatives are viewed the same when it comes to the idea of collateral benefits. Certain groups of initiatives are perceived to have more significant impacts on various aspects of SCP than others. Table 6.1 ranks the ten groups of security initiatives based on their popularity of implementation and lists their corresponding collateral benefits (i.e. aspects of SCP that are found to be statistically significantly different between those respondents who have implemented that initiative and those who have not).

Table 6.1: Ranking security initiatives by implementation popularity with no. of SCP aspects that are statistically significant.

Security Initiatives (Ranked by Popularity of Implementation)	**Significant SCP Aspects Affected**
Personnel security	Time Availability Responsiveness
Physical security & access control	
Operations/security related certifications	None
Advanced data compliance	Time Responsiveness
Business partner requirements	
Container/ULD security	Time Availability
Procedural security	Reliability
Security training & outreach programs	Efficiency Time Availability Reliability Responsiveness
Management support & sponsorship	
Tracking & monitoring	Time Responsiveness

It is interesting to note that of all the security initiatives, Tracking and Monitoring is the least implemented security initiative but is at the same time, perceived by respondents to be the one that can bring about a relatively good amount of collateral benefits in terms of time and

responsiveness performance. The other two least implemented initiatives – security training and management support, are also perceived to have significant positive impacts on SCP.

On the contrary, one of the more widely implemented security initiatives - Security Related Certifications, is perceived to bring about little or no collateral benefits. This finding again reflects very strongly the reality that the private sector is currently adopting security initiatives out of compliance instead of self-interest.

Shippers Should Lead the Holistic Effort

Shippers and service providers also differ in their opinions on the effectiveness of instituting business partner requirements. The service providers in the sample are somewhat neutral about the effectiveness of instituting business partner requirements and personnel security on security performance but shippers feel otherwise. These results support the findings from the field interviews where service provider organizations such as the 3PLs, port operators and ocean carriers expressed that although they see security improvement as a holistic effort among different stakeholders in the supply chain, shippers (i.e. ultimate owners of the cargo) should be taking the lead in these efforts.

6.2 Evaluating the Effectiveness of Security Effort

Although not perceived to be a competitive advantage/supply chain driver in the near term, industry practitioners, shippers and service providers alike, do see security as a component of overall SCP. Results from this study indicate that KPIs for security performance are indeed a subset of traditional SCP from the industry practitioners' point of view.

Results from this study together with existing literature on SCP suggest that traditional SCP evaluation is made up of six key components:

- Efficiency (utilization of resources including time, money, people and infrastructure)
- Reliability (on-time, speed)
- Accuracy
- Availability (business planning effectiveness)
- Responsiveness (agility and flexibility)

- Security

Specifically, security performance measurements can be further classified into four key components that are very similar to the components of supply chain management:

- those measuring the accuracy and reliability of information
- those measuring the effectiveness of physical breaches prevention
- those measuring the cost of security initiatives
- those measuring the safety of operations and personnel

Results from this study also indicate that industry practitioners perceive security performance to have implications on not only one but many aspects of traditional SCP, especially in terms of timeliness, reliability, availability and efficiency.

6.3 Managerial Implications of Results

Security Investments Should be Viewed as Any Other Supply Chain Investments

It is essential for private organizations to recognize that security investments, like any other supply chain investments, bring about supply chain tradeoffs. What is more important is that at the end of the day, there should be a net positive impact on overall supply chain performance.

Specifically, instituting the right operating procedures with sound checks and balances, training personnel appropriately and ensuring higher level management support, is the way to go in ensuring reliability in an organization's supply chain operations in this increasingly uncertain environment. And it is apparent why this is so. These initiatives are much more long-term in nature and affect a more fundamental level of business operations than physical security and access control, personnel security, obtaining security certifications and transmitting shipment information in advance.

What to Invest?

An extension of Table 6.1, Table 6.2 shows the corresponding ranking of security initiatives based on perceived SCP impacts (i.e. collateral benefits) and their perceived impact on security itself.

Based on the insights and experience of the maritime supply chain community and the findings in this study, Figure 6.1 illustrates a route that private organizations can take in improving the security of their supply chain. It seems then that the way to go in improving supply chain security is to kick start the security efforts with appropriate investments in physical security and access control mechanisms. Simple and easy to implement measures include restricting access to sensitive areas, reviewing and renewing (if needed) employee identification system and using uniforms to distinguish between staff and visitors, establishing a visitor logging system and monitoring all pickups and deliveries.

Table 6.2: Ranking security initiatives.

<table>
<tr><th colspan="2">Collateral Benefits</th><th rowspan="2">Statistically Significant impacts on Security (Table 5.41)</th></tr>
<tr><th>Rank based on "Perceptions" (Figure 5.10)</th><th>Rank based on "Actual Experience" (Table 5.42)</th></tr>
<tr><td rowspan="10">1. Tracking & Monitoring (5.39)

2. Management Support (5.21)

3. Physical Security and Access Control (5.18)

4. Business Partner Requirements (5.17)

5. Security Training (5.13)

6. Container Security (5.05)

7. Procedural Security (5.03)

8. Advanced Data (5.02)

9. Personnel Security (5.00)

10. Security Related Certification (4.78)</td><td>All Aspects:
Security Training
Management Support

(Efficiency, Time, Reliability, Availability, Responsiveness)</td><td rowspan="10">Security Related Certification

Business Partner Requirements

Advanced Data

Physical Security & Access Control

Security Training

Personnel Security

Management Support</td></tr>
<tr><td>3 Aspects:
Personnel Security
Physical Security and Access Control

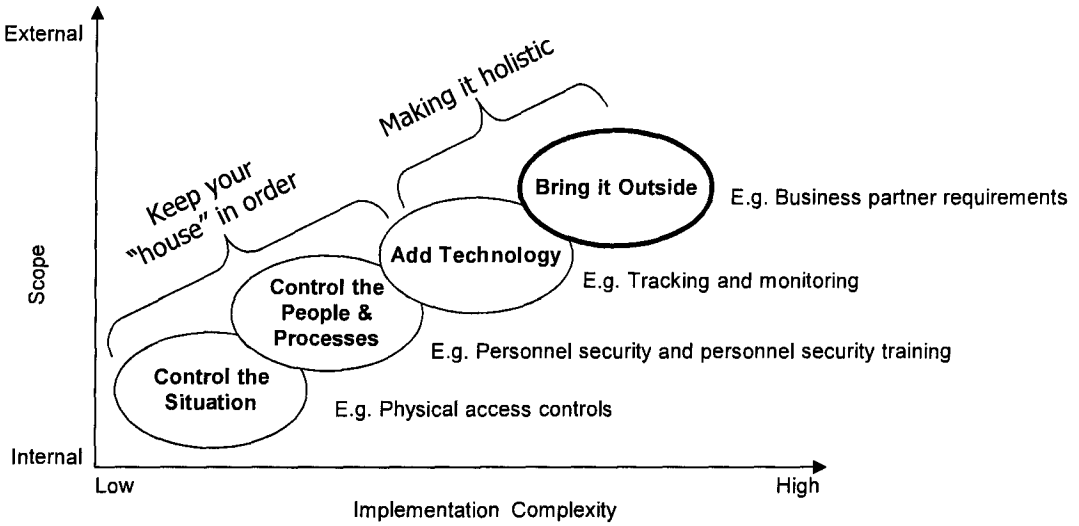
(Time, Availability, Responsiveness)</td></tr>
<tr><td>2 Aspects:
Tracking & Monitoring
Advanced Data
Business Partner Requirements

(Time, Responsiveness)</td></tr>
<tr><td>2 Aspects:
Container Security

(Time, Availability)</td></tr>
<tr><td>1 Aspect:
Procedural Security

(Reliability)</td></tr>
<tr><td>None:
Security Related Certifications</td></tr>
</table>

Figure 6.1: The route to improving supply chain security.



The next step would be to establish procedures to ensure personnel security and conduct security training to all personnel. Initiatives such as conducting pre-employment background checks and proper employment termination procedures can be established as a start to ensure personnel security. Once that is done, it is important to permeate the importance of security to the entire organization through training and awareness building. An organization is ultimately about its people.

Next, one can look to instituting appropriate technologies that seeks to improve the visibility of one's supply chain operations. Tracking and monitoring types of projects will improve an organization's visibility of its supply chain and thereby allow a more agile response to disruptions. It will also enable an organization to more efficiently and effectively utilise its order fulfilment resources.

After taking care of internal security matters, the next step is to bring the overall security effort to other stakeholders in the supply chain. The supply chain is made up of many sequential and simultaneous events/tasks that are necessary to move products from where they originate to where they are desired. And many stakeholders are involved along the way, thereby creating many handoffs and many different ways of doing things. It is therefore of no good for only any one of the components to be secure and the rest not. Similar to the concept where a supply

chain is only as efficient as its weakest link, a supply chain is only as secure as it's least secure component.

The need for the different stakeholders to collaborate on security efforts thus cannot be over-emphasised. Externally-oriented security initiatives such as instituting business partner requirements and security related requirements can be negotiated and established with business partners to ensure a minimum level of security mechanisms in the supply chain. Organizations in the private sector that were interviewed for this study have echoed the importance of a holistic effort for any security effort to be effective.

Last but not least, it is important to bear in mind that security improvements are long term investments and similar to other long term major business endeavours, it is essential to garner top management endorsement for any security efforts.

When Evaluating Security Investments, Look to Four Key Components

When evaluating security efforts, an organization can look at four key aspects – Information, Cost, People and Cargo (Figure 6.2) to determine the appropriate KPIs to be used. The set of KPIs that an organization should pick or use to evaluate their security investments and initiatives should include at least one from each of these four areas for comprehensiveness as well as to capture any potential trade-offs.

Figure 6.2: Security efforts evaluation framework.

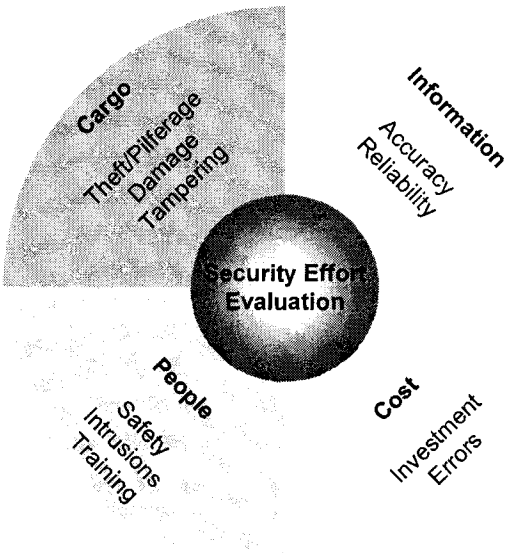


Figure 6.2 provides examples of KPIs in each area that organizations can utilize to evaluate their security performance.

In terms of information, examples of KPIs to assess the accuracy of information sent and received include (1) number of EDI re-transmissions for shipment manifests and (2) number of re-issued bills-of-lading as a result of errors. Examples of KPIs to assess the reliability of information sent and received such as completeness and consistency in information transmission performance include (1) percentage of EDI re-transmissions and (2) percentage of incomplete bills-of-lading or booking forms received from shippers.

In terms of cost, examples of KPIs to assess the total cost of investment include (1) total initial outlay for security equipment and/or headcount, (2) cost of conducting security training and (3) cost of obtaining security certification. Examples of KPIs to assess the costs of errors and re-work include (1) cost per man hour x the number of hours spent on re-working documents or correcting errors and (2) value of lost sales due to overages, shortages and damages.

In terms of people, examples of assessing and monitoring the safety performance of operations include (1) number of safety accidents and near incidents and (2) number of illegal and attempted unauthorised entries into restricted areas. Examples of KPIs for assessing the amount and quality of security training programs include (1) personnel average assessment grade for security awareness programs and (2) number of security related training programs.

In terms of cargo, examples of KPIs for monitoring cargo thefts and pilferages include (1) the amount and number of cargo thefts and pilferages and (2) the amount and frequency of overages, shortages and damages. The frequency of cargo overages, shortages and damages are good indicators of loop holes in the cargo movement process and indicates the potential for cargo tampering.

This study does not endeavour to provide an exhaustive list of KPIs for each of the above categories. This is because the KPIs in each of the above categories will differ between any two organizations. For instance, a KPI for pilferage for an organization handling apparel may not be appropriate or the same for another organization handling precious metals. The organization handling apparel may be interested in capturing and monitoring the number of incidents beyond what is allowed for shrinkage but the organization handling precious metals will want to

measure the value of pilferage with no shrinkage amount allowed. Another example, an organization handling chemicals will be interested in the number of spill incidents as an indication of the level of safety in its operations but this will not be relevant for an organization handling fast moving consumer products.

Therefore, it is important for an organization endeavouring to use the above framework, to recognise the need to identify KPIs that are relevant to its own business operations. The important thing is to ensure that the set of KPIs should include indicators from each of the four areas.

6.4 Limitations of Study

The findings from this study are interesting and are definitely a springboard for further research in the realm of supply chain security management. There are nevertheless some limitations that we have to be cognizant of.

Sample Size

The sample size for the survey was obtained from the membership databases from CSCMP Canada, China, Hong Kong, Singapore and U.S., the Canadian Transportation & Logistics weekly e-newsletter and the Supply Chain Logistics Council (SCL) Canada. Thus, the results of the study are only generalizable to the extent that these members resemble the population of the maritime supply chain community that is involved in cargo movement between Asia and North America and are knowledgeable about their organization's supply chain management and security management efforts.

Considering the sensitivity and complexity of the subject matter, this sample size obtained is considered reasonable. Although sufficient for the analytical techniques used in this study, the sample size can certainly be larger to achieve better model fits and power. The results from this study endeavours to reflect industry opinions, therefore the larger the sample size, the better the results will be able to serve its purpose.

Common Method Variance for Factor Analysis

Measures of a construct have variance due to the construct being measured as well as variance due to measurement error. This measurement error is made up of two components – random

error and systematic error (the error due to method effect). Measurement error is omnipotent and its confounding influences on research findings cannot be avoided and this study is no exception.

The amount of construct, method and random error variance can be estimated for Common Factor method of extraction but not Principal Component method. This is because the Principal Component method derives factors that contain small proportions of unique variance and in some instances, error variances (that include variance due to method and variance due to random error). This is different from the Common Factor method which derives factors based only on common variance (i.e. variance that is shared with all other variables in the analysis).

It is recognized that the method effect is present in this study as with any other empirical study. And although not calculated, it is important to note that the method effect does not appear to be an issue in the study. This is because there is not a single factor that accounts for more than 50% of the total variance explained. Figures 5.8 and 5.9 show the scree plots for the SCP and SP factor analyses respectively. The amount of variance explained by the first factor for SCP and SP is 26.80% and 35.96% respectively.

Self-Rated Performance

In view of the issue of confidentiality that most private organizations have over performance type information and to encourage more responses, self-rated performance data instead of truly objective KPI performance data were asked. The performance data are therefore subjected to the limitation of individual respondent's judgement and interpretation of level of performance.

Operational Characteristics Not Covered

The survey instrument used in this study has tried to capture as much information as possible about an organization's operational characteristics without compromising the rate of response. There is however some data items that have to left out due to scope limitation and concerns over the negative impact on response rate. These include items that can be used as indicators for an organization's degree of overseas sourcing and the extent of implementation of each security initiatives.

The degree of overseas sourcing especially from countries that are generally known to be less secure in terms of cargo movement infrastructure, may impact the degree of importance that

organizations place on security management and the types of security efforts that they may undertake and the extent to which they would take them.

The extent of the implementation of a security initiative will also affect the amount of impact it will have on security performance and supply chain performance (i.e. collateral benefits).

6.5 Future Research

Next, we examine the scope for future research in this topic area. It is hoped that the findings from this study will spark off further quantitative research in this topic area. Below are some potential future research directions.

Other Organizational Characteristics

Future research efforts in this topic area should include further studies including other potential business factors that can affect security efforts and their impacts on security performance and supply chain performance. These potential business factors can include an organization's extent of overseas sourcing and an organization's corporate culture.

Other Trade Routes

Different geographical areas create different operating environments that breed different operational practices and behaviours. These factors are expected to produce different attitudes and behaviours towards security management. As such, other trade routes can be studied to identify and understand the differences (if any) in private organizations' opinions and behaviour towards security efforts and performance evaluation.

Other Supply Chains

This study focused on the stakeholders in the maritime supply chain. Other supply chain communities that use primarily air transportation or rail transportation poses different supply chain challenges. The different operational intricacies can yield attitudes, behaviours and the same security efforts may yield different security performance results. These other supply chain communities can therefore be studied and results compared as a step towards a more comprehensive understanding of the complex topic of supply chain security management.

REFERENCES

Anastasi, A. (1976), *Psychological Testing,* 4th Ed. New York: Macmillan.

Anonymous (2006), "Marketplace," *Security Management*, Vol. 50, No. 4, pp. 128-133.

Anonymous (2006), "Marketplace," *Security Management*, Vol. 50, No. 5, pp. 122-126.

Anonymous (2006), "Marketplace," *Security Management*, Vol. 50, No. 6, pp. 148-150.

Arbuckler, J. L. (2003), *Amos 5.0 Update to the Amos User's Guide*, SmallWaters Corporation.

Arbuckler, J. L. and W. Wothke (1995), *Amos 4.0 User's Guide*, SmallWaters Corporation.

Armstrong, J. S. and P. Soelberg, P. (1968), "On the Interpretation of Factor Analysis," *Psychological Bulletin*, Vol. 70, pp. 361-364.

Banomyong, R. (2005), "The Impact of Port and Trade Security Initiatives on Maritime Supply-Chain Management," *Maritime Policy and Management*, Vol. 32, No. 1, pp. 3-13.

Baumgartner, H. and C. Homburg (1996), "Applications Structural Equation Modeling in Marketing and Consumer Research: A Review," *International Journal of Research in Marketing,* Vol. 13, pp. 139-161.

Bearden, W. O., R. G. Netmeyer, and M. F. Mobley (1993), *Handbook of Marketing Scales: Multi-item Measures for Marketing and Consumer Behavior Research,* Newbury Park, CA: Sage.

Bernasek, A. (2000), "The Friction Economy: American Businesses Just Got the Bill for the Terrorist Attacks: $151 billion a Year," *Fortune*, Vol. 145, No. 4, pp. 104-110.

Blanchard, B. S. (1992), *Logistics Engineering and Management*, Engelwood Cliffs, NJ: Prentice Hall.

Byrne, B. M. (2006), *Structural Equation Modeling with EQS: Basic Concepts, Applications and Programming (2nd Ed)*, Mahwah, NJ: Lawrence Erlbaum Associates, Publishers.

Carmines, E. G. and R. A. Zeller (1979), *Reliability and Validity Assessment,* Beverly Hills: Sage.

Cassidy, W.B. (2003), "Breaking Global Barriers: With the Help of Technology and Third-Party Services, Smaller Shippers are Cracking International Market," *Traffic World*, Vol. 267, No. 21, pp. 21-24.

Caton, R.F. (2004), "Paper Security Isn't Enough," *Journal of Commerce*, June 28, pp. 1.

Cattell, R. B. (1978), *The Scientific Use of Factor Analysis in Behavioural and Life Sciences*, New York: Plenum.

Chopra, S. and P. Meindl (2004), *Supply Chain Management: Strategy, Planning and Operations*, 2nd Edition, Pearson/Prentice Hall, Upper Saddle River, New Jersey.

Christopher, M. (2000), "The Agile Supply Chain," *Industrial Marketing Management*, Vol. 29, No. 1.

Christopher, M. and D. Towill (2000), "Supply Chain Migration from Lean to Agile and Customized," *Supply Chain Management*, Vol. 5, No. 4, pp. 206-13.

Chow, G. (2007), "Collateral Benefits of Security and Supply Chain Improvements at International Gateways," *Calgary Asia Pacific Gateway and Corridor Round Table,* March 28-29, 2007.

Chow, G., D. Frank, and A. Gados (2006), "Regulations and Initiatives Affecting Secure, Efficient and Safe Cross-Border Freight Movements (unpublished draft)," *Bureau of Intelligent Transportation Systems and Freight Security (BITSAFS), Sauder School of Business, University of British Columbia.*

Chow, G., D. Frank, and H. Yew (2006), "Review of ITS Technologies with Application to the Security and Efficiency of Cross-Border Freight Movement (unpublished draft)," *Bureau of Intelligent Transportation Systems and Freight Security (BITSAFS), Sauder School of Business, University of British Columbia.*

Chow, G., T. D. Heaver, and L. E. Henriksson (1994), "Logistics Performance: Definition and Measurement," *International Journal of Physical Distribution & Logistics Management,* Vol. 24, No. 1, pp. 17-28.

Churchill, G. A. (1979), "A Paradigm for Developing Better Measures of Marketing Constructs," *Journal of Marketing Research*, Vol. 16, No. 1, pp. 64-73.

Closs, D. J. and E. F. McGarrell (2004), "Enhancing Security Throughout the Supply Chain," *IBM Center for The Business of Government*, Special Report Series.

Closs, D., D. Lynch, J. M. Whipple, and D. Voss (2006), "Enhancing Supply Chain Security," *CSCMP 2006 Conference*, San Antonio, October 15-18.

Comrey, A. L. (1978), "Common Methodological Problems in Factor Analytic Studies," *Journal of Consulting and Clinical Psychology*, Vol. 46, pp. 648-659.

Cook, J. D., S. J. Hepworth, T. D. Wall, and P. B. Warr (1981), *The Experience of Work*, San Diego: Academic Press.

Cote, J. A. and M. R. Buckley (1987), "Estimating Trait, Method, and Error Variance: Generalizing Across 70 Construct Validation Studies," *Journal of Marketing Research*, Vol. 24, No. 3, pp. 315-318.

Cox, E. P. (1980), "The Optimal Number of Response Alternatives for a Scale: A Review," *Journal of Marketing Research*, Vol. 17, pp. 407-422.

Coyle, J. J., E. J. Bardi, and C. J. Langley (1992), *The Management of Business Logistics*, 5th Edition, St. Paul: West Pub. Co.

Craeger, J. A. (1958), "General Resolution of Correlation Matrices into Components and its Utilization in Multiple and Partial Regression," *Psych*, Vol. 23, pp. 1-8.

Crosby, L. and S. A. LeMay (1998), "Empirical Determination of Shipper Requirements for Motor Carrier Services: SERVQUAL, Direct Questioning and Policy Capturing Methods," *Journal of Business Logistics*, Vol. 19, No. 1, pp. 139.

Cubalchini-Travis, L. (2006), "Lean Distribution," *Quality Progress,* Vol. 39, No. 11, pp. 81.

Damas, P. (2001), "Supply Chains at War," *American Shipper*, Nov, pp. 17-18.

Daugherty, P. J., T. P. Stank, and A. E. Ellinger (1998), "Leveraging Logistics/Distribution Capabilities: The Effect of Logistics Service on Market Share," *Journal of Business Logistics*, Vol. 19, No. 2, pp. 35-51.

Deloach, J. W. (2000), *Enterprise-Wide Risk Management, Strategies for Linking Risk and Opportunities*, Financial Times/Prentice Hall, London.

Doherty, N. A. (2000), *Integrated Risk Management – Techniques and Strategies for Managing Corporate Risk*, McGraw Hill, New York, USA.

Dunn, S. C., R. F. Seaker, A. Stenger, and R. Young (1993), "An Assessment of Logistics Research Paradigms," Working Paper 93-5, *Center for Logistics Research*, The Pennsylvania State University.

Dunn, S. C., R. F. Seaker, and M. A. Waller, (1994), "Latent Variables in Logistics Research: Scale Development and Validation," *Journal of Business Logistics*, Vol. 15, No. 2, pp. 145-172.

Dwyer, P. S. (1940), "The Evaluation of Multiple and Partial Correlation Coefficients from the Factorial Matrix," *Psych*, Vol. 5, pp. 211-232.

Edmonson, R. G. (2006), "Five Years Later...." *Journal of Commerce*, New York, September 11.

Emerson, C. J. and C. M. Grimm (1996), "Logistics and Marketing Components of Customer Service: An Empirical Test of the Mentzer, Gomes and Krapfel Model," *International Journal of Physical Distribution & Logistics Management*, Vol. 26, No. 8, pp. 29.

European Conference of Ministers of Transport (ECMT) (2005), *Container Transport Security Across Modes.*

Fabrigar, L. R., D. T. Wegener, R. C. MacCallum, and E. J. Strahan (1999), "Evaluating the Use of Exploratory Factor Analysis in Psychological Research," *Psychological Methods*, Vol. 4, No. 3, pp. 272-299.

Fawcett, S. E., L. L. Stanley, and S. R. Smith (1997), "Developing a Logistics Capability to Improve the Performance of International Operations," *Journal of Business Logistics*, Vol. 18, No. 2, pp. 101-127.

Ferguson-Amores, M. C., M. Garcia Rodríguez, and J. Ruiz-Navarro (2005), "Strategies of Renewal: The Transition from 'Total Quality Management' to the 'Learning Organization'," *Management Learning*, Vol. 36, No. 2, pp. 149-180.

FIA International Research Ltd. (2001), *Contraband, Organised Crime and the Threat to the Transportation and Supply Chain Function*, September.

Ford, J. K., R. C. MacCallum, and M. Tait (1986), "The Applications of Exploratory Factor Analysis in Applied Psychology: A Critical Review and Analysis," *Personnel Psychology*, Vol. 39, pp. 291-314.

Garver, M. S. and J. T. Mentzer (1999), "Logistics Research Methods: Employing Structural Equation Modeling to Test for Construct Validity," *Journal of Business Logistics*, Vol. 20, No. 1, pp. 33-57.

Gassenheimer, J. B., J. U. Sterling, and R. A. Robicheaux (1989), "Long-term Channel Member Relationships," *International Journal of Physical Distribution and Materials Management*, Vol. 19, No. 12, pp. 15-28.

