BEING PROACTIVE TO INCREASING SUPPLY CHAIN SECURITY CHALLENGES: A QUANTITATIVE AND QUALITATIVE APPROACH

A Dissertation

by

GUANYI LU

Submitted to the Office of Graduate Studies of
Texas A&M University
in partial fulfillment of the requirements for the degree of

DOCTOR OF PHILOSOPHY

Chair of Committee,	Xenophon A. Koufteros
Committee Members,	Gregory R. Heim
	R. Duane Ireland
	David X. Peng
Head of Department,	Richard Metters

August 2013

Major Subject: Information and Operations Management

ABSTRACT

Supply chain security has become relevant to both practitioners and academics for years, yet the understanding of this topic is still incomplete. The literature produces relatively few explanatory and confirmatory studies, offers ambiguous definitions and terminology and the theoretical development is inconsistent.

In this dissertation, I review relevant research streams and employ four in-depth case studies to conceptualize supply chain security (SCS). I also utilize the principles of human immunology to propose a taxonomy of supply chain security management (SCSM) mechanisms. Building on institutional theory and the taxonomy, I further examine the antecedents as well as the consequences of SCSM mechanisms via a large empirical data set collected during 2011-2013. The sample includes responses from 462 firms.

Specifically, in my first model I draw on the institutional theory and posit that five institutional isomorphism pressures (i.e., government, customer, peer, normative, and performance pressure) impact four classes of SCSM mechanisms (i.e., prevention, detection, reaction, and restoration). In addition, shared SCS perception (SSP) and top management commitment (TMC) are hypothesized to moderate (strengthen) the relationships between institutional pressures and SCSM mechanisms. In my second model, I propose that the four classes of mechanisms explain five different supply chain performance dimensions (i.e., security performance, cost performance, supply chain

responsiveness, supply chain resilience, and supply chain visibility). I also specify differential effects for both models; some effects are more salient than others.

The results suggest that not all institutional pressures motivate the implementation of SCSM mechanisms. While normative pressure and performance pressure act as predominantly powerful predictors of SCSM mechanisms, other pressures appear to have negligible or even adverse effects. Surprisingly, data analysis suggests that coercive institutional pressures (i.e., government pressure and customer pressure) do not exhibit the strongest effects on SCSM mechanisms as the literature would suggest. As far as the moderation effect is concerned, the results illustrate that neither SSP nor TMC interact with all institutional pressures to affect the employment of SCSM mechanisms. In addition, TMC can even impede the implementation of reaction- and restoration-oriented SCSM mechanisms when interacting with government pressure. Regarding supply chain performance, the results demonstrate that SCSM mechanisms have strong effects on multiple supply chain performance measures. Further assessments reveal that the effect of SCSM mechanisms on supply chain security performance is stronger than its effects on other performance dimensions.

DEDICATION

To my loving wife, Lin, and son, Eric. Your support and encouragement throughout this process has enabled any contribution which will be realized as a result of this study. Thank you.

ACKNOWLEDGEMENTS

I would like to thank my committee chair, Dr. Koufteros, and my committee members, Dr. Heim, Dr. Ireland, and Dr. Peng, for their guidance and support throughout the course of this research.

Thanks also go to my friends and colleagues and the department faculty and staff for making my time at Texas A&M University a great experience.

Finally, thanks to my wife, Lin, for her encouragement, patience, and love.

TABLE OF CONTENTS

Page

LIST OF FIGURES

Page

LIST OF TABLES

Page

CHAPTER I

INTRODUCTION

The increasing occurrences of supply chain disruptions have continuously called for better supply chain risk management. With longer supply chain routes and shorter clock speeds, organizations are facing more disruptions in their global supply chains. The 9/11 terrorist attacks have disrupted the operations of many firms and cost the U.S. stock market $1.4 trillion in value during that week (Bob, 2001); the severe flooding of Thailand in 2011 temporally suspended 40 percent of the world's hard-disk drive production (Ladendorf, 2011); the August 14, 2003 blackout in the Northeastern U.S. resulted in loss of power for hundreds of factories in eight states in the U.S. and the Canadian province of Ontario (Moon, 2008). These are but a few recent reminders of the inherent vulnerability of the global supply networks. The economic impact of these disruptions is significant and potentially devastating for firms (Hendrick and Singhal, 2003, 2005). As a result, many scholars have been seeking ways to help managers minimize risk and solve problems (Chopra and Sodhi, 2004; Helferich and Cook, 2002; Kleindorfer and Saad, 2005; Sheffi, 2007).