Gilovich, T., D. Keltner, and R. E. Nisbett (2005), *Social Psychology*, W. W. Norton.

Goldsby, T. J., S. E. Griffis, and A. S. Roath (2006), "Modeling Lean, Agile, and Leagile Supply Chain Strategies," *Journal of Business Logistics*, Vol. 27, No. 1, pp. 57.

Gorsuch, R. L. (1983), *Factor Analysis* (2nd Ed.), Hillsdale, NJ: Erlbaum.

Gupta, V., P. J. Hanges, and P. Dorfman (2002), "Cultural Clusters: Methodology and Findings," *Journal of World Business*, Vol. 37, pp. 11-15.

Grover, R. and M. Vriens (2006), *The Handbook of Marketing Research: Uses, Misuses and Future Advances*, Sage Publications.

Hair, J. F. Jr., R. E. Anderson, R. L. Tatham, and W. C. Black (1998), *Multivariate Data Analysis*, Prentice Hall.

Hall, R. (1991), *Organizations: Structures, Processes and Outcomes*, Prentice-Hall, New York and London, pp. 267.

Harman, H. H. (1967), *Modern Factor Analysis, 2nd Edition (Revised)*, Chicago and London: The University of Chicago Press.

Helferich, O. K. and R. L. Cook (2003), *"Securing the Supply Chain,"* Chicago: Council of Logistics Management.

Hiles, A. and P. Barnes (2001), *The Definitive Handbook of Business Continuity Management*, J. Wiley and Sons, Chichester.

Hinkins, T. R. (1995), "A Review of Scale Development Practices in the Study of Organizations," *Journal of Management*, Vol. 21, No. 5, pp. 967-988.

Hinkin, T. R. and C. A. Schriesheim (1989), "Development and Application of New Scales to Measure the French and Raven (1959) Bases of Social Power," *Journal of Applied Psychology,* Vol. 74, No. 4, pp. 561-567.

Hofstede, G. (1980). *Cultures Consequences*, Sage, Beverly Hills, CA.

Jacoby, J. and M. S. Matell (1971), "Three-Point Likert Scales are Good Enough," *Journal of Marketing Research*, Vol. 8, No. 4, pp. 495-500.

Jüttner, U., H. Peck, and M. Christopher (2002), "Supply Chain Risk Management: Outlining an Agenda for Future Research, in Griffiths J., Hewitt, F. and Ireland, P. (eds)," *Proceedings of the Logistics Research Network 7th Annual Conference*, pp. 443-450.

Kagono, T., I. Nonaka, K. Sakakibara, and A. Okumura (1985), *Strategic vs. Evolutionary Management: A U.S.-Japan Comparison of Strategy and Organization*, North Holland, Elsevier Science Publishers B.V., Amsterdam.

Keller, Scott B., K. Savitskie, Theodore P. Stank, Daniel F. Lynch, and Alexander E. Ellinger (2002), "A Summary and Analysis of Multi-item Scales Used in Logistics Research," Journal of Business Logistics, Vol. 23, No. 2, pp. 83-281.

Kelley, L., A. Whatley, and R. Worthley (1987), "Assessing the Effects of Culture on Managerial Attitudes: A Three-Culture Test," *Journal of International Business Studies,* Vol. 18, No. 2, pp.17.

Kenny, D. A. (1979), *Correlation and Causality, New* York: Wiley.

Knight, F. H. (1921), *Risk, Uncertainty and Profit*, Houghton and Mifflin, Boston and New York.

Koch, R. (2004), "A Secure Supply Chain Blueprint," *Unisys White Paper Series.*

Langhoff, T., N. Pillai, and R. Koch (2005), "Secure Commerce Roadmap – The Industry's View for Securing Commerce," *Unisys Technical White Paper Series.*

Lawrence, M. (2006), "Middle East, Asia Drive Up Terrorism," *Security Management*, Vol. 50, No. 4, pp. 28.

Lee, H. L. (2004), "Supply Chain Security – Are You Ready?" *Stanford Global Supply Chain Management Forum*, September.

Lee, H. L. and M. Wolfe (2003), "Supply Chain Security Without Tears," *Supply Chain Management Review*, Vol. 7, No. 1, pp. 12-21.

Li, S., S. S. Rao, T. S. Ragu-Nathan, and B. Ragu-Nathan (2005), "Development and Validation of a Measurement Instrument for Studying Supply Chain Management Practices," *Journal of Operations Management*, Vol. 23, No. 6, pp. 618-641.

Lindlof, T. R. and B. C. Taylor (2002), *Qualitative Communication Research Methods*, Sage Publications.

Lissitz, R. W. and S. B. Green (1975), "Effect of the Number of Scale Points on Reliability: A Monte Carlo Approach," *Journal of Applied Psychology,* Vol. 60, pp. 10-13.

MacCallum, R. C. (1983), "A Comparison of Factor Analysis Programs in SPSS, BMDP, and SAS," *Psychometrika*, Vol. 48, pp. 223-231.

MacCallum, R. C., M. W. Browne and H. M. Sugawara (1996), "Power Analysis and Determination of Sample Size for Covariance Structural Modeling," *Psychol Methods*, Vol. 1, pp. 130-149.

MacCallum, R. C., K. F. Widaman, S. Zhang, and S. Hong (1999), "Sample Size in Factor Analysis," *Psychological Methods*, Vol. 4, pp. 84-89.

Malhotra, N. K. (2007), Marketing *Research: An Applied Orientation (5th Ed)*, Upper Saddle River, NJ: Prentice Hall.

Maloni, M. and W. C. Benton (2000), "Power Influences in the Supply Chain," *Journal of Business Logistics*, Vol. 21, No. 1, pp. 49-73.

Mason-Jones, R., B. Naylor, and D. Towill (2000), "Engineering the Agile Supply Chain," *International Journal of Agile Management Systems*, Vol. 2, No. 1, pp. 54-61.

Matear, S. and R. Gray (1993), "Factors Influencing Freight Service Choice for Shippers and Freight Suppliers," *International Journal of Physical Distribution & Logistics Management*, Vol. 23, No. 2, pp. 25.

Matsumoto, D. (1993), "Ethnic Differences in Affect Intensity, Emotion Judgments, Display Rule Attitudes, and Self-Reported Emotional Expression in an American Sample," *Motivation and Emotion,* Vol. 17, No. 2, pp. 107-123.

McCullagh, P. (1980), "Regression Models for Ordinal Data," Journal of Royal Statistical Society, Vol. 42, No. 2, pp. 109-142.

McGinnis, M. (1990), "The Relative Importance of Cost & Service in Freight Transportation Choice: Before and After Deregulation," *Transportation Journal*, Vol. 30, Fall 1990.

McGinnis, M., T. M. Corsi, and M. J. Roberts (1981), "A Multiple Criteria Analysis of Modal Choice," *Journal of Business Logistics*, Vol. 2, No. 2.

McQuitty, S. (2004), "Statistical Power and Structural Equation Models in Business Research," *Journal of Business Research*, Vol. 57, No. 2, pp. 175-183.

Menon, M. K., M. A. McGinnis, and K. B. Ackerman (1998), "Selection Criteria for Providers of Third Party Logistics Services: An Exploratory Study," *Journal of Business Logistics*, Vol. 19, No. 1, pp. 121.

Mentzer, J. T. and D. J. Flint (1997), "Validity in Logistics Research," *Journal of Business Logistics*, Vol. 18, No. 1, pp. 199-216.

Mentzer, J. T., D. J. Flint, and J. L. Kent (1999), "Developing a Logistics Service Quality Scale," *Journal of Business Logistics*, Vol. 20, No. 1, pp. 9-32.

Mentzer, J. T. and K. B. Kahn (1995), "A Framework of Logistics Research," *Journal of Business Logistics*, Vol. 16, No. 1, pp. 231-250.

Mentzer, J. T., B. P. Konrad (1991), "An Efficiency/Effectiveness Approach to Logistics Performance Analysis," *Journal of Business Logistics*, Vol. 12, No. 1, pp. 33.

Miller, G. A. (1956), "The Magical Number Seven, Plus or Minus Two: Some Limits on Our Capacity for Processing Information," *Psychological Review*, Vol. 63, No. 2, pp. 81-97.

Mol, T. (2002), "An Accident Theory that Ties Safety and Productivity Together," *Occupational Hazards*, Vol. 64, No. 10, pp. 89-93.

Mossman, F. H., P. Bankit, and O. K. Helferich (1977), *Logistics Systems Analysis*, Washington, D.C.: University Press of America.
Novack, R. A., L. M. Rinehart, and C. Langley, Jr. (1994), "An Internal Assessment of Logistics Value," *Journal of Business Logistics*, Vol. 15, No. 1, pp. 113.

Nunnally, J. C. (1976), *Psychometric Theory,* 2nd Ed., New York: McGraw-Hill.

Norrman, A. and R. Lindroth (2002), "Supply Chain Risk Management: Purchasers' vs Planners' Views on Sharing Capacity Investment Risks in the Telecom Industry," *Proceedings of the 11th International Annual IPSERA Conference, Twente University,* 25th -27th March, pp. 577-595.

Norrman, A. and R. Lindroth (2004), "Categorization of Supply Chain Risk and Risk Management," *Supply Chain Risk*, Aldershot, Hampshire, England, pp.14-27.

Page, P. (2006), "Port Security," *Traffic World*, Newark, September 18.

Parker, R. W. (2003), "Grading the Government," *The University of Chicago Law Review*, Vol. 70, No. 4, pp. 1345.

Paulsson, U. (2004), "Supply Chain Risk Management," *Supply Chain Risk*, Aldershot, Hampshire, England, pp.79-96.

Pearson, J. N. and J. Semeijn (1999), "Service Priorities in Small and large Firms Engaged in International Logistics," *International Journal of Physical Distribution & Logistics Management*, Vol. 29, No. 3, pp. 181.

Peleg-Gillai, B., G. Bhat, and L. Sept (2006), "Innovators in Supply Chain Security," *The Manufacturing Innovation Series*, The Manufacturing Institute.

Peter, J. P. (1979), "Reliability: A Review of Psychometric Basics and Recent Marketing Practices," *Journal of Marketing Research*, Vol. 16, February, pp. 6-17.

Piazza, P. (2006), "More Compliance, Less Security?" *Security Management*, Vol. 50, No. 6, pp. 50-52.

Preston, C. C. and A. M. Colman (2000), "Optimal Number of Response Categories in Rating Scales: Reliability, Validity, Discriminating Power, and Respondent Preferences," *Acta Psychologica*, Vol. 104, pp. 1-15.

Price, W. (2004), "Reducing the Risk of Terror Events at Seaports," *Review of Policy Research*, Vol. 21, No. 3, pp. 329.

Raghunathan, T. S., P. K. Bagchi, and E. J. Bardi (1988), "Motor Carrier Services: The U.S. Experience," *International Journal of Physical Distribution and Materials Management*, Vol. 18, No. 5, pp. 3-7.

Rascoff, S. J. and R. L. Revesz (2002), "The Biases of Risk Tradeoff Analysis: Towards Parity in Environment and Health-and-Safety Regulation," *The University of Chicago Review*, Vol. 69, No. 4, pp. 1763.

Rice, J. B. Jr. and P. W. Spayd (2005), "Investing in Supply Chain Security: Collateral Benefits," *IBM Center for the Business of Government*, Special Report Series.

Ritchie, B. and C. Brindley (2004), "Risk Characteristics of the Supply Chain – A Contingency Framework," *Supply Chain Risk*, Aldershot, Hampshire, England, pp. 28-42.

Roznowski, M. (1989), "Examination of the Measurement Properties of the Job Descriptive Index with Experimental Items," *Journal of Applied Psychology,* Vol. 74, pp. 805-814.

Russell, D. M. and J. P. Saldanha (2003), "Five Tenets of Security-Aware Logistics and Supply Chain Operation," *Transportation Journal*, Vol. 42, No. 4, pp. 44-54.

Sallivan, J. and I. Nonaka (1988), "Culture and Strategic Issue Categorization Theory," *Management International Review*, Vol. 28, No. 3, pp. 6-10.

Savalei, V. and P. Bentler (2006), "Structural Equation Modeling," *The Handbook of Marketing Research: Uses, Misuses and Future Advances*, Sage Publications, pp. 330-364.

Schmitt, N. W. and D. M. Stults (1985), "Factors Defined by Negatively Keyed Items: The Results of Careless Respondents?" *Applied Psychological Measurement,* Vol. 9, pp. 367-373.

Schneider, S. C. and A. D. Meyer (1991), "Interpreting and Responding to Strategic Issues: The Impact," *Strategic Management Journal,* Vol. 12, No. 4, pp. 307.

Schriesheim, C. A. and R. J. Eisenbach (1991), "Item Wording Effects on Exploratory Factor-Analytic Results: An Experimental Investigation," *Proceedings of the 1990 Southern Management Association Annual meetings*, pp. 396-398.

Sharma, A. and D. M. Lambert (1990), "Segmentation of Markets Based on Customer Service," *International Journal of Physical Distribution and Logistics Management*, Vol. 20, No. 7, pp. 19-27.

Shaw, M. E., and J. M. Wright (1967), *Scales for the Measurement of Attitudes,* New York: McGraw-Hill.

Sheffi, Y. (2001), "Supply Chain Management Under the Threat of International Terrorism," *The International Journal of Logistics Management*, Vol. 12, No. 2, pp. 1-11.

Sheu, C., L. Lee, and B. Niehoff (2006), "A Voluntary Logistics Security Program and International Supply Chain Partnership," *Supply Chain Management: An International Journal*, Vol. 11, No. 4, pp. 363-374.

Smart and Secure Tradelanes (2003), *Phase One Review, Network Visibility: Leveraging Security and Efficiency in Today's Global Supply Chains*, November.

Sommer, T. (2006), "Supply Chain Security Proposal Will Cripple Businesses," *Financial Times*, London (UK), September 4.

Stank, T. P. and C. W. Lackey, Jr. (1997), "Enhancing Performance Through Logistical Capabilities in Mexican Maquiladora," *Journal of Business Logistics,* Vol. 18, No. 1, pp. 91.

Stank, T. P., S. B. Keller, and P. J. Daugherty (2001), "Supply Chain Collaboration & Logistical Service Performance," *Journal of Business Logistics*, Vol. 22, No. 1, pp. 29.

Sterling, J. U. and D. M. Lambert (1987), "Establishing Customer Service Strategies Within the Marketing Mix," *Journal of Business Logistics*, Vol. 8, No. 1, pp. 1.

Supply Chain Council (2006), "*Supply-Chain Operations Reference-model,*" Version 8.0.

Towill, D. R. and M. Christopher (2003), "The Supply Chain Strategy Conundrum: To Be Lean or Agile or To Be Lean and Agile," *Supply Chain Practice*, Vol. 5, No. 2, pp. 30-44.

U.S. Customs and Border Protection (CPB) (2006), "Supply Chain Security Best Practices Catalog," *http://www.cpb.com.*

Velicer, W. F. and Fava, J. L. (1998), "Effects of Variable and Subject Sampling on Factor Pattern Recovery," *Psychological Methods*, Vol. 3, pp. 231–251.

Viscusi, W. K. and T. Gayer (2002), "Safety at Any Price?" *Regulation*, Vol. 25, No. 3, pp. 54-63.

Warren, F. (1992), *Introduction in: Royal Society Study Group, Risk Analysis, Perception and Management*, The Royal Society, London.

Weiss, D. (1976), *Multivariate Procedures, In M. D. Dunnete (Ed.), Handbook of Industrial/Organizational Psychology*, Chicago, IL: Rand McNally.

Willis, H. H. and D. S. Ortiz (2004), "Evaluating the Security of the Global Containerized Supply Chain," *RAND Technical Report Series.*

Wisner, J. D. (2003), "A Structural Equation Model of Supply Chain Management Strategies and Firm Performance," *Journal of Business Logistics*, Vol. 24, No. 1, pp. 1-26.

Wolpert, J. (1980), "The Dignity of Risk," *Transactions of the Institute of British Geographers,* New Series, Vol. 5, No. 4, pp. 391.

Worthen, B. (2006), "Customs Rattles the Supply Chain: The Government Wants You to Secure Your Supply Chain," *The CIO*, Vol. 19, No. 10, pp. 1.

Zedillo, E. (2006), "Nuclear Attack – The Worst Threat," *Forbes*, Vol. 177, No. 1, pp. 29.

APPENDIX A

Field Interview Questionnaires

FIELD INTERVIEW QUESTIONAIRE
DRIVING BUSINESS VALUE THROUGH SUPPLY CHAIN SECURITY

This interview is conducted as a part of the Masters' research thesis at the Sauder School of Business, University of British Columbia, Canada. The study aims to identify the best practices and key performance measurements used in securing the marine container supply chain

All information obtained from this interview is regarded as confidential and will be used solely for the purpose of this study only. Your kind cooperation will be highly appreciated.

PART A - INTERVIEWEE & ORGANIZATION INFORMATION

Date of Interview: _____

Name of Organization: _____

Name of Person Interviewed: _____

Designation & Responsibilities:

_____

A1. What is your organization type?

- ❑ Port Authority
- ❑ Terminal Operators
- ❑ Customs Authority
- ❑ Customs Broker
- ❑ Freight Consolidator
- ❑ Freight Forwarder
- ❑ Exporter (Shipper)
- ❑ Buyer (Importer)
- ❑ 3rd Party Logistics Provider
- ❑ Trucking / Intermodal Company
- ❑ Ocean Carrier
- ❑ Others Please indicate: _____

A2. What is(are) your organization's main trade route(s)? Tick all that is applicable.

- ❑ Intra Asia (Incl. Indian sub-continent and Australasia)
- ❑ Intra Americas
- ❑ Intra Europe
- ❑ Trans Pacific (Asia-North America)
- ❑ Trans Pacific (Asia-South America)
- ❑ Trans Pacific (North America-Asia)
- ❑ Trans Pacific (South America-Asia)
- ❑ Asia Europe (Asia-Europe)
- ❑ Trans Atlantic (North America-Europe)
- ❑ Trans Atlantic (South America-Europe)
- ❑ Asia Europe (Europe-Asia)
- ❑ Trans Atlantic (Europe-North America)
- ❑ Trans Atlantic (Europe-South America)
- ❑ Asia Middle East/Africa (Asia-ME/Africa)
- ❑ N.A. Middle East/Africa (N.A.-ME/Africa)
- ❑ Europe Middle East/Africa (EU-ME/Africa)
- ❑ Asia Middle East/Africa (ME/Africa-Asia)
- ❑ N.A. Middle East/Africa (ME/Africa-N.A.)
- ❑ N.A. Middle East/Africa (ME/Africa-EU.)
- ❑ Others. Please indicate: _____

A3. What is your organization's annual revenue for 2005 (in US$)?

- ❑ less than US$20 million
- ❑ US$20 million to US$100 million
- ❑ US$100 million to US$500 million
- ❑ US$500 million to US$1 billion
- ❑ more than US$1 billion
- Estimate: _____

A4. How many employees are there in your organization globally?

- ❑ less than 100
- ❑ 100 to 500
- ❑ 500 to 1,000
- ❑ 1,000 to 5,000
- ❑ more than 5,000
- Estimate: _____

A5. What is your scope of control or influence over your supply chain?

Aspects of Supply Chain	Not Controlled	In-house	Outsourced
Choice of suppliers (i.e. manufacturers)			
Trucking / other inter-modal move from factory to origin port			
Warehousing / freight consolidation at origin			
Customs clearance at origin			
Choice of port of loading			
Choice of terminal at origin			
Choice of carriers (i.e. freight contracts)			
Choice of port of destination			
Choice of terminal at destination			
Customs clearance at destination			
Warehousing / freight deconsolidation at destination			
Trucking / other inter-modal move to final destination			

For Shippers Only

A6. Do you see supply chain management as a competitive advantage for your business?

❑ Yes ❑ No

If yes, what is your organization's logistics and supply chain strategy or value proposition?

- ❑ Efficiency / Cost of fulfillment
- ❑ Timeliness of product and service delivery
- ❑ Responsiveness to customer needs (Flexibility)
- ❑ Availability of products and services (e.g. minimum backorders, maximum fill rates)
- ❑ Reliability of operations (e.g. accuracy and recovery from disruptions)
- ❑ Others. Please indicate: _____

If no, what is your organization's value proposition? That is, what (e.g. research and development, marketing) gives your business the competitive edge over your competitors?

For Service Providers Only

A6. What is your organization's value proposition to your customers?

PART B - SUPPLY CHAIN PERFORMANCE

Note: Please respond to the following questions based on the scope of the supply chain that your company has control over or assumes responsibility for. This is established in A5.

B1. What KPIs does your company use to evaluate the performance of your supply chain operations? And how would you rate your performance in each of them relative to competition?

Prompts: E.g., what KPIs do you use to measure performance in terms of efficiency, reliability of service, responsiveness to customers' needs, ensuring availability of products /services and timeliness of product/service delivery?

Performance Measurements	Rating
Efficiency performance ...	Poor 1 2 3 4 5 Excellent
	Poor 1 2 3 4 5 Excellent
Timeliness performance ...	Poor 1 2 3 4 5 Excellent
	Poor 1 2 3 4 5 Excellent
Responsiveness performance ...	Poor 1 2 3 4 5 Excellent
	Poor 1 2 3 4 5 Excellent
Availability of products & services performance ...	Poor 1 2 3 4 5 Excellent
	Poor 1 2 3 4 5 Excellent
Reliability of operations performance ...	Poor 1 2 3 4 5 Excellent
	Poor 1 2 3 4 5 Excellent

Note : If you need more space, please do not hesitate to use a separate sheet of paper.

B2. Is there an overall measure(s) that you use to measure supply chain performance?

❑ Yes ❑ No

If yes, please indicate what this measure(s) is and how would you rate your performance? If this overall measure has already been identified above, please mark it with "*".

Overall Supply Chain Performance Measurement	Rating
	Poor 1 2 3 4 5 Excellent

PART C – SUPPLY CHAIN SECURITY PERFORMANCE

C1. Is ensuring security in your supply chain important to you?

- ❑ Extremely important. Go to Question C2.
- ❑ Very important. Go to Question C2.
- ❑ Quite important. Go to Question C2.
- ❑ Not so important. Go to Question C2.
- ❑ Not at all. Go to Question C3.

C2. How do you think each of the aspects of supply chain performance contribute to overall supply chain performance?

Supply Chain Performance Aspect	Not at all	Relatively insignificant	Not sure	Relatively substantial	Very substantial
Responsiveness/Flexibility					
Timeliness					
Efficiency					
Resiliency/ Availability					
Reliability					
Security					

C3. What KPIs does your company use to evaluate the security performance of your supply chain? And how would you rate your performance in each of them?

Performance Measurements	Rating
	Poor — Excellent 1 2 3 4 5

Note : If you need more space, please do not hesitate to use a separate sheet of paper.

C4. Is there an overall measure that you use to measure supply chain security performance? If there is, please indicate what this measure is and how would you rate your performance?

❑ Yes ❑ No

If there is, please indicate what this measure is and how would you rate your performance? If this overall measure has already been identified above, please mark it with "*".

Overall Security Performance Measurement	Rating
	Poor — Excellent 1 2 3 4 5

PART D – SUPPLY CHAIN SECURITY INITIATIVES

D1. Has your organization made any investments (past and present) or planning to make investments in security-related initiatives such as applying for CT-PAT certification, deploying tracking systems and more stringent personnel checks and organizational changes etc. to ensure your shipments, personnel and infrastructure are secured?

❑ Yes ❑ No

If yes, what are they? And please indicate if they were made before or after 9/11.

B = Before 9/11 A = After 9/11 F = Future

Check: 1 very low impact, 3 average impact, 5 very high impact

Supply Chain Security Initiatives	B	A	F	Impact on Security Performance						Impact on Supply Chain Performance					
				1	2	3	4	5	NA	1	2	3	4	5	NA
Business Partner Requirements Such as ... ❑ Require certification such as C-TPAT ❑ Contractual obligations ❑ Audits and compliance manuals for partners ❑ Collaboration ❑ Partner selection procedures ❑ Customer outreach ❑ Others: _____															
Container/Trailer/ Unit Load Device Security Such as ... ❑ Inspections ❑ Seals ❑ Tracking ❑ Inventory/storage practices ❑ Others: _____															
Conveyance Security Such as ... ❑ En-route inspections ❑ Parking assignment ❑ Monitoring / Security escorts ❑ Route design ❑ Spot checks ❑ Others: _____															

Physical Access Controls Such as ... ❑ Biometric technology ❑ Monitoring access patterns ❑ Restricting access to certain areas ❑ Multiple check points ❑ Visitor pre-clearance ❑ Driver waiting area ❑ Escalation matrix ❑ Others: _____																
Personnel Security Such as ... ❑ Pre-employment background checks ❑ Termination procedures ❑ Code of conduct ❑ Others: _____																
Procedural Security Such as ... ❑ Written procedures ❑ Measuring and monitoring incidents ❑ Protect/control use of company stationery ❑ RFID / EDI ❑ Staff rotation ❑ Others: _____																
Security Training Such as ... ❑ Awareness ❑ Outreach ❑ Incentives ❑ Incident reporting ❑ Others: _____																

Physical Security Such as ... ❑ Fencing / Gates ❑ Security guards and patrol ❑ Locking mechanisms ❑ Lighting ❑ Surveillance ❑ Others: _____															
IT Security Such as ... ❑ Internal access restrictions ❑ External access restrictions ❑ User / usage policies and procedures ❑ Recovery plans ❑ Others: _____															

If no, please indicate the reason(s) why.

D2. How is your ability to secure the supply chain in your part of the process affected by actions of your upstream and downstream supply chain partners?

D3. How can you or do you impact the ability of your upstream and downstream partners to secure the supply chain?