Researchers have typically taken two interrelated routes to understanding supply chain risk. In one direction, researchers have built upon the classic stochastic modeling and simulation approaches (Haimes, 1998) to explore two critical risk-related factors: the probability of a risk and the magnitude of losses related to that risk (Shavell, 1984). Theoretical advances (e.g., Kleindorfer and Saad, 2005; Ritchie and Brindley, 2007;

Tang, 2006a) and ample numerical analyses (Djavanshir and Khorramshahgol, 2006; Faisal, Banwet, and Shankar, 2006; Gneezy, List, and Wu, 2006; Goh, Lim, and Meng, 2007) have helped scholars gain an in-depth understanding of how firms can reduce the probability and/or the economic loss as related to supply chain disruptions and thereby improve firm performance. For example, several recent analytical studies have demonstrated that supply chain risk management strategies positively influence firm performance (e.g., Tang and Tomlin, 2008; Tomlin, 2006).

Taking another approach, researchers have also sought to understand the root causes of supply chain risk so that firms can intentionally design strategies and implement practices to address potential supply chain disasters (Craighead, Blackhurst, Rungtusanatham, Handfield, 2007; Braunscheidel and Suresh, 2009). Scholars have shown how to utilize the total quality management (TQM) philosophy to control risks (Lee and Whang, 2005), explored why some disruptions may be more severe than others (Craighead et al., 2007), categorized the sources of risk (Christopher and Peck, 2004; Wagner and Bode, 2006), and proposed a number of models to tackle salient supply chain risks (e.g., Elkins, Handfield, Blackhurst, and Craighead, 2005; Kleindorfer and Saad, 2005; Knemeyer, Zinn, and Eroglu, 2009; Tang, 2006b; Weiss and Maher, 2009).

However, despite the fact that a number of empirical and analytical studies have demonstrated significant relationships between risk management and firm performance, supply chain security (SCS) breaches are largely ignored (Martens et al., 2011; Williams et al., 2008). The neglect of SCS breaches makes the understanding of supply chain risk incomplete at best: theft alone costs retailers and consumers $104 billion a year and is

the most common cause of inventory shrinkage (Retail Info Systems News, 2008). In addition, the nature of SCS has fundamentally changed since the terrorist attacks on September 11, 2001 (Sheffi, 2001; Quinn, 2003). The scope of SCS has gone beyond simply preventing theft or other illegal access to supply chain assets to protecting the supply chain from any illicit use (e.g., smuggling weapons of mass destruction, counterfeit products, adulterated drugs) that could cause severe damage beyond the cost to human life (DHS report, 2007; Narasimhan and Talluri, 2009). Globalization, the threat of terrorism, and the increasingly complex nature of criminal activities have made the security of end-to-end supply chains much more salient.

SCS breaches appear to be increasing in recent years and thus the threat to supply chains has gained momentum. Three out of the ten most devastating terrorist attacks registered in the last 100 years took place during the last few years (i.e., the September 11 terrorist attacks, the 2005 Madrid Subway Explosion, the 2008 Mumbai attacks) They are events that arise havoc for supply chains. A report from the Department of Commerce's Bureau of Industry and Security (BIS) documented a significant growth in incidents of counterfeit parts across the electronics industry from 3,300 incidents in 2005 to more than 8,000 incidents in 2008 (BIS report, 2010). Business data breaches increased from 116 cases in 2005 to 405 cases in 2011 (Chronology of Data Breaches, 2011), including the SONY 2011 data breach which cost the company approximately $171.4 million due to the theft of 77 million customer records. These security breaches have generated tremendous direct and indirect expenditures for businesses and the economy. For example, the Federal Bureau of Investigation (FBI) estimates counterfeit

merchandise alone costs U.S. businesses $200-$250 billion in revenue and results in losses of 750,000 jobs on an annual basis (http://www.gao.gov/new.items/d10423.pdf).