实地考察面谈问卷
通过供应链的保安推动企业价值

这次的面谈会是做为加拿大卑诗哥伦比亚大学，运输经济学与物流硕士学位科研论文的一部分而举行的。这个研究的主要目的在于寻找并设定一套广泛认可并有助于企业考核贵司在供应连保安方面的表现的考核指标。

通过这次面谈所取得的信息将受到严格的保密，且仅用于这个研究项目之用。在此敬谢您热心的配合与合作。

A. 受访者与受访企业的信息

面谈日期：
企业名字：
受访者姓名：

职衔与职务：

A1.请问贵司的企业类别是?

- ❑ 港务局
- ❑ 海港总站调度员
- ❑ 海关总署
- ❑ 海关代理人
- ❑ 货物混载业者
- ❑ 货物运输业者
- ❑ 出口商
- ❑ 进口商
- ❑ 第三方物流供应商
- ❑ 承运商/运输公司
- ❑ 海洋运输载体
- ❑ 其他 ：请说明 _____

A2.请问以下哪些是贵司的主要航线？请打勾。

- ❑ 亚洲内部（包括印度和南太平洋洲）
- ❑ 美国内部
- ❑ 欧洲内部
- ❑ 跨太平洋（亚洲至北美洲）
- ❑ 跨太平洋（北美洲至亚洲）
- ❑ 跨太平洋（亚洲至南美洲）
- ❑ 跨太平洋（南美洲至亚洲）
- ❑ 亚欧（亚洲至欧洲）
- ❑ 亚欧（欧洲至亚洲）
- ❑ 跨大西洋(北美洲至欧洲)
- ❑ 跨大西洋(欧洲至北美洲)
- ❑ 跨大西洋(南美洲至欧洲)
- ❑ 跨大西洋(欧洲至南美洲)
- ❑ 亚洲至中东/非洲
- ❑ 中东/非洲至亚洲
- ❑ 北美至中东/非洲
- ❑ 中东/非洲至北美
- ❑ 欧洲至中东/非洲
- ❑ 中东/非洲至欧洲
- ❑ 其他，请说明_____

A3. 请问贵司2005年的营业额（美金）有多少？请估计或在以下的选项选择。

- ❑ 少于2,000万美金
- ❑ 介于2,000万到1亿美金
- ❑ 介于1亿到5亿美金
- ❑ 介于5亿到10亿美金
- ❑ 多于10亿美金
- 估计：_____

A4. 请问贵司的规模（员工数量)有多大？？请估计或在以下的选项选择。

- ❑ 少于100
- ❑ 介于100到500
- ❑ 介于500到1,000
- ❑ 介于1,000到5,000
- ❑ 多于5,000
- 估计：_____

A5. 请问贵司对于自身供应链的影响力有多大，控制的范围有多广？

供应链的不同方面	不在控制范围以内	内部运作	外包
供应商的选择 （e.g. 制造商）			
从工厂陆运或以其他的运输方式运载到起发地港口			
起发地的仓储/货物混载			
起发地港口的清关			
装货港口的选择			
起发地海港总站的选择			
运输载体的选择（i.e.货物运输合约）			
目的地港口的选择			
目的地海港总站的选择			
目的地的清关			
目的地的仓储/货物分拣			
从目的地港口陆运或以其他的运输方式运载到最终目的地			

进/出口商：

A6. 您认为物流和供应链管理是否是贵司的竞争优势？

- ❑ 是
- ❑ 不是

若以上答案是“是“，请问贵司的物流和供应链策略或价值是什么？

- ❑ 效率
- ❑ 货物配送/服务准时性
- ❑ 对於客户要求的反映能力，速度/应变能力
- ❑ 货物/服务的可及性
- ❑ 运作的可靠性（例如，运作在受到影响后恢复的速度和准角度）。
- ❑ 其他。请说明：_____

若以上答案是“不是“，请问贵司的价值是什么呢？换句话说，贵司在哪一些其他方面具有突出的竞争力。

物流服务供应商：

A6.请问贵司给于您的客户的价值是什么？

B. 供应链的表现

注：请您按照贵司对自身供应链拥有控制权或需履行责任的范围，并以列明在A5的项目，回复以下问题。

B1. 请问贵司有哪些用于考核贵司在供应链运作方面表现的指标?
与其他竞争对手相比，您会如何评估贵司在供应链方面的表现呢？

提示：例如，贵司利用哪些考核指标来评估贵司在供应链运作方面，例如效率，服务的可靠性，对于客户需求的反应能力和速度，如何确保货物/服务的可及性以及货物/服务准时送达目的地方面的表现？

考核指标	评估标准
效率方面的表现	差 1 2 3 4 5 极佳
	差 1 2 3 4 5 极佳
准时性方面的表现	差 1 2 3 4 5 极佳
	差 1 2 3 4 5 极佳
反应能力和速度方面的表现	差 1 2 3 4 5 极佳
	差 1 2 3 4 5 极佳
货物/服务可及性的表现	差 1 2 3 4 5 极佳
	差 1 2 3 4 5 极佳
运作可靠性方面的表现	差 1 2 3 4 5 极佳
	差 1 2 3 4 5 极佳

注：若您需要多一些空间做答，请使用另一页纸。

B2. 请问贵司是否拥有一个用于考核贵司供应链方面的表现的整体考核指标吗？
❑ 有 ❑ 没有

若有，请列明此考核指标以及贵司如何评估您的表现。若这个考核指标已列明在上述问题答案，请表上 “*”。

整体的供应链考核指标	评估标准
	差 极佳 1 2 3 4 5

C. 供应链保安方面的表现

C1.请问贵司是否认为确保贵司的供应链拥有一定的保安措施是重要的呢?

- ❑ 非常重要。请继续回答问题 C2.
- ❑ 很重要。请继续回答问题 C2.
- ❑ 相当重要。请继续回答问题 C2.
- ❑ 不是很重要。请继续回答问题 C2.
- ❑ 根本不重要。请继续回答问题 C3.

C2.请问您认为以下各供应链方面的表现对于整体的供应链起着什么样的影响呢?

供应链的不同方面	完全没有影响	相当小的影响	不肯定	相当大的影响	非常大的影响
对于客户需求的反应能力，速度/应变能力方面的表现					
准时性					
效率					
可及性					
可靠性					
保安					

C3.请问贵司有哪些用于考核贵司在供应链保安方面的表现的指标?
请问贵司如何评估贵司在各方面的表现呢?

考核指标	评估标准
	差 极佳 1 2 3 4 5
	差 极佳 1 2 3 4 5

注：若您需要多一些空间做答，请使用另一页纸。

C4.请问贵司是否拥有一个用于考核贵司供应链保安方面的表现的整体考核指标吗?

❑ 有 ❑ 没有

若有，请列明此考核指标以及贵司如何评估您的表现。若这个考核指标已列明在上述问题答案，请表上 “*”。

整体的供应链保安考核指标	评估标准
	差 极佳 1 2 3 4 5

D. 供应链的保安措施

D1. 请问贵司近期是否有在实施保安措施方面做出任何投资或打算在这方面进行投资呢?如申请和准备CT-PAT证书的考核，推行智能运输追 踪系统如GPS等以及实施更严格的检查措施等，以便去确保贵司在货物，人员和基础设施的安全? 若有，请列明。

❑ 有　　❑ 没有

若有，请问有哪些并列明这些措施是否是在911事件之前还是之后实施的。

B = 911事件之前　A = 911事件之后　　F = 未来　　检查: 1 = 很小的冲击/影响, 3 = 中等的冲击/影响, 5 = 很大的冲击/影响

供应链的保安措施	B	A	F	对于供应链保安表现的冲击/影响						对于供应链表现的冲击/影响					
				1	2	3	4	5	NA	1	2	3	4	5	NA
商业伙伴的需求　　如… ❑ 证书需求如CT-PAT证书 ❑ 契约义务 ❑ 审计和给与合作伙伴的条例遵守指南 ❑ 合作 ❑ 伙伴选择程序 ❑ 客户沟通与联系 ❑ 其他: _____															
集装箱/拖车等保安措施　　如… ❑ 安检系统/程序 ❑ 格式锁 ❑ 追踪系统/程序 ❑ 库存运作 ❑ 其他 _____															

搬运器与沿途的保安　　如… ❑ 运输途中的安检 ❑ 停泊位置安排 ❑ 监视/保安随从 ❑ 运输路线设计 / 突击检查 ❑ 其他 _____																
设施出入控制措施　　如… ❑ 生物科技 ❑ 监视出入情况 / 禁止出入某些地方 ❑ 竖立多个检查站 ❑ 访客安检 / 司机等候处 ❑ 上级申报程序 ❑ 其他 _____																
人员方面的保安措施　　如… ❑ 聘用前的背景调查 ❑ 终止聘用程序 ❑ 品行规范 ❑ 其他 _____																
程序方面的保安措施　　如… ❑ 拟写的程序 ❑ 考核和监视事件 ❑ 保护/控制公司内文具的利用 ❑ RFID / EDI ❑ 人员调动 ❑ 其他 _____																

保安培训　　如… ❑ 意识 ❑ 奖励 ❑ 事故报告程序 ❑ 其他 _____																
基础设施的保安　　如… ❑ 围栏/门 ❑ 保安人员和巡逻程序 ❑ 保安锁的机制 ❑ 灯光 ❑ 监控设施 ❑ 其他 _____																
保安措施　　如… ❑ 内部使用的限制 ❑ 对外使用的限制 ❑ 用户/用法的条例和程序 ❑ 救方案 ❑ 其他 _____																

若没有，请列明原因。

D2. 请问贵司的供应链合作伙伴如何影响您确保自身供应链方面的安全呢？

D3. 请问贵司如何影响您的供应链伙伴一同确保整个供应链的安全呢？

APPENDIX B

Web Survey Questionnaires

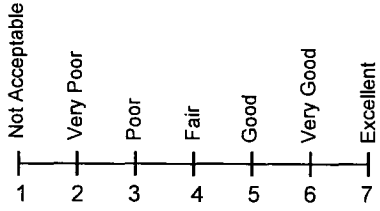
*** SHIPPER ***
ENGLISH VERSION

Section A. Self Performance Appraisal

A1. For the following survey, are you answering the questions for your entire firm or for your division/strategic business unit?

❑ Entire firm ❑ My division or strategic business unit (SBU)

Score / Rating

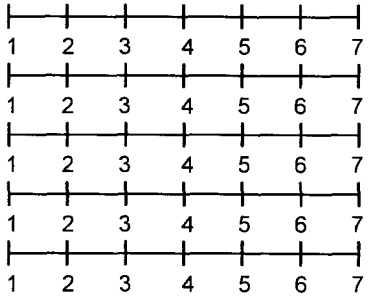


A2. On a scale of 1 to 7 where [1=Not Acceptable and 7=Excellent], please rate how secure you think your supply chain is.

(Secure as in the probability of your supply chain being compromised in terms of pilferages, thefts, damages, terrorism and other crimes such as smuggling, contraband etc.)

A3. On a scale of 1 to 7 where [1=Not Acceptable and 7=Excellent], please rate how well you think your logistics/supply chain operations are performing in the following aspects.

1. Efficiency (including cost of fulfillment, productivity)
2. Timeliness of product delivery (including speed and on-time performance)
3. Reliability of operations (including accuracy and recovery from disruptions)
4. Availability of products
5. Responsiveness to customers' needs (including flexibility and agility)



Section B. Organization Profiling

B1. To what main industrial sector does your organization belong? (Check all that apply).

❑ Buyer (Importer) ❑ Shipper (Exporter) ❑ Others, please specify: _____

B2. What supply chain(s) does your organization belong to? (Check all that apply).

- ❑ Fast Moving Consumer Goods (FMCG)
- ❑ Automotive
- ❑ Heavy Machinery
- ❑ Electronics / High Tech Products
- ❑ Pharmaceuticals
- ❑ Aerospace
- ❑ Perishables / Food Products
- ❑ Chemicals
- ❑ Others, please specify: _____

B3. Does your organization handle hazardous cargo?

- ❑ No
- ❑ Yes, what _____ %

B4. Does your organization ship full container loads?

- ❑ No
- ❑ Yes, what _____ %

B5. What is(are) your organization's main trade route(s)? (Check no more than 3).

- ❑ Intra Asia
- ❑ Intra Americas (within N.A. and S.A.)
- ❑ Intra Europe

- ❑ Trans Pacific (Asia → N.A.)
- ❑ Trans Pacific (Asia → S.A.)
- ❑ Trans Pacific (N.A. → Asia)
- ❑ Trans Pacific (S.A. → Asia)

- ❑ Asia Europe (Asia → Europe)
- ❑ Trans Atlantic (N.A. → Europe)
- ❑ Trans Atlantic (S.A. → Europe)
- ❑ Asia Europe (Europe → Asia)
- ❑ Trans Atlantic (Europe → N.A.)
- ❑ Trans Atlantic (Europe → S.A.)

- ❑ Asia → Middle East/Africa
- ❑ N.A. → Middle East/Africa
- ❑ S.A. → Middle East/Africa
- ❑ Europe → Middle East/Africa
- ❑ Middle East/Africa → Asia
- ❑ Middle East/Africa → N.A.
- ❑ Middle East/Africa → S.A.
- ❑ Middle East/Africa → Europe

- ❑ Others. please specify: _____

Legend : *N.A.: North America and Central America (includes Panama and all countries north of Pananma)*
S.A.: South America (all countries south of Panama)

B6. What is your organization's annual revenue for 2005 (in US$)? Please select a range from below.

- ❑ less than US$20 million
- ❑ US$20 million to US$100 million
- ❑ US$100 million to US$500 million
- ❑ US$500 million to US$1 billion
- ❑ more than US$1 billion

B7. Which of the following supply chain activities do you directly select/make final decisions for?
Please indicate "X" under "Make Final Decisions" column against each activity that you select/make final decision for.
Please indicate "X" under "Outsource Final Decision Making" column against each activity that you do not make final decision for.
For those activities that are not applicable to your organization, please indicate "X" under the "Not Applicable" column.

Aspects of Supply Chain	Outsource Final Decision Making	Make Final Decisions In-house	Not Applicable
Choice of suppliers (e.g. manufacturers)			
Trucking or other inter-modal transportation from factory to origin port			
Warehousing at origin			
Freight consolidation at origin			
Customs clearance at origin			
Cross-border trucking to origin port or final destination (if required)			
Choice of port of loading			
Choice of terminal at origin			
Choice of carriers (i.e. freight contracts)			
Choice of port of destination			
Choice of terminal at destination			
Customs clearance at destination			
Cross-border trucking from destination port to final destination (if required)			
Warehousing at destination			
Freight deconsolidation / break bulk at destination			
Trucking or other inter-modal transportation to final location at destination			

B8. If your organization considers supply chain management as part of your business value proposition/competitive advantage, please indicate the strategic importance of the following supply chain drivers for your organization. [1=Not at all Important, 2=Slightly Important, 3=Somewhat Important, 4=Moderately Important, 5=Important, 6=Very Important, 7=Extremely Important].

Supply Chain Drivers	Not Important ... Somewhat Important ... Very Important
1. Efficiency (including cost of fulfillment, productivity)	1 2 3 4 5 6 7
2. Timeliness of product delivery (including speed and on-time performance)	1 2 3 4 5 6 7
3. Reliability of operations (including accuracy and recovery from disruptions)	1 2 3 4 5 6 7
4. Availability of products	1 2 3 4 5 6 7
5. Responsiveness to customers' needs (including flexibility and agility)	1 2 3 4 5 6 7
6. Security	1 2 3 4 5 6 7

Section C. Key Performance Indicators (KPIs)

C1. In your opinion, should there be KPIs for security performance/efforts?

❑ Yes ❑ No ❑ Unsure/Undecided

C2. Next, using a 3-point scale: [1=Inappropriate, 2=Indifferent/Unsure, 3=Appropriate], please indicate under the relevant "Appropriateness" scales, the degree to which you think that each KPI below is an appropriate indicator for Supply Chain Performance and Security Performance.

Key Performance Indicators (KPI)	Appropriateness For Supply Chain Performance: Inappropriate Indifferent Appropriate	Appropriateness For Security Performance: Inappropriate Indifferent Appropriate
1. Asset utilization (e.g. production capacity, containers, trucks).	1 2 3	1 2 3
2. Results from a random security audit.	1 2 3	1 2 3
3. Operations efficiency (e.g. labour productivity, cases picked per hour).	1 2 3	1 2 3
4. Number of security policy violations.	1 2 3	1 2 3

Key Performance Indicators (KPI)	Appropriateness For Supply Chain Performance	Appropriateness For Security Performance
5. Level of insurance premiums for cargo and/or operations.	Inappropriate Indifferent Appropriate 1 2 3	Inappropriate Indifferent Appropriate 1 2 3
6. Level of inventory (in warehouses or in pipeline).	1 2 3	1 2 3
7. Number/frequency of customs inspections.	1 2 3	1 2 3
8. Logistics costs as a percentage (%) of sales or per product unit.	1 2 3	1 2 3
9. On-time transmission of shipment information.	1 2 3	1 2 3
10. Number of unauthorized entry incidents.	1 2 3	1 2 3
11. Order fulfillment lead times (e.g. order-to-cash cycle time).	1 2 3	1 2 3
12. On-time delivery (e.g. % on-time order delivery, information transmission).	1 2 3	1 2 3
13. Length of time to deliver expedited orders.	1 2 3	1 2 3
14. Customs clearance lead-time (import and/or export).	1 2 3	1 2 3
15. Accuracy rate of shipment information (e.g. manifest transmission).	1 2 3	1 2 3
16. Number/frequency of service errors and failures.	1 2 3	1 2 3
17. Results from periodic safety audit.	1 2 3	1 2 3
18. Accuracy rate of inventory records (e.g. cycle counting variance).	1 2 3	1 2 3
19. Accuracy rate of invoicing.	1 2 3	1 2 3
20. Number/frequency of pilferage/theft/security incidents.	1 2 3	1 2 3
21. Amount of freight claims and/or freight loss (in monetary terms).	1 2 3	1 2 3
22. Number/frequency of personnel safety accidents.	1 2 3	1 2 3
23. Amount/frequency of overages, shortages and damages (OS&D).	1 2 3	1 2 3

Key Performance Indicators (KPI)	Appropriateness For Supply Chain Performance	Appropriateness For Security Performance
	Inappropriate Indifferent Appropriate 1 2 3	Inappropriate Indifferent Appropriate 1 2 3
24. Amount/frequency of operations deviations (e.g. capacity deviations).	1 2 3	1 2 3
25. Number/frequency of back orders.	1 2 3	1 2 3
26. Number/frequency of order cancellations/ rejections.	1 2 3	1 2 3
27. Average time taken to respond to client problems.	1 2 3	1 2 3
28. Average time taken to resolve client problems.	1 2 3	1 2 3
29. Results from customer service satisfaction / feedback survey.	1 2 3	1 2 3
30. Order fill rate.	1 2 3	1 2 3
31. Number and type of special requests satisfied.	1 2 3	1 2 3
32. Number and type of customer complaints resolved.	1 2 3	1 2 3
33. Others:	1 2 3	1 2 3
34. Others:	1 2 3	1 2 3
35. Others:	1 2 3	1 2 3

Section D. Supply Chain Security Initiatives

For each type/group of security initiative below, please indicate whether your organization is currently Implementing / Implemented (I), Planning to implement (P) or Not implementing (N) that initiative.

Also, for each initiative currently Implementing / Implemented (I) or Planning to Implement (P), please indicate under "Impact on Supply Chain Performance", how the initiative has impacted or will impact your supply chain performance, using a 7-point scale: [1=Extremely Negative, 2=Very Negative, 3=Moderately Negative, 4=Unsure/Neutral, 5=Moderately Positive, 6=Very Positive, 7=Extremely Positive].

Security Initiatives	Implementation Status	Impact on Supply Chain Performance
		Extremely Negative / Very Negative / Moderately Negative / Unsure / Neutral / Moderately Positive / Very Positive / Extremely Positive (1 2 3 4 5 6 7)
1. Operations/Security Related Certifications. Internationally recognized certifications for operations excellence including security and risk assessment.	I P N	Efficiency: 1 2 3 4 5 6 7
		Timeliness: 1 2 3 4 5 6 7
Examples:-		Reliability: 1 2 3 4 5 6 7
• Customs-Trade Partnership Against Terrorism (C-TPAT) (U.S.).		Availability: 1 2 3 4 5 6 7
• Partners-In-Protection (PIP) (Canada).		Responsiveness: 1 2 3 4 5 6 7
• Secure-Trade-Partnership (STP) (Singapore).		Security: 1 2 3 4 5 6 7
• Free and Secure Trade (FAST) (U.S. and Canada).		
• Transported Asset Protection Association (TAPA).		
• International Ship and Port Facility Security (ISPS).		
2. Advanced Data. Compliance to data submission programs through secure information transmission technology.	I P N	Efficiency: 1 2 3 4 5 6 7
		Timeliness: 1 2 3 4 5 6 7
Examples:-		Reliability: 1 2 3 4 5 6 7
• 24-hours Advance Manifest Rule & Automated Commercial Environment (ACE) (U.S.).		Availability: 1 2 3 4 5 6 7
• Advanced Commercial Information (ACI) (Canada).		Responsiveness: 1 2 3 4 5 6 7
• Traceable/secure electronic data transmissions.		Security: 1 2 3 4 5 6 7
• Advanced shipping notices (ASNs).		

Security Initiatives	Implementation Status	Impact on Supply Chain Performance
		Extremely Negative / Very Negative / Moderately Negative / Unsure / Neutral / Quite Positive / Moderately Positive / Extremely Positive (1 2 3 4 5 6 7)
3. Business Partners Requirements.		
Working with business partners to ensure security measures are in place and adhered to.	I P N	Efficiency: 1 2 3 4 5 6 7
		Timeliness: 1 2 3 4 5 6 7
Examples:-		Reliability: 1 2 3 4 5 6 7
Towards Manufacturer/Supplier/Vendor		Availability: 1 2 3 4 5 6 7
• Contractual obligations.		Responsiveness: 1 2 3 4 5 6 7
• Factory certification requirements.		Security: 1 2 3 4 5 6 7
• Supplier code of conduct.		
Towards Service Provider		
• Representative at overseas office.		
• Prohibit subcontracting.		
• Require background clearances for personnel.		
• Contractual obligations/procedures for selection.		
Towards Customer		
• Prevent misuse of products through education.		
• Verify business references, credit checks.		
• Establish routine pickup/drop-off points.		
4. Security Training & Outreach Programs.	I P N	Efficiency: 1 2 3 4 5 6 7
		Timeliness: 1 2 3 4 5 6 7
Examples:-		Reliability: 1 2 3 4 5 6 7
• Use alert levels		Availability: 1 2 3 4 5 6 7
• Communicate terrorism information to employees.		Responsiveness: 1 2 3 4 5 6 7
• Periodic training, specialized training in handling breaches, conducting investigations, inspections etc.		Security: 1 2 3 4 5 6 7
• Train business partners.		
• Provide incentives for incident reporting.		
• Collaborate with local law enforcement.		

Security Initiatives	Implementation Status	Impact on Supply Chain Performance
		Extremely Negative (1) · Very Negative (2) · Moderately Negative (3) · Unsure / Neutral (4) · Quite Positive (5) · Moderately Positive (6) · Extremely Positive (7)
5. Procedural Security. Incorporate security into business practices through accountability and a system of checks and balances. Examples:- Risk Assessment & Incident Management • Establish internal security personnel network • Establish incident database and procedures to handle suspicious activities, incident reporting and response. • Emergency and evacuation plans. Cargo Handling • Barcode/RFID scanning to detect discrepancies and ensure only manifested cargo is loaded. • Use carton tape imprinted with company's name. • Rotate shipping/receiving personnel.	I P N	Efficiency: 1 2 3 4 5 6 7 Timeliness: 1 2 3 4 5 6 7 Reliability: 1 2 3 4 5 6 7 Availability: 1 2 3 4 5 6 7 Responsiveness: 1 2 3 4 5 6 7 Security: 1 2 3 4 5 6 7
6. Physical Security and Access Control. Prevent unauthorized entry to facilities, maintain control of personnel and protect company assets. Examples:- • 24-hours security guard and/or police patrol • Fence/gate with magnetic sensors, alarm systems. For Employees • Biometric technology, color-coding uniforms. • Photo ID cards and password controlled locks. For Visitors & Deliveries/Cargo Pickup (Including Mail) • ID verification and exchange for visitor's badge. • Schedule pickups and establish driver waiting area. • Screen/random inspect incoming packages/vehicles.	I P N	Efficiency: 1 2 3 4 5 6 7 Timeliness: 1 2 3 4 5 6 7 Reliability: 1 2 3 4 5 6 7 Availability: 1 2 3 4 5 6 7 Responsiveness: 1 2 3 4 5 6 7 Security: 1 2 3 4 5 6 7

Security Initiatives	Implementation Status	Impact on Supply Chain Performance
		Extremely Negative / Very Negative / Moderately Negative / Unsure / Neutral / Quite Positive / Moderately Positive / Extremely Positive (1 2 3 4 5 6 7)
7. Tracking & Monitoring (Conveyance Security). Inspect, secure and track conveyance to ensure mode of transport is not used to facilitate terrorism or illegal acts. Examples:- Trucking/Drayage • Monitor "unusual" requests and time lags for container turnaround time on premises. • Global Positioning System (GPS), truck transponders, online shipment visibility tool, CCTVs. • Utilize panic buttons, security escorts/travel in convoys. • Designate routes and establish alternate routes • Examine fuel consumption to detect route deviations. • Staff rotation to prevent internal conspiracies. Ocean Carriers • Control use of equipment • Satellite monitoring, remote surveillance and detect stowaways	I P N	Efficiency: 1 2 3 4 5 6 7 Timeliness: 1 2 3 4 5 6 7 Reliability: 1 2 3 4 5 6 7 Availability: 1 2 3 4 5 6 7 Responsiveness: 1 2 3 4 5 6 7 Security: 1 2 3 4 5 6 7
8. Personnel Security. Examples:- • Pre-employment background checks. • Termination procedures. • Employee handbook for internal code of conduct. • Employee security awareness training.	I P N	Efficiency: 1 2 3 4 5 6 7 Timeliness: 1 2 3 4 5 6 7 Reliability: 1 2 3 4 5 6 7 Availability: 1 2 3 4 5 6 7 Responsiveness: 1 2 3 4 5 6 7 Security: 1 2 3 4 5 6 7

Security Initiatives	Implementation Status	Impact on Supply Chain Performance
		Extremely Negative / Very Negative / Moderately Negative / Unsure / Neutral / Quite Positive / Moderately Positive / Extremely Positive (1 2 3 4 5 6 7)
9. Container/Trailer/Unit Load Device (ULD) Security. Container inspection, storage, tracking, seal control, issuance and verification. Examples:- Trucking/Drayage • Exterior inspection, container and seal condition, and seal no. verification and seal issuance controls. • Secure empty containers and less-than-truckloads. Ocean Carriers & Container Seals • Seals on every container on board and checks at every hand-off. • E-seals, other advanced container locking technology. • "Smart Box" – container with heavy-duty seal and electronic security device that communicates evidence of tampering, register every legitimate and unauthorized opening of container.	I P N	Efficiency: 1 2 3 4 5 6 7 Timeliness: 1 2 3 4 5 6 7 Reliability: 1 2 3 4 5 6 7 Availability: 1 2 3 4 5 6 7 Responsiveness: 1 2 3 4 5 6 7 Security: 1 2 3 4 5 6 7
10. Management support and sponsorship. Senior management's involvement in organization's supply chain security program and dedicating necessary resources to the efforts. Examples:- Domestic • Establish security committee and conduct periodic briefings • Incorporate security into "Continuous Improvement" philosophy and mission statement • Top management maintains high level of familiarity with overseas business partners, their practices and affiliations and ensures all subsidiaries develop and implement a sound security plan Worldwide • Establish security directors and global security council to formulate global security guidelines, methods for assessment	I P N	Efficiency: 1 2 3 4 5 6 7 Timeliness: 1 2 3 4 5 6 7 Reliability: 1 2 3 4 5 6 7 Availability: 1 2 3 4 5 6 7 Responsiveness: 1 2 3 4 5 6 7 Security: 1 2 3 4 5 6 7

Section E. Respondents' Information

E1. How did you get to know about this survey?

- ❑ Canadian Supply Chain Logistics Association
- ❑ Canadian Transportation Magazine
- ❑ SecuritySurvey2007@freightsecurity.ubc.ca
- ❑ A personal contact
- ❑ Others, please specify: _____

E2. Where is your physical location?

- ❑ Canada
- ❑ China
- ❑ Hong Kong
- ❑ Singapore
- ❑ United States of America
- ❑ Others, please specify: _____

E3. What is your title/position in your organization?

E4. What is the name of your organization? (Optional).

E5. Please indicate the country whose culture influences your business perspectives, thoughts, ideas and opinions the most.

E6. If you are interested in receiving an executive summary of the findings, please provide us with your email address below.

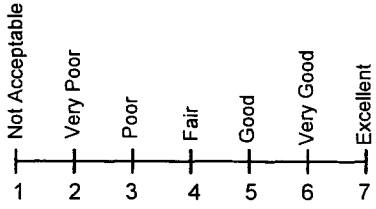
*** SERVICE PROVIDER ***
ENGLISH VERSION

Section A. Self Performance Appraisal

A1. For the following survey, are you answering the questions for your entire firm or for your division/strategic business unit?

❑ Entire firm ❑ My division or strategic business unit (SBU)

Score / Rating

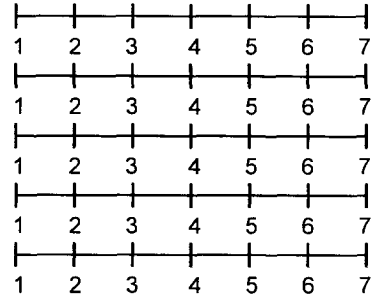


A2. On a scale of 1 to 7 where [1=Not Acceptable and 7=Excellent], please rate how secure you think your supply chain is.

(Secure as in the probability of your supply chain being compromised in terms of pilferages, thefts, damages, terrorism and other crimes such as smuggling, contraband etc.)

A3. On a scale of 1 to 7 where [1=Not Acceptable and 7=Excellent], please rate how well you think your logistics/supply chain operations are performing in the following aspects.

1. Efficiency (including cost of fulfillment, productivity)
2. Timeliness of product delivery (including speed and on-time performance)
3. Reliability of operations (including accuracy and recovery from disruptions)
4. Availability of products
5. Responsiveness to customers' needs (including flexibility and agility)



Section B. Organization Profiling

B1. To what main industrial sector does your organization belong? (Check all that apply).

❑ Port Authority
❑ Ocean Carrier
❑ Trucking / Inter-modal Company
❑ Others, please specify: _____
❑ Terminal Operators
❑ Customs Broker
❑ Freight Consolidator
❑ 3rd Party Logistics Provider
❑ Customs Authority
❑ Freight Forwarder

B2. What industry/sector does your organization serve the most? (Check no more than 3).

- ❑ Fast Moving Consumer Goods (FMCG)
- ❑ Automotive
- ❑ Heavy Machinery
- ❑ Electronics / High Tech Products
- ❑ Pharmaceuticals
- ❑ Aerospace
- ❑ Perishables / Food Products
- ❑ Chemicals
- ❑ Others, please specify: _____

B3. Does your organization handle hazardous cargo?

- ❑ No
- ❑ Yes, what _____ %

B4. Does your organization ship full container loads?

- ❑ No
- ❑ Yes, what _____ %

B5. What is(are) your organization's main trade route(s)? (Check no more than 3).

- ❑ Intra Asia
- ❑ Intra Americas (within N.A. and S.A.)
- ❑ Intra Europe

- ❑ Trans Pacific (Asia → N.A.)
- ❑ Trans Pacific (Asia → S.A.)
- ❑ Trans Pacific (N.A. → Asia)
- ❑ Trans Pacific (S.A. → Asia)

- ❑ Asia Europe (Asia → Europe)
- ❑ Trans Atlantic (N.A. → Europe)
- ❑ Trans Atlantic (S.A. → Europe)
- ❑ Asia Europe (Europe → Asia)
- ❑ Trans Atlantic (Europe → N.A.)
- ❑ Trans Atlantic (Europe → S.A.)

- ❑ Asia → Middle East/Africa
- ❑ N.A. → Middle East/Africa
- ❑ S.A. → Middle East/Africa
- ❑ Europe → Middle East/Africa
- ❑ Middle East/Africa → Asia
- ❑ Middle East/Africa → N.A.
- ❑ Middle East/Africa → S.A.
- ❑ Middle East/Africa → Europe

- ❑ Not Applicable
- ❑ Others. please specify: _____

Legend : *N.A.: North America and Central America (includes Panama and all countries north of Pananma)*
S.A.: South America (all countries south of Panama)

B6. What is your organization's annual revenue for 2005 (in US$)? Please select a range from below.

- ❑ less than US$20 million
- ❑ US$20 million to US$100 million
- ❑ US$100 million to US$500 million
- ❑ US$500 million to US$1 billion
- ❑ more than US$1 billion

B7. Which of the following supply chain activities do you directly select/make final decisions for?
Please indicate "X" under the "Make Final Decisions" column against each activity that you select/make final decision for.
Please indicate "X" under "Outsource Final Decision Making" column against each activity that you do not make final decision for.
For those activities that are not applicable to your organization, please indicate "X" under the "Not Applicable" column.

Aspects of Supply Chain	Outsource Final Decision Making	Make Final Decisions In-house	Not Applicable
Trucking or other inter-modal transportation from factory to origin port			
Warehousing at origin			
Freight consolidation at origin			
Customs clearance at origin			
Cross-border trucking to origin port or final destination (if required)			
Choice of port of loading			
Choice of terminal at origin			
Choice of carriers (i.e. freight contracts)			
Choice of port of destination			
Choice of terminal at destination			
Customs clearance at destination			
Cross-border trucking from destination port to final destination (if required)			
Warehousing at destination			
Freight deconsolidation / break bulk at destination			
Trucking or other inter-modal transportation to final location at destination			

B8. If Please indicate the strategic importance of the following supply chain drivers for your organization. [1=Not at all Important, 2=Slightly Important, 3=Somewhat Important, 4=Moderately Important, 5=Important, 6=Very Important, 7=Extremely Important].

Supply Chain Drivers	Not Important ... Somewhat Important ... Very Important
1. Efficiency (including cost of fulfillment, productivity)	1 2 3 4 5 6 7
2. Timeliness of product delivery (including speed and on-time performance)	1 2 3 4 5 6 7
3. Reliability of operations (including accuracy and recovery from disruptions)	1 2 3 4 5 6 7
4. Availability of products	1 2 3 4 5 6 7
5. Responsiveness to customers' needs (including flexibility and agility)	1 2 3 4 5 6 7
6. Security	1 2 3 4 5 6 7

Section C. Key Performance Indicators (KPIs)

C1. In your opinion, should there be KPIs for security performance/efforts?

❑ Yes ❑ No ❑ Unsure/Undecided

C2. Next, using a 3-point scale: [1=Inappropriate, 2=Indifferent/Unsure, 3=Appropriate], please indicate under the relevant "Appropriateness" scales, the degree to which you think that each KPI below is an appropriate indicator for Supply Chain Performance and Security Performance.

Key Performance Indicators (KPI)	Appropriateness For Supply Chain Performance (Inappropriate Indifferent Appropriate)	Appropriateness For Security Performance (Inappropriate Indifferent Appropriate)
1. Asset utilization (e.g. vessel, containers, trucks).	1 2 3	1 2 3
2. Results from a random security audit.	1 2 3	1 2 3
3. Operations efficiency (e.g. control crane rate, warehouse productivity).	1 2 3	1 2 3
4. Number of security policy violations.	1 2 3	1 2 3

Key Performance Indicators (KPI)	Appropriateness For Supply Chain Performance	Appropriateness For Security Performance
5. Level of insurance premiums for cargo and/or operations.	Inappropriate Indifferent Appropriate 1 2 3	Inappropriate Indifferent Appropriate 1 2 3
6. Level of inventory (in warehouses).	1 2 3	1 2 3
7. Number/frequency of customs inspections.	1 2 3	1 2 3
8. Logistics costs as a percentage (%) of sales or per product unit.	1 2 3	1 2 3
9. On-time transmission of shipment information.	1 2 3	1 2 3
10. Number of unauthorized entry incidents.	1 2 3	1 2 3
11. Service fulfillment lead times (e.g. truck/permit turnaround time).	1 2 3	1 2 3
12. On-time service delivery (e.g. berth-on-arrival, information transmission).	1 2 3	1 2 3
13. Length of time to deliver expedited orders.	1 2 3	1 2 3
14. Customs clearance lead-time (import and/or export).	1 2 3	1 2 3
15. Accuracy rate of shipment information (e.g. manifest transmission).	1 2 3	1 2 3
16. Number/frequency of service errors and failures.	1 2 3	1 2 3
17. Results from periodic safety audit.	1 2 3	1 2 3
18. Accuracy rate of inventory records (e.g. cycle counting variance).	1 2 3	1 2 3
19. Accuracy rate of invoicing.	1 2 3	1 2 3
20. Number/frequency of pilferage/theft/security incidents.	1 2 3	1 2 3
21. Amount of freight claims and/or freight loss (in monetary terms).	1 2 3	1 2 3
22. Number/frequency of personnel safety accidents.	1 2 3	1 2 3
23. Amount/frequency of overages, shortages and damages (OS&D).	1 2 3	1 2 3

Key Performance Indicators (KPI)	Appropriateness For Supply Chain Performance	Appropriateness For Security Performance
24. Amount/frequency of operations deviations (e.g. capacity deviations).	Inappropriate Indifferent Appropriate 1 2 3	Inappropriate Indifferent Appropriate 1 2 3
25. Number/frequency of "back orders" (e.g. container rolls, delivery delays).	1 2 3	1 2 3
26. Number/frequency of order cancellations/ rejections.	1 2 3	1 2 3
27. Average time taken to respond to client problems.	1 2 3	1 2 3
28. Average time taken to resolve client problems.	1 2 3	1 2 3
29. Results from customer service satisfaction / feedback survey.	1 2 3	1 2 3
30. Order fill rate.	1 2 3	1 2 3
31. Number and type of special requests satisfied.	1 2 3	1 2 3
32. Number and type of customer complaints resolved.	1 2 3	1 2 3
33. Others:	1 2 3	1 2 3
34. Others:	1 2 3	1 2 3
35. Others:	1 2 3	1 2 3

Section D. Supply Chain Security Initiatives

For each type/group of security initiative below, please indicate whether your organization is currently Implementing / Implemented (I), Planning to implement (P) or Not implementing (N) that initiative.

Also, for each initiative currently Implementing / Implemented (I) or Planning to Implement (P), please indicate under "Impact on Supply Chain Performance", how the initiative has impacted or will impact your supply chain performance, using a 7-point scale: [1=Extremely Negative, 2=Very Negative, 3=Moderately Negative, 4=Unsure/Neutral, 5=Moderately Positive, 6=Very Positive, 7=Extremely Positive].

Security Initiatives	Implementation Status	Impact on Supply Chain Performance
		Extremely Negative / Very Negative / Moderately Negative / Unsure / Neutral / Moderately Positive / Very Positive / Extremely Positive (1 2 3 4 5 6 7)
1. Operations/Security Related Certifications. Internationally recognized certifications for operations excellence including security and risk assessment.	I P N	Efficiency: 1 2 3 4 5 6 7
		Timeliness: 1 2 3 4 5 6 7
Examples:-		Reliability: 1 2 3 4 5 6 7
• Customs-Trade Partnership Against Terrorism (C-TPAT) (U.S.).		Availability: 1 2 3 4 5 6 7
• Partners-In-Protection (PIP) (Canada).		Responsiveness: 1 2 3 4 5 6 7
• Secure-Trade-Partnership (STP) (Singapore).		Security: 1 2 3 4 5 6 7
• Free and Secure Trade (FAST) (U.S. and Canada).		
• Transported Asset Protection Association (TAPA).		
• International Ship and Port Facility Security (ISPS).		
2. Advanced Data. Compliance to data submission programs through secure information transmission technology.	I P N	Efficiency: 1 2 3 4 5 6 7
		Timeliness: 1 2 3 4 5 6 7
Examples:-		Reliability: 1 2 3 4 5 6 7
• 24-hours Advance Manifest Rule & Automated Commercial Environment (ACE) (U.S.).		Availability: 1 2 3 4 5 6 7
• Advanced Commercial Information (ACI) (Canada).		Responsiveness: 1 2 3 4 5 6 7
• Traceable/secure electronic data transmissions.		Security: 1 2 3 4 5 6 7
• Advanced shipping notices (ASNs).		

Security Initiatives	Status	Impact on Supply Chain Performance
		Extremely Negative (1) · Very Negative (2) · Moderately Negative (3) · Unsure / Neutral (4) · Moderately Positive (5) · Very Positive (6) · Extremely Positive (7)
3. Business Partners Requirements.		
Working with business partners to ensure security measures are in place and adhered to.	I P N	Efficiency: 1 2 3 4 5 6 7 Timeliness: 1 2 3 4 5 6 7 Reliability: 1 2 3 4 5 6 7 Availability: 1 2 3 4 5 6 7 Responsiveness: 1 2 3 4 5 6 7 Security: 1 2 3 4 5 6 7
Examples:- Towards Manufacturer/Supplier/Vendor • Contractual obligations. • Factory certification requirements. • Supplier code of conduct. Towards Service Provider • Representative at overseas office. • Prohibit subcontracting. • Require background clearances for personnel. • Contractual obligations/procedures for selection. Towards Customer • Prevent misuse of products through education. • Verify business references, credit checks. • Establish routine pickup/drop-off points.		
4. Security Training & Outreach Programs.	I P N	Efficiency: 1 2 3 4 5 6 7 Timeliness: 1 2 3 4 5 6 7 Reliability: 1 2 3 4 5 6 7 Availability: 1 2 3 4 5 6 7 Responsiveness: 1 2 3 4 5 6 7 Security: 1 2 3 4 5 6 7
Examples:- • Use alert levels • Communicate terrorism information to employees. • Periodic training, specialized training in handling breaches, conducting investigations, inspections etc. • Train business partners. • Provide incentives for incident reporting. • Collaborate with local law enforcement.		

Security Initiatives	Status	Impact on Supply Chain Performance
		Extremely Negative (1) · Very Negative (2) · Moderately Negative (3) · Unsure / Neutral (4) · Moderately Positive (5) · Very Positive (6) · Extremely Positive (7)
5. Procedural Security. Incorporate security into business practices through accountability and a system of checks and balances. Examples:- Risk Assessment & Incident Management • Establish internal security personnel network • Establish incident database and procedures to handle suspicious activities, incident reporting and response. • Emergency and evacuation plans. Cargo Handling • Barcode/RFID scanning to detect discrepancies and ensure only manifested cargo is loaded. • Use carton tape imprinted with company's name. • Rotate shipping/receiving personnel.	I P N	Efficiency: 1 2 3 4 5 6 7 Timeliness: 1 2 3 4 5 6 7 Reliability: 1 2 3 4 5 6 7 Availability: 1 2 3 4 5 6 7 Responsiveness: 1 2 3 4 5 6 7 Security: 1 2 3 4 5 6 7
6. Physical Security and Access Control. Prevent unauthorized entry to facilities, maintain control of personnel and protect company assets. Examples:- • 24-hours security guard and/or police patrol • Fence/gate with magnetic sensors, alarm systems. For Employees • Biometric technology, color-coding uniforms. • Photo ID cards and password controlled locks. For Visitors & Deliveries/Cargo Pickup (Including Mail) • ID verification and exchange for visitor's badge. • Schedule pickups and establish driver waiting area. • Screen/random inspect incoming packages/vehicles.	I P N	Efficiency: 1 2 3 4 5 6 7 Timeliness: 1 2 3 4 5 6 7 Reliability: 1 2 3 4 5 6 7 Availability: 1 2 3 4 5 6 7 Responsiveness: 1 2 3 4 5 6 7 Security: 1 2 3 4 5 6 7

Security Initiatives	Implementation Status	Impact on Supply Chain Performance
		Extremely Negative / Very Negative / Moderately Negative / Unsure / Neutral / Moderately Positive / Very Positive / Extremely Positive
7. Tracking & Monitoring (Conveyance Security). Inspect, secure and track conveyance to ensure mode of transport is not used to facilitate terrorism or illegal acts. Examples:- Trucking/Drayage • Monitor "unusual" requests and time lags for container turnaround time on premises. • Global Positioning System (GPS), truck transponders, online shipment visibility tool, CCTVs. • Utilize panic buttons, security escorts/travel in convoys. • Designate routes and establish alternate routes • Examine fuel consumption to detect route deviations. • Staff rotation to prevent internal conspiracies. Ocean Carriers • Control use of equipment • Satellite monitoring, remote surveillance and detect stowaways	I P N	Efficiency: 1 2 3 4 5 6 7 Timeliness: 1 2 3 4 5 6 7 Reliability: 1 2 3 4 5 6 7 Availability: 1 2 3 4 5 6 7 Responsiveness: 1 2 3 4 5 6 7 Security: 1 2 3 4 5 6 7
8. Personnel Security. Examples:- • Pre-employment background checks. • Termination procedures. • Employee handbook for internal code of conduct. • Employee security awareness training.	I P N	Efficiency: 1 2 3 4 5 6 7 Timeliness: 1 2 3 4 5 6 7 Reliability: 1 2 3 4 5 6 7 Availability: 1 2 3 4 5 6 7 Responsiveness: 1 2 3 4 5 6 7 Security: 1 2 3 4 5 6 7

Security Initiatives	Implementation Status	Impact on Supply Chain Performance
		Extremely Negative (1) · Very Negative (2) · Moderately Negative (3) · Unsure / Neutral (4) · Moderately Positive (5) · Very Positive (6) · Extremely Positive (7)
9. Container/Trailer/Unit Load Device (ULD) Security. Container inspection, storage, tracking, seal control, issuance and verification. Examples:- Trucking/Drayage • Exterior inspection, container and seal condition, and seal no. verification and seal issuance controls. • Secure empty containers and less-than-truckloads. Ocean Carriers & Container Seals • Seals on every container on board and checks at every hand-off. • E-seals, other advanced container locking technology. • "Smart Box" – container with heavy-duty seal and electronic security device that communicates evidence of tampering, register every legitimate and unauthorized opening of container.	I P N	Efficiency: 1 2 3 4 5 6 7 Timeliness: 1 2 3 4 5 6 7 Reliability: 1 2 3 4 5 6 7 Availability: 1 2 3 4 5 6 7 Responsiveness: 1 2 3 4 5 6 7 Security: 1 2 3 4 5 6 7
10. Management support and sponsorship. Senior management's involvement in organization's supply chain security program and dedicating necessary resources to the efforts. Examples:- Domestic • Establish security committee and conduct periodic briefings • Incorporate security into "Continuous Improvement" philosophy and mission statement • Top management maintains high level of familiarity with overseas business partners, their practices and affiliations and ensures all subsidiaries develop and implement a sound security plan Worldwide • Establish security directors and global security council to formulate global security guidelines, methods for assessment	I P N	Efficiency: 1 2 3 4 5 6 7 Timeliness: 1 2 3 4 5 6 7 Reliability: 1 2 3 4 5 6 7 Availability: 1 2 3 4 5 6 7 Responsiveness: 1 2 3 4 5 6 7 Security: 1 2 3 4 5 6 7

Section E. Respondents' Information

E1. How did you get to know about this survey?

- ❑ Canadian Supply Chain Logistics Association
- ❑ Canadian Transportation Magazine
- ❑ SecuritySurvey2007@freightsecurity.ubc.ca
- ❑ A personal contact
- ❑ Others, please specify: _____

E2. Where is your physical location?

- ❑ Canada
- ❑ China
- ❑ Hong Kong
- ❑ Singapore
- ❑ United States of America
- ❑ Others, please specify: _____

E3. What is your title/position in your organization?

E4. What is the name of your organization? (Optional).

E5. Please indicate the country whose culture influences your business perspectives, thoughts, ideas and opinions the most.

E6. If you are interested in receiving an executive summary of the findings, please provide us with your email address below.

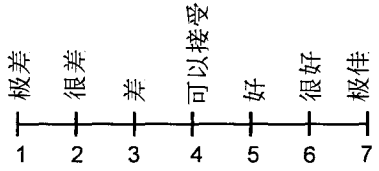
* 进/出口商 *
中文版

项目A. 企业营运表现自我评估

A1. 请问您是以什么身份对于以下的问卷进行作答？

❑ 正个公司　　❑ 我负责的营业单位

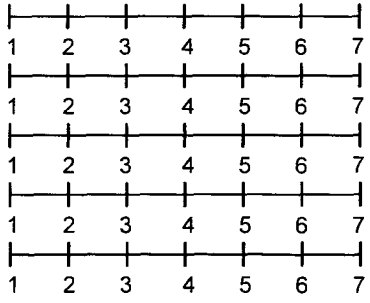
自我表现评估



A2. 请问您认为贵公司在供应链保安/安全方面的表现如何？[“1”为“极差”和“7”为“极佳”]。

(保安/安全的定义在于贵公司的供应链受到下列状况影响的比例：1) 遗失 2) 盗窃 3) 破损 4) 恐怖袭击 5) 其它例如盗版、走私等。)

A3. 请问您认为贵公司在供应链以下各方面的表现如何？[“1”为“极差”和“7”为“极佳”]。



1. 效率(包括产品/服务配送成本)
2. 货物配送准时性（包括准时性，速度）
3. 运作的可靠性（运作的准确度，和在受到影响后恢复的速度与能力）
4. 货物的可及性（如货品存货量是否能及时应付订单需求）
5. 反应能力（包括对于客户要求的应变能力，运作调整的敏捷性）

项目B. 企业与营运资料

B1. 请问贵公司属于以下哪种企业类别？(请在所有适当的选项旁打勾)。

❑ 进口商 (Importer)　　❑ 出口商 (Exporter)　　❑ 其他，请说明: _____

B2. 请问贵公司属于下列哪种供应链?(请在所有适当的选项打勾)。

❑ 快速消费品 (FMCG)　❑ 电子/高科技产品　❑ 易耗品/食品类
❑ 汽车/汽车零件　❑ 医药　❑ 化工业
❑ 重型器械　❑ 航空　❑ 其他，请说明：_____

B3. 请问贵公司所供应的产品是否包括危险品?

❑ 没有　❑ 有，请说明 % _____ %

B4. 请问贵公司所供应的产品运输方式是否有包括整集装箱(i.e. full container loads)?