Not only is the economy affected, but some studies illustrate that SCS breaches could also affect everyday life. Drugs have been smuggled in mediums such as toys, furniture, holiday candles, tennis shoes, and even statues of Jesus Christ via the global supply system (CNN, 2009). Drugs claim thousands of lives and millions of dollars each year and induce drug-fueled criminal behaviors. Based on the most recent survey, 38,371 U.S. people died of drug-induced causes in 2007, and the country spent more than $20 billion each year to control drug abuse in the last three years (i.e., 2009-2011, Office of National Drug Control Policy, see: http://www.whitehouse.gov/sites/default/files/ondcp/Fact_Sheets/consequences_of_illicit_drug_use.pdf). There is also evidence that "the illicit tobacco trade is carried out by transnational criminal groups and has been used to raise funds for terrorist organizations...If the global illicit trade were eliminated, governments would gain at least $31 billion [e.g., lost tax due to tobacco smuggling], and from 2030 onwards would save over 160,000 lives a year" (Joossens et al, 2011). Weapon smuggling is another major concern related to public safety. According to Stephen Flynn (2008), president of the Center for National Policy, the most probable way that the American people will become targets of a nuclear weapon would be for al-Qaeda or a future adversary to smuggle it into the United States through global supply chains.

In summary, the hidden economic and political impacts of SCS breaches are tremendous and potentially devastating. Thus, it is of vital importance to understand the nature of SCS and how firms respond to SCS breaches.

1.1 Research Question Statements

The SCS literature has produced relatively few explanatory and confirmatory studies, offered ambiguous definitions and terminology; and theoretical development is lacking and can be characterized as inconsistent (Autry and Bobbitt, 2008). The topic of supply chain security is quite relevant, but there is no formal and widely accepted definition of SCS in the academic literature. A systematic classification of supply chain security management (SCSM) mechanisms is also absent. As a result, the scope of SCS appears to be rather broad and blurred. Empirical research on SCS is also scant (Martens et al., 2011). The antecedents of SCSM mechanisms have been generally ignored (one exception is Williams et al., 2009a). Due to the very nature of this topic being "security", researchers struggle to access relevant information from practitioners. Many of the existing studies are conceptual in nature or based on a qualitative approach. Large-scale empirical research which can test propositions is quite rare.

There are five unresolved issues: (1) the specification of the concept of SCS, which may potentially facilitate the development of this research stream, (2) the establishment of a systematic taxonomy of SCSM mechanisms that allow researchers to improve our understanding in this domain, (3) the identification of antecedents of SCSM mechanisms, which reflects a firm's overall strategy against SCS challenges, (4) the

boundary conditions and organizational traits that shape the effects of these antecedents on SCSM mechanism, and (5) the large scale empirical tests that examine the effects of SCSM mechanisms on supply chain performance. This study aims at resolving these issues. The specific research questions this dissertation attempts to address are:

(1) How do we define SCS (and correspondingly SCSM)?

(2) How can we classify SCSM mechanisms into a conceptually sound but yet succinct taxonomy?

(3) What are the underlying drivers for the implementation of SCSM mechanisms?

(4) Are there any organizational factors that shape the relationships between these drivers and the SCSM mechanisms?

(5) Do SCSM mechanisms substantively affect performance?

The first research question relates to the conceptualization of SCS. It is unfortunate that no formal definition of SCS can be found in the academic literature. The lack of a clear and formal definition of SCS inhibits progress in the development of SCS research (Autry and Bobbitt, 2008). For example, without such a definition, how can researchers effectively distinguish between security oriented practices from non-security oriented (e.g. safety oriented) ones? Furthermore, SCSM mechanisms seem to span across many supply chain management subfields—from inventory management to customer relationships, from shipment arrangements to organizational culture. A broad scope may be advantageous as it stimulates diverse schools of thought. But "boundaries" should be established such that the research stream can maintain its focus and

relevance—an important benefit of having a clear definition of supply chain security. With a clear definition, scholars may further develop more accurate terminologies and reduce the ambiguity regarding the SCS vocabulary (Autry and Bobbitt, 2008).