❑ 没有　❑ 有，请说明 %: _____ %

B5. 请问贵公司的主要商船航线有哪些? 请打勾。(不超过3个)。

❑ 亚洲内部(包括印度和南太平洋)　❑ 南北美洲内部　❑ 欧洲内部

❑ 跨太平洋（亚洲至北美洲　❑ 跨太平洋（北美洲至亚洲）
❑ 跨太平洋（亚洲至南美洲）　❑ 跨太平洋（南美洲至亚洲）

❑ 亚欧（亚洲至欧洲　❑ 亚欧（欧洲至亚洲）
❑ 跨大西洋（北美洲至欧洲）　❑ 跨大西洋（欧洲至北美洲）
❑ 跨大西洋（南美洲至欧洲）　❑ 跨大西洋（欧洲至南美洲）

❑ 亚洲至中 /非洲　❑ 中东/非洲至亚洲
❑ 北美洲至中 /非洲　❑ 中东/非洲至北美洲
❑ 南美洲至中 /非洲　❑ 中东/非洲至南美洲
❑ 欧洲至中 /非洲　❑ 中东/非洲至欧洲

❑ 请说明，其他_____

备注： ** 北美和中美洲(包括巴拿马及巴拿马以北的国家)*　** 南美洲(包括巴拿马以南的所有国家)*

B6. 请问贵公司2005年的营业额（美金）？请在以下选项作选择。

- ❑ 少于2,000万美金
- ❑ 介于2,000万到1亿美金
- ❑ 介于1亿到5亿美金
- ❑ 介于5亿到10亿美金
- ❑ 多于10亿美金

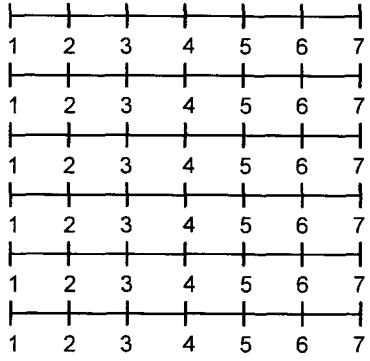
B7. 请问贵公司在以下哪几种供应链运作活动中拥有最后的决定/选择权？
如该选项拥有决定权，请在对应的“有最后决定权”栏里打“X”。
如该选项的决定权外包，请在对应的“外包最后决定权”栏里打“X”。如该选项并不适用于贵公司的供应链，请在对应的“不适用”栏里打“X”。

供应链的不同方面	外包最后决定权	由最后决定权	不适用
供应商的选择（如制造商）			
从工厂以陆运或其他运输方式运载到起发地港口			
起发地的仓储			
起发地的货物混载			
起发地港口的清官			
起发地到港口目的地的跨边界运输（若需要）			
装货港口的选择			
起发地港口总站的选择			
运输公司的选择(如签订运输协议)			
目的地港口的选择			
目的地港口总站的选择			
目的地港口的清官			
从目的地港口到最终目的地的跨边界运输(若需要)			
目的地的仓储			
目的地的货物分拣			
从目的地港口以陆运或其他运输式运载到最终目的地			

B8. 如果贵公司认为供应链管理是您的竞争优势之一，请表明以下各策略对于贵公司供应链管理的重要性？[1=完全不重要， 2=不重要，3=不太重要，4=一般重要，5=比较重要，6=很重要，7=非常重要]。

物流和供应链策略

1. 效率(包括产品/服务配送成本)
2. 货物配送准时性（包括准时性，速度）
3. 运作的可靠性（运作的准确度，和在受到影响后恢复的速度与能力）
4. 货物的可及性（如货品存货量是否能及时应付订单需求）
5. 反应能力（包括对于客户要求的应变能力，运作调整的敏捷性）
6. 保安



项目C. 企业与营运考核指标

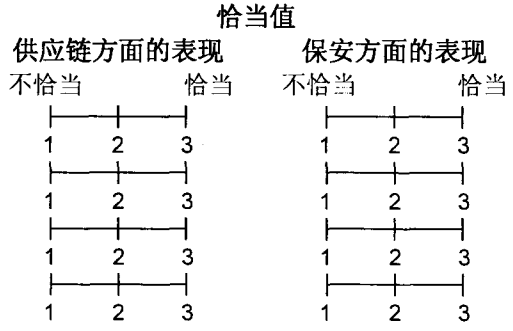
C1. 请问您认为是否应该为公司在供应链保安方面的表现/努力设定考核指标(KPI)吗?

❑ 应该 ❑ 不应该 ❑ 不确定/未定

C2. 接下来，请您以一至三分的标度[1=不恰当，2=无所谓/不确定，3=恰当]，在适当的“恰当值”栏里，表明贵公司对以下各考核指标(KPI)作为考核供应链方面的表现和保安方面的表现是否恰当。

考核指标 (KPI)

1. 资产利用率(如生产容量，集装箱，货车)。
2. 保安审查(突发与非突发)的成绩。
3. 运作效率(如劳动生产力，每小时的捡货速度)。
4. 保安人员或员工没有遵守保安条例事件的次数与频率。



考核指标（KPI）

5. 货物和运作方面的保险费用。

6. 库存量(仓库内或在途)。

7. 海关安检的次数与频率。

8. 物流成本对最终销售额的比例或每生产产品单位。

9. 传输与航运相关物流运作信息的准时性/率。

10. 非法或未批准侵入事件的次数与频率。

11. 订货至交货周转时间(如订单至收款的周期)。

12. 送货的准时性(如准时送货，文件的百分比)。

13. 急单处理和交货时间。

14. 清关时间(进口或出口)。

15. 物流相关信息的准确度(如运输文件，装箱单的传输)。

16. 服务出错和失败的次数/频率。

17. 期性安全审计的成绩。

18. 库存记录的准确度(如盘点的差异)。

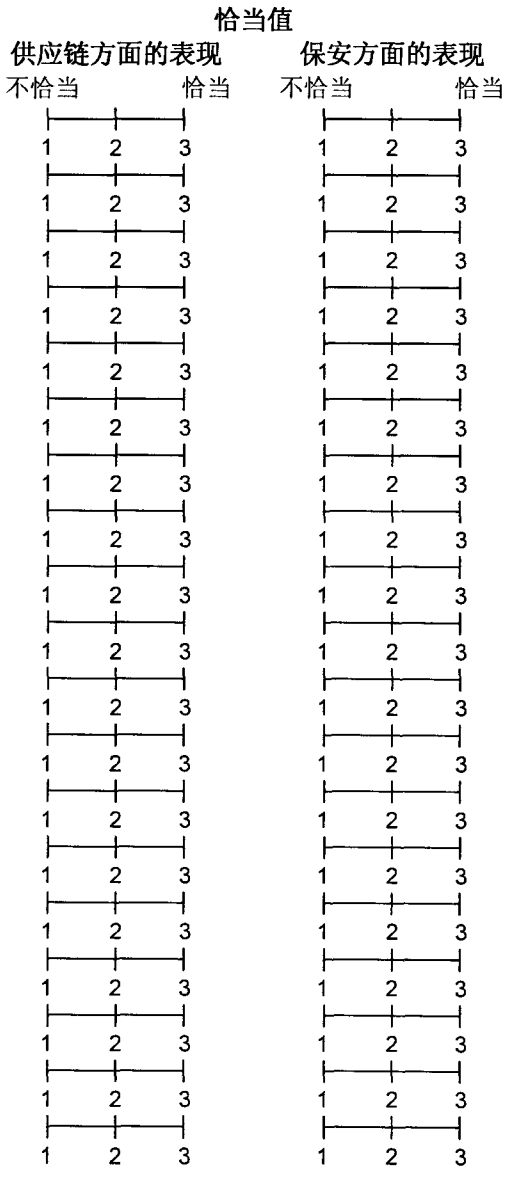
19. 开发票的准确度。

20. 货物偷窃或保安意外的发生次数与频率。

21. 货物损失赔偿数额。

22. 员工安全意外的次数与频率。

23. 过剩，短缺和破损(OS&D)的次数与频率。



考核指标 (KPI)

	恰当值	
	供应链方面的表现	保安方面的表现
	不恰当 恰当	不恰当 恰当
24. 货物处理程序上的偏差的次数与频率(生产资源偏差)。	1 2 3	1 2 3
25. 无法及时完成的订单(如过期订单)的次数与频率。	1 2 3	1 2 3
26. 订单取消或拒绝的次数与频率。	1 2 3	1 2 3
27. 对客户问题的反应时间。	1 2 3	1 2 3
28. 解决客户问题的时间。	1 2 3	1 2 3
29. 客户满意度和意见的市场调查的成绩。	1 2 3	1 2 3
30. 订单符合率。	1 2 3	1 2 3
31. 满足客户特别要求的种类和数量比例。	1 2 3	1 2 3
32. 解决客户投诉的种类和数量比例。	1 2 3	1 2 3
33. 其它:	1 2 3	1 2 3
34. 其它:	1 2 3	1 2 3
35. 其它:	1 2 3	1 2 3

项目D. 供应链保安方面的应对措施

接下来，请您在下列各项中表明贵公司目前是否正在实施/已实施(I),计划实施(P)或不打算实施(N)此保安措施。

同时，请您也为贵公司目前正在实施/已实施(I)和计划实施(P)的措施中表明供应链的表现，请在“对供应链的影响”栏里表明此措施在哪方面如何影响贵司在供应链的表现。请您以1至7分[1=非常反面，2=反面，3=比较反面，4=不确定，5=比较正面,6=正面,7=非常正面]，表示您的观点。

保安措施

实施状态

对供应链的影响

非常反面 | 反面 | 比较反面 | 不确定 | 比较正面 | 正面 | 非常正面

1. 保安相关或优秀运作的证书。

I P N

效率: 1 2 3 4 5 6 7

准时性: 1 2 3 4 5 6 7

可靠性: 1 2 3 4 5 6 7

可及性: 1 2 3 4 5 6 7

反映度: 1 2 3 4 5 6 7

保安: 1 2 3 4 5 6 7

如:-

- Customs-Trade Partnership Against Terrorism (C-TPAT)(美国)
- Partners-In-Protection (PIP)(加拿大)
- Secure-Trade-Partnership (STP)(新加坡)
- Free and Secure Trade (FAST)(美国/加拿大)
- 资产运输保护协会(TAPA)
- 国际船只与港务设施保安(ISPS)

2. 提前数据/信息。

通过资讯安全传输科技提前传输信息和资料,
以符合官方在这方面的条规和协助各方查出货物抵港前的任何反常现象/差误。

I P N

效率: 1 2 3 4 5 6 7

准时性: 1 2 3 4 5 6 7

可靠性: 1 2 3 4 5 6 7

可及性: 1 2 3 4 5 6 7

反映度: 1 2 3 4 5 6 7

保安: 1 2 3 4 5 6 7

如:-

- 24-hours Advance Manifest Rule(美国)
- Advanced Commercial Information(加拿大)
- 采用可追踪/安全电子数据传输系统
- 先遣运输通知(ASNs)

保安措施	实施状态	对供应链的影响

3. 对商业伙伴的要求。

I P N

与商业合作伙伴共同建立/实施各种保安措施，并确保对措施的遵守/服从。

如:-

对供应商/生产商

- 要求服从保安方面的准则
- 商务契约责任
- 工厂保安证书/证明要求

对物流供应商

- 海外业务实地代表
- 禁止转包
- 要求人员背景调查
- 商务契约责任/供应商选择标准

对客户

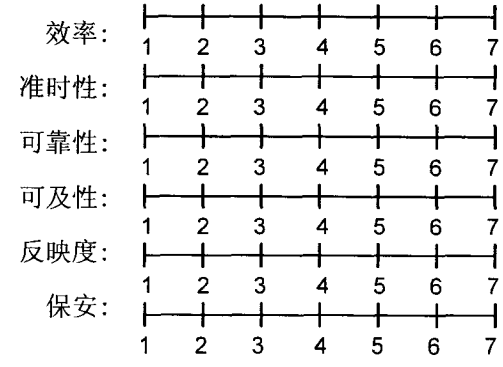
- 通过对客户教育以防止产品滥用或误用
- 核实企业伙伴资料，信誉
- 成立惯例性收货卸货点

4. 保安意识与保安程序/科技培训。

I P N

如:-

- 使用多层警戒
- 对员工传达恐怖活动方面的信息
- 保安事件调查，检查等方面的专业培训
- 商业伙伴的相关培训
- 设立奖励以鼓励员工申报事件
- 和当地司法机关保持紧密合作



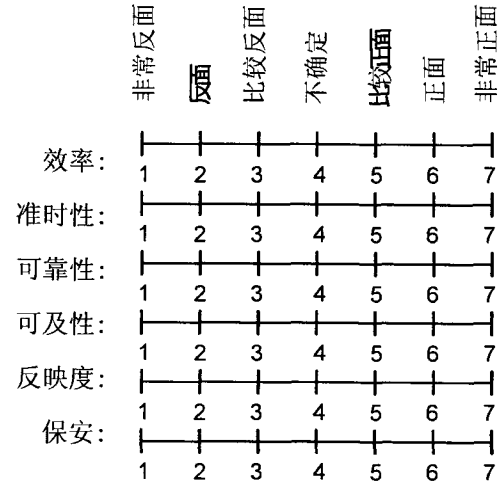
保安措施	实施状态	对供应链的影响

5. 保安程序。
将保安注入公司营运策划的一部分并设立相关的管理系统(如责任规划、检查和制衡系统等)。

I P N

如:-
风险评估/分析与事件管理
- 设立内部保安人员网络和整套的持续改善计划
- 成立事件档案库和突发事件的处理章程，如对应可疑活动，全球/当地事件
- 紧急疏散计划

货物处理
- 采用后备地址寄存码的扫描，以便查出货物处理上的差错和确保只对已向海关申报的货物进行装箱
- 特殊货物包装，如印有公司标志的胶带
- 调动收货/出货员工



6. 实际进出保安科技与权限控制。
禁止营运设施的非法/未许可的进出入，控制人员流动和保护企业财产。

I P N

如:-
- 24小时保安人员/警察巡逻
- 安装具有磁性传感的围栏/门，警报系统

内部员工
- 采用生物科技来辨认身份，颜色代码制服
- 有相片的身份证明卡和密码控制锁

访客和送货/提货(包括邮件)
- 要求访客到访前的预检和核实身份的真实性
- 身份证明卡和访客卡调换
- 成立提货日程表与卡车司机等待区
- 突检人员/邮包/邮件/卡车

保安措施	实施状态	对供应链的影响

7. 追踪/监视科技(运输过程的保安)。

I P N

检查并追踪整个运输过程，以确保所适用的运输系统不被恐怖份子/其他犯罪者滥用。

如:-

卡车货运

- 成立一套能够探测集装箱堆场/提卸货物处内非寻常/延长逗留事件
- 全球定位系统（GPS），运输货车信息收发器
- 在车内安装警报系统，安排安保人员护送高价值或敏感货物
- 安排并设定运输路线与后备路线
- 观察货车油消耗量以发现任何可疑的路线偏差
- 员工定期调动以防止内部合谋

船运公司

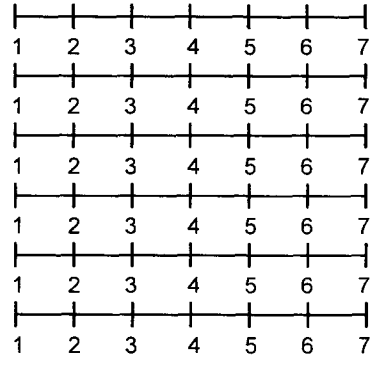
- 控制器材的适用
- 网上船运追踪工具/系统
- 监察偷渡者
- 卫星勘测、 远距离侦察

8. 员工的保安程序。

I P N

如:-

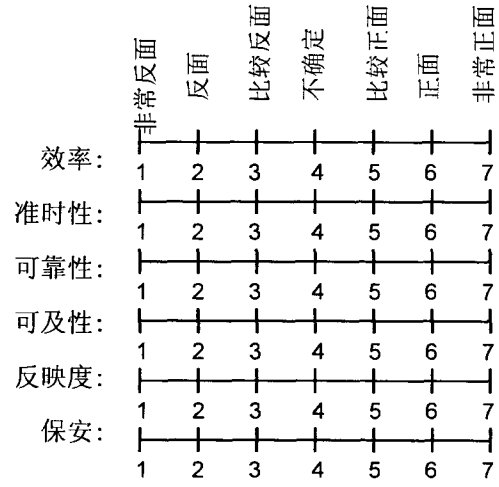
- 员工雇用前的背景调查
- 员工和约终止程序集中的安检
- 员工内部行为手册
- 员工保安意识的培训



保安措施	实施状态	对供应链的影响

9. 集装箱/单位装柜(ULD)的保安。
包括集装箱检查、 存贮和跟踪，及集装箱封印适用的管理、控制与核实。

I P N



如:-
卡车拖运
- 外部检查,集装箱与集装箱封印号码的核实,集装箱封印的情况
- 为空箱和散货上锁/安全存放

船运公司与集装箱封印科技
- 为船上的每一个集装箱打上集装箱封印并在运输过程中设立多个检查点
- 电子锁(E-Seals)/其它更尖端的集装箱上锁科技
- “Smart Box”-
  为集装箱安装坚固的封印和电子保安器材以便审查和记录任何非法开箱或拆封活动

10. 管理层的支持和保证。
高层管理人员对自身公司供应链保安计划的积极参与，并妥善的投入所需资源。

I P N

如:-
国内
- 成立国内保安委员会并实行定期的保安简报
- 将保安条款列入连续改善的计划和目标宣言
- 高层管理人员时刻与海外的商业伙伴保持联系，并掌握他们的营运方针
- 高层管理人员确保所有子公司都具有并实行整套的保安计划

全球性
- 设立国内保安经理，国际保安委员会，以便策划国际保安规则和评估标准

项目E. 应答者资料

E1. 请问您是如何知晓这项研究/这份问卷?

❑ 加拿大物流协会 (Canadian Supply Chain Logistics Association)
❑ 加拿大交通副刊 (Canadian Transportation Magazine)
❑ 2007年物流保安研究项目(SecuritySurvey2007@freightsecurity.ubc.ca)
❑ 个人联络
❑ 其他，请说明：_____

E2. 请问您位于哪个国家?

❑ 加拿大
❑ 中国
❑ 香港
❑ 新加坡
❑ 美国
❑ 其他 请说明: _____

E3. 请问您在贵公司的职位是什么?

E4. 请问贵公司的名字是什么? (可选择不答)。

E5. 请问哪个国家的文化对您的商业观点和看法有着最大的影响?

E6. 如果您想获取一份研究结果摘要报告书，请在此附上您的电子邮件地址。

* 物流服务供应商 *
中文版

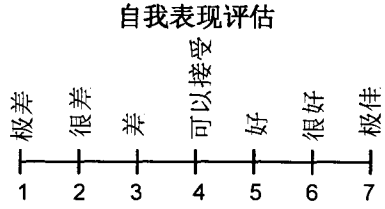
项目A. 企业营运表现自我评估

A1. 请问您是以什么身份对于以下的问卷进行作答？

❑ 正个公司　　❑ 我负责的营业单位

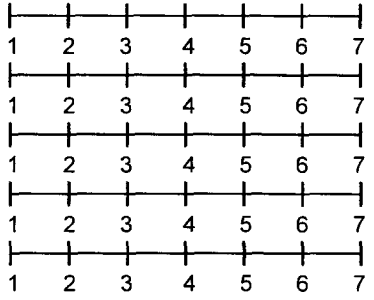
A2. 请问您认为贵公司在供应链保安/安全方面的表现如何？[“1”为“极差”和“7”为“极佳”]。

(保安/安全的定义在于贵公司的供应链受到下列状况影响的比例：1) 遗失 2) 盗窃 3) 破损 4) 恐怖袭击 5) 其它例如盗版、走私等。)



A3. 请问您认为贵公司在供应链以下各方面的表现如何？[“1”为“极差”和“7”为“极佳”]。

1. 效率(包括产品/服务配送成本)
2. 货物配送准时性（包括准时性，速度）
3. 运作的可靠性（运作的准确度，和在受到影响后恢复的速度与能力）
4. 货物的可及性（如货品存货量是否能及时应付订单需求）
5. 反应能力（包括对于客户要求的应变能力，运作调整的敏捷性）



项目B. 企业与营运资料

B1. 请问贵公司属于以下哪种企业类别？(请在所有适当的选项旁打勾)。

❑ 港务局(Port Authority)　❑ 海港总站(Terminal Operators)　❑ 第三方物流供应商(3rd Party Logistics Provider)
❑ 海洋运输公司 (Ocean Carrier)　❑ 海关报关公司 (Customs Broker)　❑ 海关总署 (Customs Authority)
❑ 承运商/运输公司(Trucking/Inter-modal Company)

❑ 货物混载业者(Consolidator)　❑ 货物运输业者(Forwarder)　❑ 其他，请说明：_____

B2. 请问贵司所服务的客户多数属于下列哪种供应链 ？(请在所有适当的选项打勾)。

❑ 快速消费品 (FMCG)　❑ 电子/高科技产品　❑ 易耗品/食品类
❑ 汽车/汽车零件　❑ 医药　❑ 化工业
❑ 重型器械　❑ 航空　❑ 其他，请说明：_____

B3. 请问贵公司所供应的产品是否包括危险品？

❑ 没有　❑ 有，请说明 % _____ %

B4. 请问贵公司所供应的产品运输方式是否有包括整集装箱(i.e. full container loads)？

❑ 没有　❑ 有，请说明 %: _____ %

B5. 请问贵公司的主要商船航线有哪些？请打勾。(不超过3个)。

❑ 亚洲内部(包括印度和南太平洋洲)　❑ 南北美洲内部　❑ 欧洲内部

❑ 跨太平洋（亚洲至北美洲）　❑ 跨太平洋（北美洲至亚洲）
❑ 跨太平洋（亚洲至南美洲）　❑ 跨太平洋（南美洲至亚洲）

❑ 亚欧（亚洲至欧洲）　❑ 亚欧（欧洲至亚洲）
❑ 跨大西洋（北美洲至欧洲）　❑ 跨大西洋（欧洲至北美洲）
❑ 跨大西洋（南美洲至欧洲）　❑ 跨大西洋（欧洲至南美洲）

❑ 亚洲至中东/非洲　❑ 中东/非洲至亚洲
❑北美洲至中东/非洲　❑ 中东/非洲至北美洲
❑ 南美洲至中东/非洲　❑ 中东/非洲至南美洲
❑欧洲至中东/非洲　❑中东/非洲至欧洲

❑ 请说明，其他_____

备注： ** 北美和中美洲(包括巴拿马及巴拿马以北的国家)*　** 南美洲(包括巴拿马以南的所有国家)*

B6. 请问贵公司2005年的营业额（美金）？请在以下选项作选择。

- ❑ 少于2,000万美金
- ❑ 介于2,000万到1亿美金
- ❑ 介于1亿到5亿美金
- ❑ 介于5亿到10亿美金
- ❑ 多于10亿美金

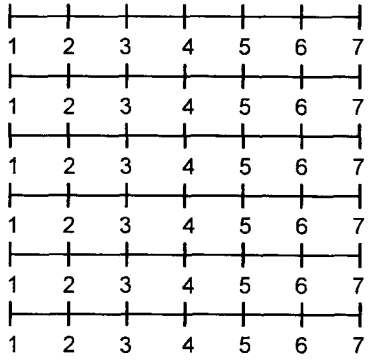
B7. 请问贵公司在以下哪几种供应链运作活动中拥有最后的决定/选择权？
如该选项拥有决定权，请在对应的“有最后决定权”栏里打“X”。
如该选项的决定权外包，请在对应的“外包最后决定权”栏里打“X”。
如该选项并不适用于贵公司的供应链，请在对应的“不适用”栏里打“X”。

供应链的不同方面	外包最后决定权	由最后决定权	不适用
供应商的选择（如制造商）			
从工厂以陆运或其他运输方式运载到起发地港口			
起发地的仓储			
起发地的货物混载			
起发地港口的清官			
起发地到港口目的地的跨边界运输（若需要）			
装货港口的选择			
起发地港口总站的选择			
运输公司的选择(如签订运输协议)			
目的地港口的选择			
目的地港口总站的选择			
目的地港口的清官			
从目的地港口到最终目的地的跨边界运输(若需要)			
目的地的仓储			
目的地的货物分拣			
从目的地港口以陆运或其他运输式运载到最终目的地			

B9. 请表明以下各策略对贵公司供应链管理的重要性？[1=完全不重要，　　2=不重要，　　3=不太重要，　　4=一般重要，5=比较重要，6=很重要，7=非常重要]。

物流和供应链策略

1. 效率(包括产品/服务配送成本)
2. 货物配送准时性（包括准时性，速度）
3. 运作的可靠性（运作的准确度，和在受到影响后恢复的速度与能力）
4. 货物的可及性（如货品存货量是否能及时应付订单需求）
5. 反应能力（包括对于客户要求的应变能力，运作调整的敏捷性）
6. 保安



项目C. 企业与营运考核指标

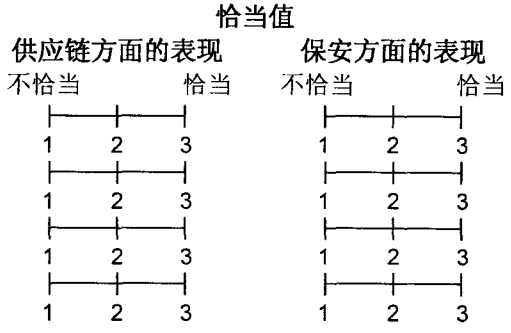
C1. 请问您认为是否应该为公司在供应链保安方面的表现/努力设定考核指标(KPI)吗?

❑ 应该　　❑ 不应该　　❑ 不确定/未定

C2. 接下来，请您以一至三分的标度[1=不恰当，2=无所谓/不确定，3=恰当]，在适当的“恰当值”栏里，表明贵公司对以下各考核指标(KPI)作为考核供应链方面的表现和保安方面的表现是否恰当。

考核指标 (KPI)

1. 资产利用率(如轮船，集装箱，货车)。
2. 保安审查(突发与非突发)的成绩。
3. 运作效率(如劳动生产力，每小时的捡货速度)。
4. 保安人员或员工没有遵守保安条例事件的次数与频率。



考核指标（KPI）

5. 运作方面的保险费用。

6. 库存量(仓库内或在途)。

7. 海关安检的次数与频率。

8. 物流成本对最终销售额的比例。

9. 传输与航运相关物流运作信息的准时性/率。

10. 非法或未批准侵入事件的次数与频率。

11. 订货至交货周转时间(如订单至收款的周期)。

12. 送货的准时性(如准时送货，文件的百分比)。

13. 急单处理和交货时间。

14. 清关时间(进口或出口)。

15. 物流相关信息的准确度(如运输文件，装箱单的传输)。

16. 服务出错和失败的次数/频率。

17. 期性安全审计的成绩。

18. 库存记录的准确度(如盘点的差异)。

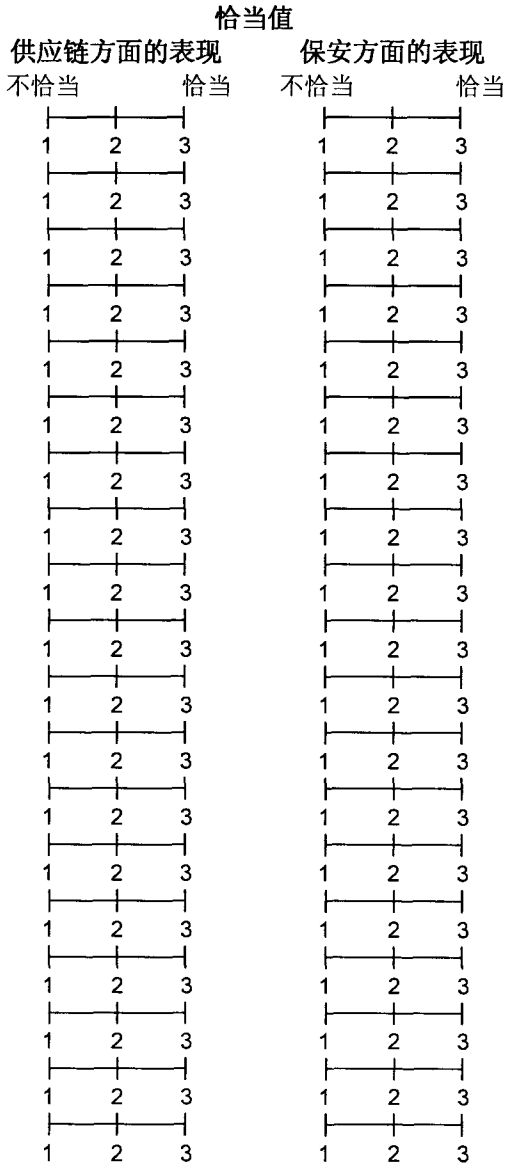
19. 开发票的准确度。

20. 货物偷窃或保安意外的发生次数与频率。

21. 货物损失赔偿数额。

22. 员工安全意外的次数与频率。

23. 过剩，短缺和破损(OS&D)的次数与频率。



考核指标 (KPI)

恰当值

	供应链方面的表现			保安方面的表现		
	不恰当		恰当	不恰当		恰当
24. 货物处理程序上的偏差的次数与频率(生产资源偏差)。	1	2	3	1	2	3
25. 无法及时完成的订单的次数与频率(如集装箱重新编排)。	1	2	3	1	2	3
26. 服务订单取消或拒绝的次数与频率。	1	2	3	1	2	3
27. 对客户问题的反应时间。	1	2	3	1	2	3
28. 解决客户问题的时间。	1	2	3	1	2	3
29. 客户满意度和意见的市场调查的成绩。	1	2	3	1	2	3
30. 服务订单符合率。	1	2	3	1	2	3
31. 满足客户特别要求的种类和数量比例。	1	2	3	1	2	3
32. 解决客户投诉的种类和数量比例。	1	2	3	1	2	3
33. 其它:	1	2	3	1	2	3
34. 其它:	1	2	3	1	2	3
35. 其它:	1	2	3	1	2	3

项目D. 供应链保安方面的应对措施

接下来，请您在下列各项中表明贵公司目前是否正在实施/已实施(I)，计划实施(P)或不打算实施(N)此保安措施。

同时，请您也为贵公司目前正在实施/已实施(I)和计划实施(P)的措施中表明供应链的表现，请在“对供应链的影响”栏里表明此措施在哪方面如何影响贵司在供应链的表现。请您以1至7分[1=非常反面，2=反面，3=比较反面，4=不确定，5=比较正面，6=正面，7=非常正面]，表示您的观点。

保安措施

实施状态

对供应链的影响

非常反面 | 反面 | 比较反面 | 不确定 | 比较正面 | 正面 | 非常正面

1. 保安相关或优秀运作的证书。

I P N

如:-

- Customs-Trade Partnership Against Terrorism (C-TPAT)(美国)
- Partners-In-Protection (PIP)(加拿大)
- Secure-Trade-Partnership (STP)(新加坡)
- Free and Secure Trade (FAST)(美国/加拿大)
- 资产运输保护协会(TAPA)
- 国际船只与港务设施保安(ISPS)

效率: 1 2 3 4 5 6 7

准时性: 1 2 3 4 5 6 7

可靠性: 1 2 3 4 5 6 7

可及性: 1 2 3 4 5 6 7

反映度: 1 2 3 4 5 6 7

保安: 1 2 3 4 5 6 7

2. 提前数据/信息。

I P N

通过资讯安全传输科技提前传输信息和资料,
以符合官方在这方面的条规和协助各方查出货物抵港前的任何反常现象/差误。

如:-

- 24-hours Advance Manifest Rule(美国)
- Advanced Commercial Information(加拿大)
- 采用可追踪/安全电子数据传输系统
- 先遣运输通知(ASNs)

效率: 1 2 3 4 5 6 7

准时性: 1 2 3 4 5 6 7

可靠性: 1 2 3 4 5 6 7

可及性: 1 2 3 4 5 6 7

反映度: 1 2 3 4 5 6 7

保安: 1 2 3 4 5 6 7

保安措施

实施状态

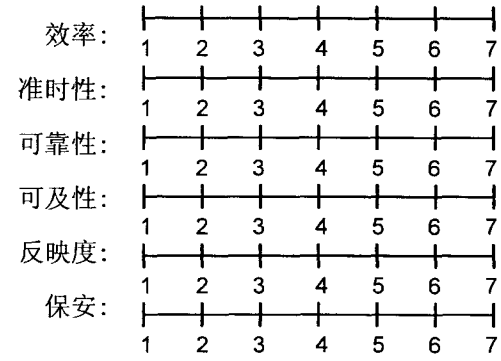
对供应链的影响

非常反面 反面 比较反面 不确定 比较正面 正面 非常正面

3. 对商业伙伴的要求。

与商业合作伙伴共同建立/实施各种保安措施，并确保对措施的遵守/服从。

I P N



如:-

对供应商/生产商

- 要求服从保安方面的准则
- 商务契约责任
- 工厂保安证书/证明要求

对物流供应商

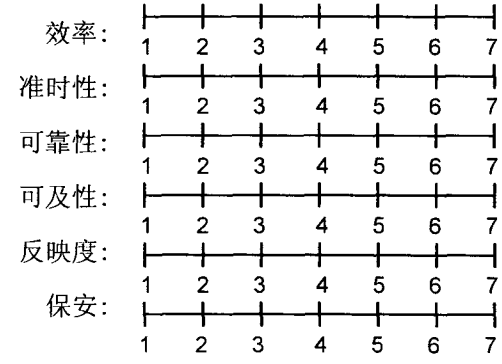
- 海外业务实地代表
- 禁止转包
- 要求人员背景调查
- 商务契约责任/供应商选择标准

对客户

- 通过对客户教育以防止产品滥用或误用
- 核实企业伙伴资料，信誉
- 成立惯例性收货卸货点

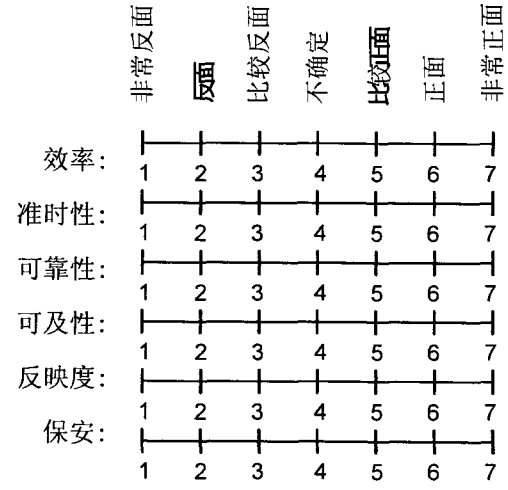
4. 保安意识与保安程序/科技培训。

I P N



如:-

- 使用多层警戒
- 对员工传达恐怖活动方面的信息
- 保安事件调查，检查等方面的专业培训
- 商业伙伴的相关培训
- 设立奖励以鼓励员工申报事件
- 和当地司法机关保持紧密合作

保安措施	实施状态	对供应链的影响
5. 保安程序。 将保安注入公司营运策划的一部分并设立相关的管理系统(如责任规划、检查和制衡系统等)。 如:- 风险评估/分析与事件管理 • 设立内部保安人员网络和整套的持续改善计划 • 成立事件档案库和突发事件的处理章程，如对应可疑活动，全球/当地事件 • 紧急疏散计划 货物处理 • 采用后备地址寄存码的扫描，以便查出货物处理上的差错和确保只对已向海关申报的货物进行装箱 • 特殊货物包装，如印有公司标志的胶带 • 调动收货/出货员工	I P N	
6. 实际进出保安科技与权限控制。 禁止营运设施的非法/未许可的进出入，控制人员流动和保护企业财产。 如:- • 24小时保安人员/警察巡逻 • 安装具有磁性传感的围栏/门，警报系统 内部员工 • 采用生物科技来辨认身份，颜色代码制服 • 有相片的身份证明卡和密码控制锁 访客和送货/提货(包括邮件) • 要求访客到访前的预检和核实身份的真实性 • 身份证明卡和访客卡调换 • 成立提货日程表与卡车司机等待区 • 突检人员/邮包/邮件/卡车	I P N	

保安措施

实施状态

对供应链的影响

非常反面 | 反面 | 比较反面 | 不确定 | 比较正面 | 正面 | 非常正面

7. 追踪/监视科技(运输过程的保安)。

检查并追踪整个运输过程，以确保所适用的运输系统不被恐怖份子/其他犯罪者滥用。

I P N

效率: 1 2 3 4 5 6 7

准时性: 1 2 3 4 5 6 7

可靠性: 1 2 3 4 5 6 7

可及性: 1 2 3 4 5 6 7

反映度: 1 2 3 4 5 6 7

保安: 1 2 3 4 5 6 7

如:-

卡车货运

- 成立一套能够探测集装箱堆场/提卸货物处内非寻常/延长逗留事件
- 全球定位系统 (GPS)，运输货车信息收发器
- 在车内安装警报系统，安排安保人员护送高价值或敏感货物
- 安排并设定运输路线与后备路线
- 观察货车油消耗量以发现任何可疑的路线偏差
- 员工定期调动以防止内部合谋

船运公司

- 控制器材的适用
- 网上船运追踪工具/系统
- 监察偷渡者
- 卫星勘测、 远距离侦察

8. 员工的保安程序。

I P N

效率: 1 2 3 4 5 6 7

准时性: 1 2 3 4 5 6 7

可靠性: 1 2 3 4 5 6 7

可及性: 1 2 3 4 5 6 7

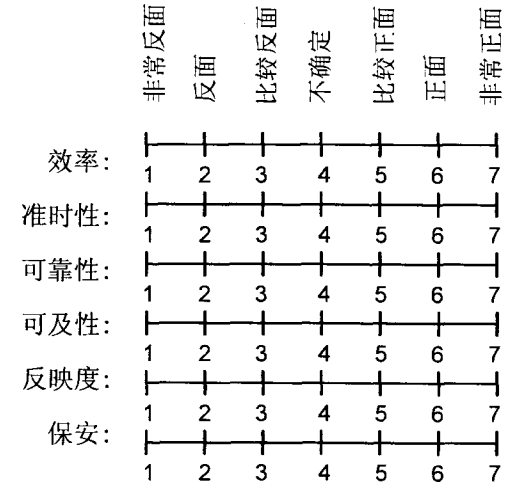
反映度: 1 2 3 4 5 6 7

保安: 1 2 3 4 5 6 7

如:-

- 员工雇用前的背景调查
- 员工和约终止程序集中的安检
- 员工内部行为手册
- 员工保安意识的培训

保安措施	实施状态	对供应链的影响



9. 集装箱/单位装柜(ULD)的保安。

I P N

包括集装箱检查、 存贮和跟踪，及集装箱封印适用的管理、控制与核实。

如:-

卡车拖运

- 外部检查,集装箱与集装箱封印号码的核实,集装箱封印的情况
- 为空箱和散货上锁/安全存放

船运公司与集装箱封印科技

- 为船上的每一个集装箱打上集装箱封印并在运输过程中设立多个检查点
- 电子锁(E-Seals)/其它更尖端的集装箱上锁科技
- “Smart Box”-
  为集装箱安装坚固的封印和电子保安器材以便审查和记录任何非法开箱或拆封活动

10. 管理层的支持和保证。

I P N

高层管理人员对自身公司供应链保安计划的积极参与，并妥善的投入所需资源。

如:-

国内

- 成立国内保安委员会并实行定期的保安简报
- 将保安条款列入连续改善的计划和目标宣言
- 高层管理人员时刻与海外的商业伙伴保持联系，并掌握他们的营运方针
- 高层管理人员确保所有子公司都具有并实行整套的保安计划

全球性

- 设立国内保安经理，国际保安委员会，以便策划国际保安规则和评估标准

项目E. 应答者资料

E1. 请问您是如何知晓这项研究/这份问卷?

❑ 加拿大物流协会(Canadian Supply Chain Logistics Association)
❑ 加拿大交通杂志(Canadian Transportation Magazine)
❑ 2007年物流保安研究项目(SecuritySurvey2007@freightsecurity.ubc.ca)
❑ 个人联络
❑ 其他，请说明：_____

E2. 请问您位于哪个国家?

❑ 加拿大
❑ 中国
❑ 香港
❑ 新加坡
❑ 美国
❑ 其他 请说明: _____

E3. 请问您在贵公司的职位是什么?

E4. 请问贵公司的名字是什么?（可选择不答）。

E5. 请问哪个国家的文化对您的商业观点和看法有着最大的影响?

E6. 如果您想获取一份研究结果摘要报告书，请在此附上您的电子邮件地址。

APPENDIX C

KPI Definitions

LIST OF KPIs

AssetUtilize	Asset utilization
SecurityAudit	Results from a periodic security audit
OpsEfficiency	Operations efficiency
PolicyViolations	Frequency of violations of security policies
InsurancePremiums	Insurance premiums
InventoryLevel	Level of inventory in warehouse
InspectionCost	Costs of customs inspections
LogCostSavings	Logistics costs savings amount
ShipmentInfo	On-time transmission of shipment information
UnauthorizedEntry	Frequency of unauthorized entry into restricted areas/zones
FulfillmentLT	Fulfillment lead-time
OTDelivery	On-time delivery
ExpeditedOrders	Frequency of expedited orders
CustomsLT	Customs clearance lead-time
InfoAccuracy	Accuracy of information
ServiceErrors	Frequency of service errors
SafetyAudit	Results from periodic safety audit
InventoryAccuracy	Accuracy of inventory records
InvoiceAccuracy	Accuracy of invoices
Pilferage	Pilferage amounts and frequency
FreightClaims	Amount and frequency of freight claims
SafetyAccidents	Frequency of safety related accidents
OSD	Cargo overages, shortages and damages
OpsDeviation	Deviation in operations capacity
BackOrders	Percentage of backorders
Cancellations	Percentage of order cancellations
ProblemResponse	Problem response lead-time
ProblemResolution	Problem resolution lead-time
FeedbackSurvey	Results from periodic customers' feedback survey
FillRate	Percentage of orders filled on first instance
SpecialRequests	Ability to handle customers' special requests
Complaints	Frequency of customers' complaints

APPENDIX D

Citations of Studies Used in Determining SCP KPIs

Citations of Studies from Keller et al. (2002):

Brown, James R., Robert F. Lusch, and Laurie P. Smith (1991), "Conflict and Satisfaction in an Industrial Channel of Distribution," *International Journal of Physical Distribution and Logistics Management*, Vol. 21, No. 6, pp. 15-26.

Crosby, Leon and Stephen A. LeMay (1998), "Empirical Determination of Shipper Requirements for Motor Carrier Services: SERVQUAL, Direct Questioning, and Policy Capturing Methods," *Journal of Business Logistics*, Vol. 19, No. 1, pp. 139-153.

Daugherty, Patricia J., Matthew B. Myers, and Chad W. Autry (1999), "Automatic Replenishment Programs: An Empirical Examination," *Journal of Business Logistics*, Vol. 20, No. 2, pp. 63-82.

Daugherty, Patricia J., Theodore P. Stank, and Alexander E. Ellinger (1998), "Leveraging Logistics/Distribution Capabilities: The Effect of Logistics Service on Market Share," *Journal of Business Logistics*, Vol. 19, No. 2, pp. 35-51.

Emerson, Carol J. and Curtis M. Grimm (1996), "Logistics and Marketing Components of Customer Service: An Empirical Test of the Mentzer, Gomes, and Krapfel Model," *International Journal of Physical Distribution and Logistics Management*, Vol. 26, No. 8, pp. 29-42.

Fawcett, Stanley E., Roger Calantone, and Sheldon R. Smith (1996), "An Investigation of the Impact of Flexibility on Global Reach and Firm Performance," *Journal of Business Logistics*, Vol. 17, No. 2, pp. 167-196.

Fawcett, Stanley E. and Sheldon R. Smith (1995), "Logistics Management and Performance for United States-Mexican Operations Under NAFTA," *Transportation Journal*, Vol. 34, No. 3, pp. 25-34.

Fawcett, Stanley E., Sheldon R. Smith, and M. Bixby Cooper (1997), "Strategic Intent, Measurement Capability, and Operation of Success: Making the Connection," *International Journal of Physical Distribution and Logistics Management*, Vol. 27, No. 7, pp. 410-421.

Gassenheimer, Jule B., Jay U. Sterling, and Robert A. Robicheaux (1989), "Long-term Channel Member Relationships," *International Journal of Physical Distribution and Materials Management*, Vol. 19, No. 12, pp. 15-28.

Goldsby, Thomas J. and Theodore P. Stank (2000), "World Class Logistics Performance and Environmentally Responsible Logistics Practices," *Journal of Business Logistics*, Vol. 21, No. 2, pp. 187-208.

Lambert, Douglas M. and Thomas C. Harrington (1989), "Establishing Customer Service Strategies Within the Marketing Mix: More Empirical Evidence," *Journal of Business Logistics*, Vol. 10, No. 2, pp. 44-60.

Maloni, Michael and W. C. Benton (2000), "Power Influences in the Supply Chain," *Journal of Business Logistics*, Vol. 22, No. 1, pp. 49-73.

Matear, Sheelagh and Richard Gray (1993), "Factors Influencing Freight Service Choice for Shippers and Freight Suppliers," *International Journal of Physical Distribution and Logistics Management*, Vol. 23, No. 2, pp. 25-35.

McGinnis, Michael A. (1979), "Shipper Attitudes Toward Freight Transportation Choice: A Factor Analytic Study," *International Journal of Physical Distribution and Materials Management*, Vol. 10, No. 1, pp. 25-34.

McGinnis, Michael A. (1990), "The Relevant Importance of Cost and Service in Freight Transportation Choice: Before and After Regulation," *Transportation Journal*, Vol. 30, No. 1, pp. 12-19.

McGinnis, M., T. M. Corsi, and M. J. Roberts (1981), "A Multiple Criteria Analysis of Modal Choice," *Journal of Business Logistics*, Vol. 2, No. 2

McGinnis, Michael A. and Johnathan W. Kohn (1990), "A Factor Analytical Study of Logistics Strategy," *Journal of Business Logistics*, Vol. 11, No. 2, pp. 41-63.

Menon, Mohan K., Michael A. McGinnis, and Kenneth B. Ackerman (1998), "Selection Criteria for Providers of third-Party Logistics Services: An Exploratory Study," *Journal of Business Logistics*, Vol. 19, No. 1, pp. 121-137.

Mentzer, John T., Daniel J. Flint, and John L. Kent (1999), "Developing a Logistics Service Quality Scale," *Journal of Business Logistics*, Vol. 20, No. 1, pp. 9-32.

Mentzer, John T. and Brenda P. Konrad (1991), "An Efficiency/Effectiveness Approach to Logistics Performance Analysis," *Journal of Business Logistics*, Vol. 12, No. 1, pp. 33-62.

Monczka, Robert M., Thomas J. Callahan, and Ernest L. Nichols, Jr. (1995), "Predictors of Relationships Among Buying and Supplying Firms," *International Journal of Physical Distribution and Logistics Management*, Vol. 25, No. 10, pp. 45-59.

Novack, Robert A., Lloyd M. Rinehart, and C. John Langley, Jr. (1994), "An Internal Assessment of Logistics Value," *Journal of Business Logistics*, Vol. 15, No. 1, pp. 113-152.

Pearson, J. N. and J. Semeijn (1999), "Service Priorities in Small and large Firms Engaged in International Logistics," *International Journal of Physical Distribution & Logistics Management*, Vol. 29, No. 3, pp. 181.

Raghunathan, T. S., Prabir K. Bagchi, and Edward J. Bardi (1998), "Motor Carrier Services: The U.S. Experience," *International Journal of Physical Distribution and Materials Management*, Vol. 18, No. 5, pp. 3-7.

Scannell, Thomas V., Shawnee K. Vickery, and Cornelia L. Dröge (2000), "Upstream Supply Chain Management and Competitive Performance in the Automotive Supply Industry," *Journal of Business Logistics*, Vol. 21, No. 2, pp. 23-48.

Semeijn, Jake (1995), "Service Priorities in International Logistics," *International Journal of Logistics Management*, Vol. 6, No. 1, pp. 27-36.

Sharma, Arun and Douglas M. Lambert (1990), "Segmentation of Markets Based on Customer Service," *International Journal of Physical Distribution and Logistics Management*, Vol. 20, No. 7, pp. 19-27.

Stank, Theodore P., Patricia J. Daugherty, and Alexander E. Ellinger (1996), "Information Exchange, Responsiveness and Logistics Provider Performance," *International Journal of Logistics Management*, Vol. 7, No. 2, pp. 43-57.

Stank, Theodore P., Scott B. Keller, and Patricia J. Daugherty (2001), "Supply Chain Collaboration and Logistical Service Performance," *Journal of Business Logistics*, Vol. 22, No. 1, pp. 29-48.

Stank, Theodore P. and Charles W. Lackey, Jr. (1997), "Enhancing Performance Through Logistical Capabilities in Mexican Maquiladora Firms," *Journal of Business Logistics*, Vol. 18, No. 1, pp. 91-123.

Sterling, J. U. and D. M. Lambert (1987), "Establishing Customer Service Strategies Within the Marketing Mix," *Journal of Business Logistics*, Vol. 8, No. 1, pp. 1.

Supply Chain Council (2006), *Supply-Chain Operations Reference-model*, Version 8.0.

Zinn, Walter and Peter C. Liu (2001), "Consumer Response to Retail Stockouts," *Journal of Business Logistics*, Vol. 22, No. 1, pp. 49-71.

Citations of Recent Studies on Supply Chain Security:

Banomyong, R. (2005), "The Impact of Port and Trade Security Initiatives on Maritime Supply-Chain Management," *Maritime Policy and Management*, Vol. 32, No. 1, pp. 3-13.

Blake, Marilyn A. (2003), "Safety: It's No Accident," *Rural Telecommunications*, Vol. 22, No. 3, pp. 52.

European Conference of Ministers of Transport (ECMT) (2005), *Container Transport Security Across Modes*.

Koch, R. (2004), "A Secure Supply Chain Blueprint," *Unisys White Paper Series*.

Langhoff, T., N. Pillai, and R. Koch (2005), "Secure Commerce Roadmap – The Industry's View for Securing Commerce," *Unisys Technical White Paper Series*.

Peleg-Gillai, B., G. Bhat, and L. Sept (2006), "Innovators in Supply Chain Security," *The Manufacturing Innovation Series*, The Manufacturing Institute.

Price, W. (2004), "Reducing the Risk of Terror Events at Seaports," *Review of Policy Research*, Vol. 21, No. 3, pp. 329.

Rice, J. B. Jr. and P. W. Spayd (2005), "Investing in Supply Chain Security: Collateral Benefits," *IBM Center for the Business of Government*, Special Report Series.

Sheffi, Y. (2001), "Supply Chain Management Under the Threat of International Terrorism," *The International Journal of Logistics Management*, Vol. 12, No. 2, pp. 1-11.

Willis, H. H. and D. S. Ortiz (2004), "Evaluating the Security of the Global Containerized Supply Chain," *RAND Technical Report Series.*

Wolfe, Michael (2004), "The Dynamics of Supply Chain Security," *The Monitor (Center for International Trade and Security (CITS))*, Vol. 10, No. 2, pp. 15-20.