The second research question concerns the lack of a systematic taxonomy of SCSM mechanisms. The academic literature and industry reports alike have linked a number of SCSM mechanisms to firm performance. Yet these SCSM mechanisms are rather broad and bear various measures. Gutierrez and Hintsa (2006) studied nine voluntary SCSM programs initiated by governments or international organizations. Comparisons of these programs show that no two programs have exactly the same dimensions and measures, indicating that even governments and leading professional organizations have different perceptions of what constitutes best SCSM mechanisms. As a result, managers tend to be unsure about how to move forward with an appropriate security plan (Closs et al., 2008). There are many lists of what to do. But they are quite diverse. How do decision-makers decide which practices to adopt if they don't know the effects of these practices on performance? How can top managers promote effective supply chain security strategies if they cannot distinguish them from the less effective ones? Some managers may have the desire to secure their supply chain but may lack the understanding and guidelines needed to develop an effective program (Unisys, 2005).

Although this study may not be able to explore all SCSM mechanisms and their respective effects, the more modest goal is to provide a means to systematically categorize SCSM mechanisms based on their purpose—developing a taxonomy. A taxonomy apportions SCSM mechanisms into different classes from which firms can

select when they need to enhance SCS performance. While a taxonomy is basic in its form, it is useful because, regardless of size, companies inevitably have limited resources and need to determine which class of SCSM mechanism will provide the most desirable outcomes for their specific needs. In other words, a taxonomy enables a firm to intentionally focus on one class of SCSM mechanism at a time according to its particular needs and resource constraints. A taxonomy can also be rather useful for academic research because it can help organize the literature and potentially identify areas which are understudied.

The third research question pertains to the antecedents of SCSM mechanisms. Investing in supply chain security is to some extent analogous to buying insurance; as long as the SCS system is working, it appears to be worthless. The benefits and outcomes of SCSM can be latent but the costs of improving security are apparent: preventing SCS breaches costs money, detection devices (e.g., GPS based tracking devices) cost money, and coordination among supply chain partners to restore operations on the aftermath of SCS crises costs money. In addition, a supply chain is as secure as its weakest link. Just one supply chain partner's irresponsible behavior or nonfeasance could nullify the security efforts of others. As a result, some firms may question why they should invest in supply chain security at all. They argue that these security investments hit their bottom lines and may lack financial justifications (Russell and Saldanha, 2003). These firms are inclined to implement security practices only in order to meet minimum legislative requirements (Thibault et al., 2006).

On the other hand, however, some companies have been proactive in their approach and have implemented a variety of security-focused initiatives and programs (Braunscheidel and Suresh, 2009; Kleindorfer and Saad, 2005; Martha and Subbakrishna, 2002, Sheffi, 2007). These firms usually go above and beyond government mandates in implementing SCSM mechanisms. Why do firms have such differing attitudes toward SCS? What specifically motivates firms to adopt programs that go above and beyond government mandates? In order to understand why SCSM mechanisms have been adopted at differing levels we need to invoke theoretical arguments other than the ones that are conventionally used (e.g., economic theory which suggests that profitability is the driver of organization actions). This dissertation uses the theoretical lenses of the institutional theory to help address this problem. Detailed discussion about the theory and the institutional antecedents of SCSM mechanisms will be provided later.