APPENDIX E

Responses Gathered from Field Interviews

Variable	Company A	Company B	Company C	Company D	Company E	Company F	Company G
Location	Singapore	Singapore	Singapore	Shanghai	Shanghai	Shanghai	Shanghai
Organization Type	Terminal Operator	Freight Consolidator/ Forwarder 3PL	Dealing with / handling customs matters	Port	Freight Consolidator/ Forwarder 3PL	Port	Terminal Operator
Interviewee's Key Role & Responsibilities	Handle container security initiatives, regulations, ITS and commercial services	Handle Asia & Middle East operations and security projects	Develop & implement security related matters	Oversee and manage all import and export activities	Lead security solutions (system, manpower and procedures) and investigation	Manage personnel and port safety and security department.	Vessel security inspection / certification. Security incidents investigation & resolution.
Key Trade Routes	Asia-Europe Intra Asia	Asia-N.America Asia-Europe Intra-Asia	US, China and Japan	Intra-Asia (60%) Asia-Europe (30%) Asia-N. America (10%)	Intra-Asia Asia-Europe Asia-North America	Intra-Asia Asia-N.America	Intra-Asia Asia-N.America
2006 Annual Revenue (US$)	> 1 billion	> 1 billion	> 1 billion	100 - 500 million	> 1 billion	Cannot disclose	Cannot disclose
Global Employee Count	> 5,000	500 – 1,000	100 – 500	100 – 500	1,000 – 5,000	> 5,000	500 – 1,000
Span of Supply Chain Control	Narrow	Wide	Not Applicable	Average	Wide	Narrow	Narrow
Value Proposition	Connectivity Efficiency Timeliness	Responsiveness Operations competency People & knowledge Timeliness	Integrity Commitment Responsiveness	Cannot disclose	Network coverage People & knowledge	Efficiency Safety and security	Service reliability Efficiency (e.g. turnaround time) Trust & integrity
Security as a Business Driver?	Yes	Maybe	Yes	No	Maybe	Yes	Yes
Importance of Security	Very Important	Very Important	Very Important	Not so Important	Very Important	Very Important	Very Important

Variable	Company A	Company B	Company C	Company D	Company E	Company F	Company G
SCP KPIs							
- Efficiency	Vessel rate Control crane rate	Container utilization		Supplier pricing	Receiving productivity Space utilisation Picking productivity		# moves per man hour
- Timeliness	Berth on arrival	Transit times Document flow Warehouse turnaround time Truck turn time On-time delivery	Permit turnaround time		On-time delivery		Container loading and unloading Berth on arrival On time departure Turnaround time within 24hours
- Responsiveness	Service failures	24hrs respond guideline # of service failures	Compliment-complaint ratio	Responsiveness to problems. Ability to propose solutions/ recommendations	# customer complaints		
- Availability				Accommodating volumes during peak season.	Order fill rate		
- Reliability		Accuracy of information Claims per PO	Post shipment sampling checks	Accuracy of paperwork submission	# accidents per employee Cycle counting variance	Tally checks/ Info accuracies - Document discrepancies	Accuracy of loading # of safety incidents
SCP Overall Measure	Throughput	Contribution margin	Traders' satisfaction index	-	-	-	-
Security KPIs	# incidents Random audit checks	# incidents # personnel trained for security Facility audit results	Collateral benefits # of inspections Customs clearance time	# thefts / pilferage Amount of damage	Security guards performance survey Property/cargo loss # supplier security incompliance Security training attendance.	Pilot testing results of technology # of unauthorised personnel # of accidents within port # of complaints from customers	Safety audit results from Ministry of Transport. # of incidents / personnel accidents (commented security is part of safety)

Variable	Company A	Company B	Company C	Company D	Company E	Company F	Company G
Current Security Initiatives	Certifications with voluntary programs such as C-TPAT. E-seals testing. Biometrics for access control. Transponders for truckers. Drivers ID card. Monitor truck turnaround time. Police patrol. 24hr CCTV monitoring. Pre-employment checks. Fencing / gates / locks.	Certifications Biometrics for access control GPS and cell phone communications for truckers. CCTV monitoring. Pre-employment checks. Termination procedures. Fencing / gates / locks. Written procedures. Handbook for vendors and business partners. Personnel security training.	Not applicable	Insurance purchase. Pre-employment background checks. Security escorts.	TAPA certification Instituting security procedures Tracking system Security escorts for certain products Route design Restricting access to certain areas Visitor pre-clearance	ISPS certification Access controls for employees and visitors Dedicated trucker waiting area Port entry checking procedures Own dedicated trucks for draying containers within port area (mention that as long as an initiative is recognised by international standards, the organisation will look into adoption)	ISPS certification H986 inspection Scanning 24hr CCTV Police boat patrol Joint security drills and contingency plans with marine police Increase security staff strength ID access card IF cards for all certified container trucks Monitor truck turnaround time within port GPS patrol cars Infra-red fencing Procedures for checking seal # discrepancies Certifying ship supplies suppliers
Future Security Initiatives	Employee awareness and outreach.					Gamma rays inspections E-seals RFID	Connect monitoring systems among terminal, port and carrier.
Security as a holistic effort?	Yes	Yes	Yes	Yes	Yes	Yes	Yes
How to influence channel partners in security effort?	Engage legislative counterparts. Use security as a competitive edge over competitors.	Require certifications from all partners. Train partners for compliance. Participate in industry-led security programs.	Develop and institute security programs.	Part of basic requirements to do business. Require equivalent certification.	Sharing experiences and communicate	Employ legal punishment for non-complying shippers. Participate in development of security legislation.	Communications and joint programs with carriers Contractual obligations

Variable	Company H	Company I	Company J	Company K	Company L	Company M	Company N
Location	Shanghai	Shanghai	Shanghai	Shanghai	Shanghai	Singapore	Singapore
Organization Type	Freight Consolidator / Forwarder 3PL	Shipper	Shipper	Shipper	Shipper	Shipper	Ocean Carrier
Interviewee's Key Role & Responsibilities	North China consolidation operations to N.America	General manager	Export and import manager	Export and import supervisor	President	Supply chain manager	Vessel operations and security
Key Trade Routes	Asia-N. America	Asia-Europe N. America-Asia	Asia-N. America (Exports) Intra-Asia (Imports)	Asia-N. America Asia-Europe	Asia-N. America (majority FOB Shanghai)	Europe-Asia N. America-Asia Intra Asia	Intra-Asia Asia-N. America Asia-Europe
2006 Annual Revenue (US$)	100 – 500 million	> 1 billion	20 – 100 million	100 – 500 million	500 million – 1 billion	> 1 billion	> 1 billion
Global Employee Count	100 - 500	500 – 1,000	1,000 – 5,000	1,000 – 5,000	100 - 500	> 5,000	> 5,000
Span of Supply Chain Control	Wide	Wide	Average	Narrow	Wide	Average	Narrow
Value Proposition	One-stop shop Skills and knowledge Global network and capabilities	Quality Environmentalism	Quality Production scale capability and production experience	Quality Price Customer service	SCM People and knowledge IT system Quality and cost Innovation and scale flexibility	SCM Operations reliability Innovation / R&D.	IT automation Service reliability
Security as a Business Driver?	Yes	No	No	No	Maybe	No	Yes
Importance of Security	Quite Important	Very Important	Quite Important	Quite Important	Quite Important	Very Important	Extremely Important

Variable	Company H	Company I	Company J	Company K	Company L	Company M	Company N
SCP KPIs							
- Efficiency	CBM per headcount Overtime	Customer cost savings	Production time per piece of apparel	Production time per piece of apparel	Production throughput Manufacturing defect rate	Cycle time of order delivery	Container moves per hour Fuel consumption
- Timeliness	On-time documents pouching / transmission of info / billing	Delivery lead times Delivery precision	On-time completion of orders	On-time completion of orders	Order completion on time	Delivery on-time performance (based on schedules)	BL timeliness Transit time Vessel turnaround time Depot delay time
- Responsiveness	Respond to customer enquires within 48 hrs # customer claims	Promise to delivery date	Respond to customer complaints	Respond to customer complaints	Responsiveness to customer enquiries		Responsiveness to customer enquiries
- Availability		Capacity planning with carriers Availability of packaging				Inventory availabilities such as back orders and order fill rate.	Equipment availability Ship stoppage # detentions at port # ship accidents
- Reliability	AMS accuracy Suppliers exception management	Invoicing accuracy Deviation management	Quality checks and controls	Quality checks and controls	Quality checks and controls		
SCP Overall Measure	Contribution margin	Customer satisfaction survey	Customer satisfaction survey	Customer satisfaction survey	Business volume growth	Customer satisfaction survey	
Security KPIs	Periodic audit results (commented # of pilferage and thefts are too rare to be effective KPIs for security)	Periodic operations and safety audit Freight loss / damage (only if cause can be identified)	Audit results # safety incidents. Commented that security is similar to safety.		Certifications # of accidents / disasters # of thefts # of strikes	Freight loss by forwarder	# security incidents Vessel security audit results # detentions at port Vessels spot inspection results

Variable	Company H	Company I	Company J	Company K	Company L	Company M	Company N
Current Security Initiatives	On-route tracking via GPS/cell Trucker ID checks Monitor truck turnaround time Visitor log/badge Pre-employment checks Written procedures for employees truckers Awareness training Monthly security broadcasts Fencing and locks Security guard patrols Separate parking area for private vehicles Password change every 45 days Virus protection firewall	ISPS certification Safety and security procedures for terminals and operations Safer container locks Cargo tracking system GPS equipped local delivery vehicles Employee ID cards Visitor pre-clearance Driver safety measures and practices	CCTVs for 24hours monitoring. ID card access. Security checks and inspections for trucks entering factories. Rely on local logistics service providers on security certifications. Safety and fire prevention procedures, awareness training and drills. Basic locks and fencing.	ID card access Gate at factory Security guard patrols at factory	Basic security for personnel and cargo such as CCTVs, security patrol, ID card access, visitor control log. Internal control procedures such as invoice checks, no lending of export licenses, accounting audits and compliance with government regulations. Commented that measures are more reactive than preventive now due to low frequency of occurrence.	Basic company security such as ID card access and employee procedural handbook. Ensure safety standards within company is stricter than international requirements. Background checks on delivery vehicles and drivers but this is more for safety purposes rather than security.	C-TPAT, ISPS certification Participation in security initiatives such as CSI, SFI. Surveillance cameras IMO required panic buttons on board all vessels Security SOP Gangway watch Visitor escorts Single entry to vessel at berth Visitor pre-clearance Ensure security certification for chartered ships Automatic Identification System (AIS) on board all vessels Security training
Future Security Initiatives			Depends on customers' requests but will only comply with reasonable ones	Depends on customers' requests but will only comply with reasonable ones	Depends on customer requirements	24 hours monitoring	Other certification programs and probably RFID
Security as a holistic effort?	Yes	Yes	Yes	Yes	Yes	Yes	Yes
How to influence channel partners in security effort?	Formalize as contractual obligations Periodic audits	Communications and education to change mindset	For suppliers: set up security requirements as pre-requisites to doing business.		Communications and cooperation but customers should drive the initiatives.	Unless proven measurable impacts, it will be tough for his industry to readily adopt any out of self-interests.	Institute security as business requirements Communicate and participate in security activities.

Variable	Company O	Company P	Company Q	Company R	Company S	Company T	Company U
Location	Singapore	Singapore	Singapore	Vancouver	Vancouver	Vancouver	Vancouver
Organization Type	Shipper	3PL	3PL	Shipper	Shipper	Terminal Operator	Shipper
Interviewee's Key Role & Responsibilities	Internal Security Consultant	Business development and account management - US military supply in Iraq and weaponry reverse logistics	Regional Security Manager, Asia Pacific	Logistics Analyst handling import customs operations	Marine Transportation Manager + Transportation Analyst	VP Operations + Manager, Security and Labour Relations	Director - Warehousing + Transportation Analyst
Key Trade Routes	Intra-Asia	Asia-Europe	All	Asia-N. America Intra N. America Only mail orders are international.	N. America-Asia (Japan and China) N. America-Europe (UK)	6 Services: West Coast to Asia	Within Canada (65%) USA (20%) Asia (esp China) (15%)
2006 Annual Revenue (US$)	> 1 billion	> 1 billion	100 - 500 million	100 - 500 million	> 1 billion	20 – 100 million	> 1 billion
Global Employee Count	> 5,000	> 5,000	1,000 – 5,000	500 – 1,000	> 5,000	100 – 500	> 5,000
Span of Supply Chain Control	Wide	Wide	Wide	Wide	Wide	Narrow	Wide
Value Proposition	SCM – Reliability and timeliness	Assets Flexibility of service offering	Good dollar value for customers	SCM – Timeliness of delivery and reliability of service	SCM – Timeliness and availability of supply	Handling capacity Efficiency and customer service	SCM – Timeliness and efficiency of fulfillment
Security as a Business Driver?	Maybe	Yes	Yes	Not at the moment	Not at the moment	Not at the moment	Not at the moment
Importance of Security	Very Important	Extremely Important	Very Important	Very Important	Very Important	Very Important	Very Important

Variable	Company O	Company P	Company Q	Company R	Company S	Company T	Company U
SCP KPIs							
- Efficiency	Logistics cost per unit Warehouse productivity measures	# case pick/ orders/receipts per man hour Fuel consumption Space utilisation Pallet occupancy rate	unable to go into specific details		Freight cost per unit Mill productivity	Container moves per hour Crane control rate Insurance premiums	Cost per case handled Cases handled per hour % Overtime vs Regular Time
- Timeliness	Delivery lead time Delivery on time %	On time delivery % Truck turnaround time	unable to go into specific details		% On-time orders Order cycle time	Truck turnaround time Rail dwell time	On time arrival of inbound orders/ vessels/ delivery to store
- Responsiveness		# customer complaints	unable to go into specific details		Customer satisfaction survey	Keep track of occurrence of customers' "Nos"	Personnel customer service
- Availability	Order fill rate	Order fill rate	unable to go into specific details		Order fill rate Supply rate from mills		Manages most out of stock situations as exceptions
- Reliability	Forecast accuracy Quality control checks	Inventory accuracy (cycle counting)	unable to go into specific details	Claim history	Safety statistics	Safety statistics such as loss time incident frequency	Accuracy of orders received Quality checks
SCP Overall Measure		Net profit		Order fill rate	Inventory turns		Cost per case / unit handled
Security KPIs	Losses # of accidents/ security incidents ROI on security investments (return calculated as the potential savings from potential losses)	# of truck kidnaps / loss / blowups # of personnel casualties	Trade Compliance	Staff awareness training OS&D Pilferages/thefts Freight risk assessment -> insurance premiums	Customs clearance lead time. Thefts/claims/losses are usually more due to human errors and therefore cannot be used to indicate security.	# container crimes # security incidents such as thefts, illegal site entry # inspections by guard force Compliance with security procedures	Safety is a good indication of security # & frequency of accidents Safety audit results Loss/damage/theft Claims Shrinkages Insurance premiums

Variable	Company O	Company P	Company Q	Company R	Company S	Company T	Company U
Current Security Initiatives	Basic security such as CCTVs, security guard patrol, control card access, visitor pre-clearance and visitor pass. C-TPAT compliant Periodic audits Decentralised security department Partner selection procedures Contractual obligations	RFID seals GPS trucks US convoy escorts 24hr monitoring at CCTVs Security patrols Security SOPs Personnel crisis training Pre-employment checks Double fencing - with barbed wire Alarm system for break-ins	All of the initiatives mentioned in the questionnaire.	All gates and access doors to DC are securely locked after hours. All visitors to report to receiving office. All access doors monitored. Adequate lighting. Alarm system. PIP certification	Contractual obligations for truckers to be WCB certified Security procedures Container checking procedures during Surveliance cameras Mandatory visitor pre-clearance Mandatory safety gear and safety officer Fencing and gates	ISO 28000 Vessel safety inspection Security declaration by all incoming vessels CCTVs Alarm systems 24/7 guard patrol Mobile patrol Driver ID cards Security procedures Corporate endorsed security manuals Staff awareness training	FAST/GPS truckers Container inspections Controlled key access seals Spot checks Track truck turnaround time Gating over weekend/night hrs Mobile security Employee bag check at end of day CCTVs Inventory yard check Vehicle monitoring system - black box Drivers safety training
Future Security Initiatives	Depends on operating environment, product type and cost is a huge consideration.	Mention that cost of basic security can be borne by service provider but beyond that should be the responsibility of the customer.		New DC will have fencing, CCTVs, security swipe cards for entry. No staff on duty allowed to bring in/take out any items. Security procedures Inbound goods inspected and verified against shipping docs.	C-TPAT certification by end of the year so depends on what the requirements are. C-TPAT certification by end of the year so depends on what the requirements are.		
Security as a holistic effort?	Yes	Yes	Yes	Yes	Yes	Yes	Yes
How to influence channel partners in security effort?	Set up contractual obligations and build relationship building.	Education and communications.	Higher management involvement	Education and communications Join trade associations	Obtaining internationally recognized certifications.		Education and communications. Really depends on market dynamics.

APPENDIX F

SPSS Cross Tabulation Results for Attitudes Towards Supply Chain Security

Cross-tabulation results for entire sample for security driver ranking with two variables – annual revenue and Firm/SBU.

Annual_Revenue * Security_Driver * Firm_or_SBU Crosstabulation

Firm_or_SBU				Security_Driver			Total
				Not Important	Moderately Important	Very Important	
Entire Firm	Annual_Revenue	< 20 mil	Count	0	3	11	14
			% within Annual_Revenue	.0%	21.4%	78.6%	100.0%
		20 mil - 100 mil	Count	1	1	15	17
			% within Annual_Revenue	5.9%	5.9%	88.2%	100.0%
		100 mil - 500 mil	Count	0	3	11	14
			% within Annual_Revenue	.0%	21.4%	78.6%	100.0%
		500 mil - 1 bil	Count	1	1	5	7
			% within Annual_Revenue	14.3%	14.3%	71.4%	100.0%
		> 1 bil	Count	0	5	31	36
			% within Annual_Revenue	.0%	13.9%	86.1%	100.0%
	Total		Count	2	13	73	88
			% within Annual_Revenue	2.3%	14.8%	83.0%	100.0%
SBU	Annual_Revenue	< 20 mil	Count	1	0	3	4
			% within Annual_Revenue	25.0%	.0%	75.0%	100.0%
		20 mil - 100 mil	Count	0	0	8	8
			% within Annual_Revenue	.0%	.0%	100.0%	100.0%
		100 mil - 500 mil	Count	0	1	16	17
			% within Annual_Revenue	.0%	5.9%	94.1%	100.0%
		500 mil - 1 bil	Count	0	0	6	6
			% within Annual_Revenue	.0%	.0%	100.0%	100.0%
		> 1 bil	Count	2	5	33	40
			% within Annual_Revenue	5.0%	12.5%	82.5%	100.0%
	Total		Count	3	6	66	75
			% within Annual_Revenue	4.0%	8.0%	88.0%	100.0%

Chi-Square Tests

Firm_or_SBU		Value	df	Asymp. Sig. (2-sided)
Entire Firm	Pearson Chi-Square	8.921[a]	8	.349
	Likelihood Ratio	7.799	8	.453
	Linear-by-Linear Association	.154	1	.695
	N of Valid Cases	88		
SBU	Pearson Chi-Square	8.814[b]	8	.358
	Likelihood Ratio	8.917	8	.349
	Linear-by-Linear Association	.289	1	.591
	N of Valid Cases	75		

Cross-tabulation results for entire sample for security driver ranking with two variables – annual revenue and respondents' physical location.

Annual_Revenue * Security_Driver * Physical_Loc Crosstabulation

Physical_Location				Security_Driver			Total
				Not Important	Moderately Important	Very Important	
North America	Annual_Revenue	< 20 mil	Count	1	2	7	10
			% within Annual_Revenue	10.0%	20.0%	70.0%	100.0%
		20 mil - 100 mil	Count	1	0	16	17
			% within Annual_Revenue	5.9%	.0%	94.1%	100.0%
		100 mil - 500 mil	Count	0	1	19	20
			% within Annual_Revenue	.0%	5.0%	95.0%	100.0%
		500 mil - 1 bil	Count	1	0	5	6
			% within Annual_Revenue	16.7%	.0%	83.3%	100.0%
		> 1 bil	Count	1	6	40	47
			% within Annual_Revenue	2.1%	12.8%	85.1%	100.0%
	Total		Count	4	9	87	100
			% within Annual_Revenue	4.0%	9.0%	87.0%	100.0%
Asia	Annual_Revenue	< 20 mil	Count	0	0	3	3
			% within Annual_Revenue	.0%	.0%	100.0%	100.0%
		20 mil - 100 mil	Count	0	0	3	3
			% within Annual_Revenue	.0%	.0%	100.0%	100.0%
		100 mil - 500 mil	Count	0	1	3	4
			% within Annual_Revenue	.0%	25.0%	75.0%	100.0%
		500 mil - 1 bil	Count	0	0	3	3
			% within Annual_Revenue	.0%	.0%	100.0%	100.0%
		> 1 bil	Count	1	1	10	12
			% within Annual_Revenue	8.3%	8.3%	83.3%	100.0%
	Total		Count	1	2	22	25
			% within Annual_Revenue	4.0%	8.0%	88.0%	100.0%

Chi-Square Tests

Physical_Loc		Value	df	Asymp. Sig. (2-sided)
Canada	Pearson Chi-Square	9.787[a]	8	.280
	Likelihood Ratio	11.033	8	.200
	Linear-by-Linear Association	.156	1	.693
	N of Valid Cases	100		
China	Pearson Chi-Square	3.504[b]	8	.899
	Likelihood Ratio	4.081	8	.850
	Linear-by-Linear Association	.822	1	.365
	N of Valid Cases	25		

Cross-tabulation results for entire sample for security driver ranking with two variables – hazardous cargo nature and respondent type.

Hazardous * Security_Driver * Respondent_Type Crosstabulation

Respondent_Type				Security_Driver			Total
				Not Important	Moderately Important	Very Important	
Shipper	Hazardous	No	Count	3	8	57	68
			% within Hazardous	4.4%	11.8%	83.8%	100.0%
		Yes	Count	0	8	37	45
			% within Hazardous	.0%	17.8%	82.2%	100.0%
	Total		Count	3	16	94	113
			% within Hazardous	2.7%	14.2%	83.2%	100.0%
Service Provider	Hazardous	No	Count	1	2	19	22
			% within Hazardous	4.5%	9.1%	86.4%	100.0%
		Yes	Count	1	1	26	28
			% within Hazardous	3.6%	3.6%	92.9%	100.0%
	Total		Count	2	3	45	50
			% within Hazardous	4.0%	6.0%	90.0%	100.0%

Chi-Square Tests

Respondent_Type		Value	df	Asymp. Sig. (2-sided)
Shipper	Pearson Chi-Square	2.685[a]	2	.261
	Likelihood Ratio	3.733	2	.155
	Linear-by-Linear Association	.101	1	.751
	N of Valid Cases	113		
Service Provider	Pearson Chi-Square	.712[b]	2	.700
	Likelihood Ratio	.711	2	.701
	Linear-by-Linear Association	.336	1	.562
	N of Valid Cases	50		

Cross-tabulation results for entire sample for security driver ranking with two variables – hazardous cargo nature and Firm/SBU.

Hazardous * Security_Driver * Firm_or_SBU Crosstabulation

Firm_or_SBU				Security_Driver			Total
				Not Important	Moderately Important	Very Important	
Entire Firm	Hazardous	No	Count	2	7	44	53
			% within Hazardous	3.8%	13.2%	83.0%	100.0%
		Yes	Count	0	6	29	35
			% within Hazardous	.0%	17.1%	82.9%	100.0%
	Total		Count	2	13	73	88
			% within Hazardous	2.3%	14.8%	83.0%	100.0%
SBU	Hazardous	No	Count	2	3	32	37
			% within Hazardous	5.4%	8.1%	86.5%	100.0%
		Yes	Count	1	3	34	38
			% within Hazardous	2.6%	7.9%	89.5%	100.0%
	Total		Count	3	6	66	75
			% within Hazardous	4.0%	8.0%	88.0%	100.0%

Chi-Square Tests

Firm_or_SBU		Value	df	Asymp. Sig. (2-sided)
Entire Firm	Pearson Chi-Square	1.542[a]	2	.463
	Likelihood Ratio	2.246	2	.325
	Linear-by-Linear Association	.135	1	.713
	N of Valid Cases	88		
SBU	Pearson Chi-Square	.381[b]	2	.827
	Likelihood Ratio	.387	2	.824
	Linear-by-Linear Association	.286	1	.593
	N of Valid Cases	75		

Cross-tabulation results for entire sample for security driver ranking with two variables – hazardous cargo nature and respondents' physical location.

Hazardous * Security_Driver * Physical_Loc Crosstabulation

Physical_ Location				Security_Driver			Total
				Not Important	Moderately Important	Very Important	
North America	Hazardous	No	Count	3	5	47	55
			% within Hazardous	5.5%	9.1%	85.5%	100.0%
		Yes	Count	1	4	40	45
			% within Hazardous	2.2%	8.9%	88.9%	100.0%
	Total		Count	4	9	87	100
			% within Hazardous	4.0%	9.0%	87.0%	100.0%
Asia	Hazardous	No	Count	1	0	9	10
			% within Hazardous	10.0%	.0%	90.0%	100.0%
		Yes	Count	0	2	13	15
			% within Hazardous	.0%	13.3%	86.7%	100.0%
	Total		Count	1	2	22	25
			% within Hazardous	4.0%	8.0%	88.0%	100.0%

Chi-Square Tests

Physical_Loc		Value	df	Asymp. Sig. (2-sided)
Canada	Pearson Chi-Square	.681[a]	2	.711
	Likelihood Ratio	.720	2	.698
	Linear-by-Linear Association	.493	1	.483
	N of Valid Cases	100		
China	Pearson Chi-Square	2.841[b]	2	.242
	Likelihood Ratio	3.883	2	.143
	Linear-by-Linear Association	.119	1	.730
	N of Valid Cases	25		

Cross-tabulation results for entire sample for security driver ranking with two variables – shipment size and respondent type.

FCL * Security_Driver * Respondent_Type Crosstabulation

Respondent_Type				Security_Driver			Total
				Not Important	Moderately Important	Very Important	
Shipper	FCL	No	Count	1	1	16	18
			% within FCL	5.6%	5.6%	88.9%	100.0%
		Yes	Count	2	15	78	95
			% within FCL	2.1%	15.8%	82.1%	100.0%
	Total		Count	3	16	94	113
			% within FCL	2.7%	14.2%	83.2%	100.0%
Service Provider	FCL	No	Count	0	1	12	13
			% within FCL	.0%	7.7%	92.3%	100.0%
		Yes	Count	2	2	33	37
			% within FCL	5.4%	5.4%	89.2%	100.0%
	Total		Count	2	3	45	50
			% within FCL	4.0%	6.0%	90.0%	100.0%

Chi-Square Tests

Respondent_Type		Value	df	Asymp. Sig. (2-sided)
Shipper	Pearson Chi-Square	1.882[a]	2	.390
	Likelihood Ratio	2.029	2	.363
	Linear-by-Linear Association	.079	1	.778
	N of Valid Cases	113		
Service Provider	Pearson Chi-Square	.797[b]	2	.671
	Likelihood Ratio	1.294	2	.524
	Linear-by-Linear Association	.342	1	.559
	N of Valid Cases	50		

Cross-tabulation results for entire sample for security driver ranking with two variables – shipment size and Firm/SBU.

FCL * Security_Driver * Firm_or_SBU Crosstabulation

Firm_or_SBU				Security_Driver			
				Not Important	Moderately Important	Very Important	Total
Entire Firm	FCL	No	Count	1	2	14	17
			% within FCL	5.9%	11.8%	82.4%	100.0%
		Yes	Count	1	11	59	71
			% within FCL	1.4%	15.5%	83.1%	100.0%
	Total		Count	2	13	73	88
			% within FCL	2.3%	14.8%	83.0%	100.0%
SBU	FCL	No	Count	0	0	14	14
			% within FCL	.0%	.0%	100.0%	100.0%
		Yes	Count	3	6	52	61
			% within FCL	4.9%	9.8%	85.2%	100.0%
	Total		Count	3	6	66	75
			% within FCL	4.0%	8.0%	88.0%	100.0%

Chi-Square Tests

Firm_or_SBU		Value	df	Asymp. Sig. (2-sided)
Entire Firm	Pearson Chi-Square	1.338[a]	2	.512
	Likelihood Ratio	1.082	2	.582
	Linear-by-Linear Association	.184	1	.668
	N of Valid Cases	88		
SBU	Pearson Chi-Square	2.347[b]	2	.309
	Likelihood Ratio	3.992	2	.136
	Linear-by-Linear Association	2.028	1	.154
	N of Valid Cases	75		

Cross-tabulation results for entire sample for security driver ranking with two variables – shipment size and respondents' physical location.

FCL * Security_Driver * Physical_Loc Crosstabulation

Physical_ Location				Security_Driver			Total
				Not Important	Moderately Important	Very Important	
North America	FCL	No	Count	1	2	19	22
			% within FCL	4.5%	9.1%	86.4%	100.0%
		Yes	Count	3	7	68	78
			% within FCL	3.8%	9.0%	87.2%	100.0%
	Total		Count	4	9	87	100
			% within FCL	4.0%	9.0%	87.0%	100.0%
Asia	FCL	No	Count	0	0	2	2
			% within FCL	.0%	.0%	100.0%	100.0%
		Yes	Count	1	2	20	23
			% within FCL	4.3%	8.7%	87.0%	100.0%
	Total		Count	1	2	22	25
			% within FCL	4.0%	8.0%	88.0%	100.0%

Chi-Square Tests

Physical_Loc		Value	df	Asymp. Sig. (2-sided)
Canada	Pearson Chi-Square	.023[a]	2	.989
	Likelihood Ratio	.022	2	.989
	Linear-by-Linear Association	.018	1	.894
	N of Valid Cases	100		
China	Pearson Chi-Square	.296[b]	2	.862
	Likelihood Ratio	.534	2	.765
	Linear-by-Linear Association	.249	1	.618
	N of Valid Cases	25		

APPENDIX G

SPSS Cross Tabulation Results for Security Initiatives

Cross-tabulation results for entire sample with two variables.

Security/Operations Related Certifications

Crosstab

			Security_Performance (Binned)			
			Low	Average	High	Total
Certification	Not Implemented	Count	0	30	3	33
		% within Certification	.0%	90.9%	9.1%	100.0%
	Implemented	Count	2	48	30	80
		% within Certification	2.5%	60.0%	37.5%	100.0%
Total		Count	2	78	33	113
		% within Certification	1.8%	69.0%	29.2%	100.0%

Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	10.515[a]	2	.005
Likelihood Ratio	12.450	2	.002
Linear-by-Linear Association	6.629	1	.010
N of Valid Cases	113		

Business Partner Requirements

Crosstab

			Security_Performance (Binned)			
			Low	Average	High	Total
Partner_Requirements	Not Implemented	Count	1	30	4	35
		% within Partner_ Requirements	2.9%	85.7%	11.4%	100.0%
	Implemented	Count	1	48	29	78
		% within Partner_ Requirements	1.3%	61.5%	37.2%	100.0%
Total		Count	2	78	33	113
		% within Partner_ Requirements	1.8%	69.0%	29.2%	100.0%

Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	7.870[a]	2	.020
Likelihood Ratio	8.781	2	.012
Linear-by-Linear Association	7.626	1	.006
N of Valid Cases	113		

Container/Trailer/Unit Load Device Security

Crosstab

			Security_Performance (Binned)			
			Low	Average	High	Total
Container_Security	Not Implemented	Count	1	29	5	35
		% within Container_Security	2.9%	82.9%	14.3%	100.0%
	Implemented	Count	1	49	28	78
		% within Container_Security	1.3%	62.8%	35.9%	100.0%
Total		Count	2	78	33	113
		% within Container_Security	1.8%	69.0%	29.2%	100.0%

Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	5.608[a]	2	.061
Likelihood Ratio	6.079	2	.048
Linear-by-Linear Association	5.490	1	.019
N of Valid Cases	113		

Advanced Data

Crosstab

			Security_Performance (Binned)			
			Low	Average	High	Total
Advanced_Data	Not Implemented	Count	0	41	3	44
		% within Advanced_Data	.0%	93.2%	6.8%	100.0%
	Implemented	Count	2	37	30	69
		% within Advanced_Data	2.9%	53.6%	43.5%	100.0%
Total		Count	2	78	33	113
		% within Advanced_Data	1.8%	69.0%	29.2%	100.0%

Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	19.731[a]	2	.000
Likelihood Ratio	23.043	2	.000
Linear-by-Linear Association	12.945	1	.000
N of Valid Cases	113		

Physical Access and Control

Crosstab

			Security_Performance (Binned)			
			Low	Average	High	Total
Physical_Security	Not Implemented	Count	1	34	3	38
		% within Physical_Security	2.6%	89.5%	7.9%	100.0%
	Implemented	Count	1	44	30	75
		% within Physical_Security	1.3%	58.7%	40.0%	100.0%
Total		Count	2	78	33	113
		% within Physical_Security	1.8%	69.0%	29.2%	100.0%

Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	12.610[a]	2	.002
Likelihood Ratio	14.586	2	.001
Linear-by-Linear Association	11.896	1	.001
N of Valid Cases	113		

Procedural Security

Crosstab

			Security_Performance (Binned)			
			Low	Average	High	Total
Procedure	Not Implemented	Count	1	18	3	22
		% within Procedure	4.5%	81.8%	13.6%	100.0%
	Implemented	Count	1	60	30	91
		% within Procedure	1.1%	65.9%	33.0%	100.0%
Total		Count	2	78	33	113
		% within Procedure	1.8%	69.0%	29.2%	100.0%

Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	4.104[a]	2	.129
Likelihood Ratio	4.257	2	.119
Linear-by-Linear Association	3.885	1	.049
N of Valid Cases	113		

Tracking and Monitoring

Crosstab

			Security_Performance (Binned)			
			Low	Average	High	Total
Tracking	Not Implemented	Count	1	52	15	68
		% within Tracking	1.5%	76.5%	22.1%	100.0%
	Implemented	Count	1	26	18	45
		% within Tracking	2.2%	57.8%	40.0%	100.0%
Total		Count	2	78	33	113
		% within Tracking	1.8%	69.0%	29.2%	100.0%

Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	4.442[a]	2	.109
Likelihood Ratio	4.394	2	.111
Linear-by-Linear Association	3.382	1	.066
N of Valid Cases	113		

Security Training

Crosstab

			Security_Performance (Binned)			
			Low	Average	High	Total
Training	Not Implemented	Count	1	7	1	9
		% within Training	11.1%	77.8%	11.1%	100.0%
	Implemented	Count	1	71	32	104
		% within Training	1.0%	68.3%	30.8%	100.0%
Total		Count	2	78	33	113
		% within Training	1.8%	69.0%	29.2%	100.0%

Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	6.026[a]	2	.049
Likelihood Ratio	3.968	2	.138
Linear-by-Linear Association	3.111	1	.078
N of Valid Cases	113		

Personnel Security

Crosstab

			Security_Performance (Binned)			
			Low	Average	High	Total
Personnel_Security	Not Implemented	Count	1	33	2	36
		% within Personnel_ Security	2.8%	91.7%	5.6%	100.0%
	Implemented	Count	1	45	31	77
		% within Personnel_ Security	1.3%	58.4%	40.3%	100.0%
Total		Count	2	78	33	113
		% within Personnel_ Security	1.8%	69.0%	29.2%	100.0%

Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	14.343[a]	2	.001
Likelihood Ratio	17.291	2	.000
Linear-by-Linear Association	13.576	1	.000
N of Valid Cases	113		

Management Support

Crosstab

			Security_Performance (Binned)			
			Low	Average	High	Total
Mgt_Support	Not Implemented	Count	1	44	8	53
		% within Mgt_Support	1.9%	83.0%	15.1%	100.0%
	Implemented	Count	1	34	25	60
		% within Mgt_Support	1.7%	56.7%	41.7%	100.0%
Total		Count	2	78	33	113
		% within Mgt_Support	1.8%	69.0%	29.2%	100.0%

Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	9.643[a]	2	.008
Likelihood Ratio	10.045	2	.007
Linear-by-Linear Association	8.539	1	.003
N of Valid Cases	113		

Cross-tabulation results for Shipper and Service Provider with three variables.

Security/Operations Related Certifications

Crosstab

Respondent_Type				Security_Performance (Binned) Low	Average	High	Total
Shipper	Certification	Not Implemented	Count	0	19	1	20
			% within Certification	.0%	95.0%	5.0%	100.0%
		Implemented	Count	2	33	17	52
			% within Certification	3.8%	63.5%	32.7%	100.0%
	Total		Count	2	52	18	72
			% within Certification	2.8%	72.2%	25.0%	100.0%
Service Provider	Certification	Not Implemented	Count		11	2	13
			% within Certification		84.6%	15.4%	100.0%
		Implemented	Count		15	13	28
			% within Certification		53.6%	46.4%	100.0%
	Total		Count		26	15	41
			% within Certification		63.4%	36.6%	100.0%

Chi-Square Tests

Respondent_Type		Value	df	Asymp. Sig. (2-sided)	Exact Sig. (2-sided)	Exact Sig. (1-sided)
Shipper	Pearson Chi-Square	7.189[b]	2	.027		
	Likelihood Ratio	9.086	2	.011		
	Linear-by-Linear Association	3.546	1	.060		
	N of Valid Cases	72				
Service Provider	Pearson Chi-Square	3.688[c]	1	.055		
	Continuity Correction[a]	2.471	1	.116		
	Likelihood Ratio	4.015	1	.045		
	Fisher's Exact Test				.084	.055
	Linear-by-Linear Association	3.598	1	.058		
	N of Valid Cases	41				

Business Partner Requirements

Crosstab

Respondent_Type				Security_Performance (Binned) Low	Average	High	Total
Shipper	Partner_Requirements	Not Implemented	Count	1	24	2	27
			% within Partner_ Requirements	3.7%	88.9%	7.4%	100.0%
		Implemented	Count	1	28	16	45
			% within Partner_ Requirements	2.2%	62.2%	35.6%	100.0%
	Total		Count	2	52	18	72
			% within Partner_ Requirements	2.8%	72.2%	25.0%	100.0%
Service Provider	Partner_Requirements	Not Implemented	Count		6	2	8
			% within Partner_ Requirements		75.0%	25.0%	100.0%
		Implemented	Count		20	13	33
			% within Partner_ Requirements		60.6%	39.4%	100.0%
	Total		Count		26	15	41
			% within Partner_ Requirements		63.4%	36.6%	100.0%

Chi-Square Tests

Respondent_Type		Value	df	Asymp. Sig. (2-sided)	Exact Sig. (2-sided)	Exact Sig. (1-sided)
Shipper	Pearson Chi-Square	7.143[b]	2	.028		
	Likelihood Ratio	8.155	2	.017		
	Linear-by-Linear Association	6.396	1	.011		
	N of Valid Cases	72				
Service Provider	Pearson Chi-Square	.575[c]	1	.448		
	Continuity Correction[a]	.122	1	.727		
	Likelihood Ratio	.601	1	.438		
	Fisher's Exact Test				.687	.373
	Linear-by-Linear Association	.561	1	.454		
	N of Valid Cases	41				

Container/Trailer/Unit Load Device Security

Crosstab

Respondent_Type				Security_Performance (Binned)			Total
				Low	Average	High	
Shipper	Container_Security	Not Implemented	Count	1	20	2	23
			% within Container_Security	4.3%	87.0%	8.7%	100.0%
		Implemented	Count	1	32	16	49
			% within Container_Security	2.0%	65.3%	32.7%	100.0%
	Total		Count	2	52	18	72
			% within Container_Security	2.8%	72.2%	25.0%	100.0%
Service Provider	Container_Security	Not Implemented	Count		9	3	12
			% within Container_Security		75.0%	25.0%	100.0%
		Implemented	Count		17	12	29
			% within Container_Security		58.6%	41.4%	100.0%
	Total		Count		26	15	41
			% within Container_Security		63.4%	36.6%	100.0%

Chi-Square Tests

Respondent_Type		Value	df	Asymp. Sig. (2-sided)	Exact Sig. (2-sided)	Exact Sig. (1-sided)
Shipper	Pearson Chi-Square	4.909[b]	2	.086		
	Likelihood Ratio	5.585	2	.061		
	Linear-by-Linear Association	4.662	1	.031		
	N of Valid Cases	72				
Service Provider	Pearson Chi-Square	.981[c]	1	.322		
	Continuity Correction[a]	.402	1	.526		
	Likelihood Ratio	1.018	1	.313		
	Fisher's Exact Test				.480	.266
	Linear-by-Linear Association	.958	1	.328		
	N of Valid Cases	41				

Advanced Data

Crosstab

Respondent_Type				Security_Performance (Binned)			Total
				Low	Average	High	
Shipper	Advanced_Data	Not Implemented	Count	0	29	3	32
			% within Advanced_Data	.0%	90.6%	9.4%	100.0%
		Implemented	Count	2	23	15	40
			% within Advanced_Data	5.0%	57.5%	37.5%	100.0%
	Total		Count	2	52	18	72
			% within Advanced_Data	2.8%	72.2%	25.0%	100.0%
Service Provider	Advanced_Data	Not Implemented	Count		12	0	12
			% within Advanced_Data		100.0%	.0%	100.0%
		Implemented	Count		14	15	29
			% within Advanced_Data		48.3%	51.7%	100.0%
	Total		Count		26	15	41
			% within Advanced_Data		63.4%	36.6%	100.0%

Chi-Square Tests

Respondent_Type		Value	df	Asymp. Sig. (2-sided)	Exact Sig. (2-sided)	Exact Sig. (1-sided)
Shipper	Pearson Chi-Square	9.926[b]	2	.007		
	Likelihood Ratio	11.309	2	.004		
	Linear-by-Linear Association	4.105	1	.043		
	N of Valid Cases	72				
Service Provider	Pearson Chi-Square	9.788[c]	1	.002		
	Continuity Correction[a]	7.685	1	.006		
	Likelihood Ratio	13.682	1	.000		
	Fisher's Exact Test				.001	.001
	Linear-by-Linear Association	9.549	1	.002		
	N of Valid Cases	41				

Physical Access and Control

Crosstab

Respondent_Type				Security_Performance (Binned)			Total
				Low	Average	High	
Shipper	Physical_Security	Not Implemented	Count	1	24	2	27
			% within Physical_Security	3.7%	88.9%	7.4%	100.0%
		Implemented	Count	1	28	16	45
			% within Physical_Security	2.2%	62.2%	35.6%	100.0%
	Total		Count	2	52	18	72
			% within Physical_Security	2.8%	72.2%	25.0%	100.0%
Service Provider	Physical_Security	Not Implemented	Count		10	1	11
			% within Physical_Security		90.9%	9.1%	100.0%
		Implemented	Count		16	14	30
			% within Physical_Security		53.3%	46.7%	100.0%
	Total		Count		26	15	41
			% within Physical_Security		63.4%	36.6%	100.0%

Chi-Square Tests

Respondent_Type		Value	df	Asymp. Sig. (2-sided)	Exact Sig. (2-sided)	Exact Sig. (1-sided)
Shipper	Pearson Chi-Square	7.143[b]	2	.028		
	Likelihood Ratio	8.155	2	.017		
	Linear-by-Linear Association	6.396	1	.011		
	N of Valid Cases	72				
Service Provider	Pearson Chi-Square	4.898[c]	1	.027		
	Continuity Correction[a]	3.413	1	.065		
	Likelihood Ratio	5.693	1	.017		
	Fisher's Exact Test				.033	.028
	Linear-by-Linear Association	4.779	1	.029		
	N of Valid Cases	41				

Procedural Security

Crosstab

Respondent_Type				Security_Performance (Binned)			Total
				Low	Average	High	
Shipper	Procedure	Not Implemented	Count	1	14	1	16
			% within Procedure	6.3%	87.5%	6.3%	100.0%
		Implemented	Count	1	38	17	56
			% within Procedure	1.8%	67.9%	30.4%	100.0%
	Total		Count	2	52	18	72
			% within Procedure	2.8%	72.2%	25.0%	100.0%
Service Provider	Procedure	Not Implemented	Count		4	2	6
			% within Procedure		66.7%	33.3%	100.0%
		Implemented	Count		22	13	35
			% within Procedure		62.9%	37.1%	100.0%
	Total		Count		26	15	41
			% within Procedure		63.4%	36.6%	100.0%

Chi-Square Tests

Respondent_Type		Value	df	Asymp. Sig. (2-sided)	Exact Sig. (2-sided)	Exact Sig. (1-sided)
Shipper	Pearson Chi-Square	4.451[b]	2	.108		
	Likelihood Ratio	5.202	2	.074		
	Linear-by-Linear Association	4.386	1	.036		
	N of Valid Cases	72				
Service Provider	Pearson Chi-Square	.032[c]	1	.858		
	Continuity Correction[a]	.000	1	1.000		
	Likelihood Ratio	.032	1	.857		
	Fisher's Exact Test				1.000	.620
	Linear-by-Linear Association	.031	1	.860		
	N of Valid Cases	41				

Tracking and Monitoring

Crosstab

Respondent_Type				Security_Performance (Binned)			Total
				Low	Average	High	
Shipper	Tracking	Not Implemented	Count	1	39	9	49
			% within Tracking	2.0%	79.6%	18.4%	100.0%
		Implemented	Count	1	13	9	23
			% within Tracking	4.3%	56.5%	39.1%	100.0%
	Total		Count	2	52	18	72
			% within Tracking	2.8%	72.2%	25.0%	100.0%
Service Provider	Tracking	Not Implemented	Count		13	6	19
			% within Tracking		68.4%	31.6%	100.0%
		Implemented	Count		13	9	22
			% within Tracking		59.1%	40.9%	100.0%
	Total		Count		26	15	41
			% within Tracking		63.4%	36.6%	100.0%

Chi-Square Tests

Respondent_Type		Value	df	Asymp. Sig. (2-sided)	Exact Sig. (2-sided)	Exact Sig. (1-sided)
Shipper	Pearson Chi-Square	4.153[b]	2	.125		
	Likelihood Ratio	4.000	2	.135		
	Linear-by-Linear Association	2.302	1	.129		
	N of Valid Cases	72				
Service Provider	Pearson Chi-Square	.383[c]	1	.536		
	Continuity Correction[a]	.086	1	.769		
	Likelihood Ratio	.384	1	.535		
	Fisher's Exact Test				.746	.386
	Linear-by-Linear Association	.373	1	.541		
	N of Valid Cases	41				

Security Training

Crosstab

Respondent_Type				Security_Performance (Binned)			Total
				Low	Average	High	
Shipper	Training	Not Implemented	Count	1	4	1	6
			% within Training	16.7%	66.7%	16.7%	100.0%
		Implemented	Count	1	48	17	66
			% within Training	1.5%	72.7%	25.8%	100.0%
	Total		Count	2	52	18	72
			% within Training	2.8%	72.2%	25.0%	100.0%
Service Provider	Training	Not Implemented	Count		3	0	3
			% within Training		100.0%	.0%	100.0%
		Implemented	Count		23	15	38
			% within Training		60.5%	39.5%	100.0%
	Total		Count		26	15	41
			% within Training		63.4%	36.6%	100.0%

Chi-Square Tests

Respondent_Type		Value	df	Asymp. Sig. (2-sided)	Exact Sig. (2-sided)	Exact Sig. (1-sided)
Shipper	Pearson Chi-Square	4.755[b]	2	.093		
	Likelihood Ratio	2.604	2	.272		
	Linear-by-Linear Association	1.396	1	.237		
	N of Valid Cases	72				
Service Provider	Pearson Chi-Square	1.867[c]	1	.172		
	Continuity Correction[a]	.554	1	.457		
	Likelihood Ratio	2.868	1	.090		
	Fisher's Exact Test				.287	.244
	Linear-by-Linear Association	1.822	1	.177		
	N of Valid Cases	41				

Personnel Security

Crosstab

Respondent_Type				Security_Performance (Binned)			
				Low	Average	High	Total
Shipper	Personnel_Security	Not Implemented	Count	1	25	0	26
			% within Personnel_Security	3.8%	96.2%	.0%	100.0%
		Implemented	Count	1	27	18	46
			% within Personnel_Security	2.2%	58.7%	39.1%	100.0%
	Total		Count	2	52	18	72
			% within Personnel_Security	2.8%	72.2%	25.0%	100.0%
Service Provider	Personnel_Security	Not Implemented	Count		8	2	10
			% within Personnel_Security		80.0%	20.0%	100.0%
		Implemented	Count		18	13	31
			% within Personnel_Security		58.1%	41.9%	100.0%
	Total		Count		26	15	41
			% within Personnel_Security		63.4%	36.6%	100.0%

Chi-Square Tests

Respondent_Type		Value	df	Asymp. Sig. (2-sided)	Exact Sig. (2-sided)	Exact Sig. (1-sided)
Shipper	Pearson Chi-Square	13.568[b]	2	.001		
	Likelihood Ratio	19.401	2	.000		
	Linear-by-Linear Association	11.940	1	.001		
	N of Valid Cases	72				
Service Provider	Pearson Chi-Square	1.568[c]	1	.210		
	Continuity Correction[a]	.765	1	.382		
	Likelihood Ratio	1.677	1	.195		
	Fisher's Exact Test				.277	.193
	Linear-by-Linear Association	1.530	1	.216		
	N of Valid Cases	41				

Management Support and Sponsorship

Crosstab

Respondent_Type				Security_Performance (Binned)			Total
				Low	Average	High	
Shipper	Mgt_Support	Not Implemented	Count	1	31	5	37
			% within Mgt_Support	2.7%	83.8%	13.5%	100.0%
		Implemented	Count	1	21	13	35
			% within Mgt_Support	2.9%	60.0%	37.1%	100.0%
	Total		Count	2	52	18	72
			% within Mgt_Support	2.8%	72.2%	25.0%	100.0%
Service Provider	Mgt_Support	Not Implemented	Count		13	3	16
			% within Mgt_Support		81.3%	18.8%	100.0%
		Implemented	Count		13	12	25
			% within Mgt_Support		52.0%	48.0%	100.0%
	Total		Count		26	15	41
			% within Mgt_Support		63.4%	36.6%	100.0%

Chi-Square Tests

Respondent_Type		Value	df	Asymp. Sig. (2-sided)	Exact Sig. (2-sided)	Exact Sig. (1-sided)
Shipper	Pearson Chi-Square	5.427[b]	2	.066		
	Likelihood Ratio	5.563	2	.062		
	Linear-by-Linear Association	4.279	1	.039		
	N of Valid Cases	72				
Service Provider	Pearson Chi-Square	3.598[c]	1	.058		
	Continuity Correction[a]	2.447	1	.118		
	Likelihood Ratio	3.791	1	.052		
	Fisher's Exact Test				.097	.057
	Linear-by-Linear Association	3.510	1	.061		
	N of Valid Cases	41				

APPENDIX H

Behavioral Research Ethics Board Approval Certificate

The University of British Columbia
Office of Research Services
Behavioural Research Ethics Board
Suite 102, 6190 Agronomy Road, Vancouver, B.C. V6T 1Z3

CERTIFICATE OF APPROVAL - MINIMAL RISK

PRINCIPAL INVESTIGATOR:	INSTITUTION / DEPARTMENT:	UBC BREB NUMBER:
Garland Chow	UBC/Sauder School of Business	H07-01313

INSTITUTION(S) WHERE RESEARCH WILL BE CARRIED OUT:

Institution	Site
UBC	Vancouver (excludes UBC Hospital)

Other locations where the research will be conducted:
field surveys at respondents premises or web surveys

CO-INVESTIGATOR(S):
Wai Leng Loke

SPONSORING AGENCIES:
Transport Canada

PROJECT TITLE:
Simulation Model of Container Transport Security for the Vancouver Gateway (Approval of the pilot project for Kelly Loke's MSc thesis)

CERTIFICATE EXPIRY DATE: April 17, 2009

DOCUMENTS INCLUDED IN THIS APPROVAL:		DATE APPROVED: April 17, 2008
Document Name	**Version**	**Date**
<u>Questionnaire, Questionnaire Cover Letter, Tests:</u>		
Field survey shippers	N/A	April 15, 2008
Field interview service providers	N/A	April 15, 2008
web survey service providers	N/A	April 15, 2008
web survey shippers	N/A	April 15, 2008
<u>Letter of Initial Contact:</u>		
Letter to potential respondents	N/A	April 15, 2008

The application for ethical review and the document(s) listed above have been reviewed and the procedures were found to be acceptable on ethical grounds for research involving human subjects.

Approval is issued on behalf of the Behavioural Research Ethics Board and signed electronically by one of the following:

Dr. M. Judith Lynam, Chair
Dr. Ken Craig, Chair
Dr. Jim Rupert, Associate Chair
Dr. Laurie Ford, Associate Chair
Dr. Daniel Salhani, Associate Chair
Dr. Anita Ho, Associate Chair