The fourth research question pertains to the lack of attention regarding the conditions shaping the effects of institutional antecedents on SCSM mechanisms. Firms vary in their perceptions of the need for better SCS and in their ability to implement SCS related initiatives (Williams et al., 2008). From one perspective, a number of firms are not—even partially—aware of the increasing importance of SCS (Rice and Spayd, 2005; Unisys 2005; Williams et al., 2008). This low level of sensitivity for SCS can perhaps be ascribed to supply chain security being inherently complex (Helferich and Cook, 2002; Williams et al., 2008). Specifically, each firm has different security needs. For instance, food and pharmaceutical firms may be highly sensitive to SCS breaches because

adulterated products can make thousands of people sick in a short period (Wein and Liu, 2005). The shared SCS perception within these firms is likely to impact the attitude of employees toward the need for SCS to a point that internal resistance to change (i.e., implementation of SCSM mechanism) would be weakened. As a result, it may strengthen the relationship between the institutional antecedents and SCSM mechanisms, ceteris paribus. In a similar vein, top management commitment toward SCS may also strengthen such relationships, ceteris paribus. When top managers have an active oversight over SCSM, the firm is more likely to develop clear security related objectives and allocate proper levels of resources for securing supply chains.

Finally, the last research question states that the substantive effects of SCSM mechanism on supply chain performance need more empirical validation. Little empirical research has been conducted regarding the relationship between supply chain security related activities and supply chain performance (Williams et al., 2008). For instance, it has been about twelve years since the 9/11 terrorist attacks in 2001 but only 15 empirical studies can be found in the literature. Few of them have appeared in leading operations and supply chain management (O&SCM) journals, indicating that SCS research is still in its infancy. In addition, seven out of the 15 studies do not test the effects of SCSM mechanisms on supply chain performance. For example, Williams et al. (2009b) develop and empirically validate the measurement scales of SCS culture but do not examine the effects of SCS culture on firm performance.

Moreover, these empirical studies appear to generate mixed results. For example, Voss et al. (2009b) demonstrate that "information related" SCSM practices are

positively related to SCS performance. On the other hand, Sheu et al. (2006) posit that the value of Customs-Trade Partnership Against Terrorism program (C-TPAT, one of the most publicized supply chain security programs) as it relates to security is not clear. Thibault et al. (2006) suggest that firms that provide higher levels of SCS are likely to raise their prices, thus jeopardizing their relationships with customers.

1.2 Research Model

To address the aforementioned research questions, this dissertation first conceptualizes and defines supply chain security based on a thorough literature review. It then proposes a taxonomy which groups SCSM mechanisms into four classes and develops a model which links the institutional drivers of SCSM, SCSM mechanisms, organizational traits, and supply chain performance. Figure 1summarizes the overall research model. Each construct is briefly discussed below.

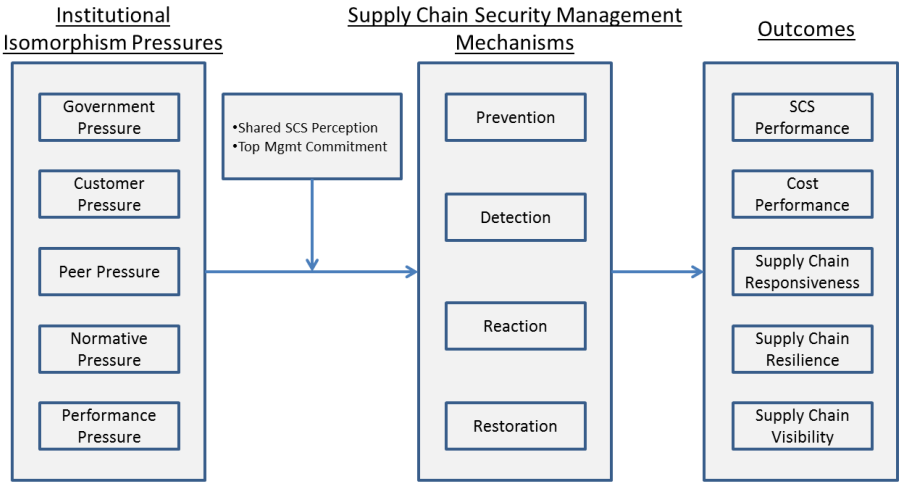

Figure 1. Overall research model

1.2.1 The Conceptualization of SCS

Based on a thorough literature review, supply chain security is defined as the absence of breaches in the supply chain. SCS breaches can include theft, product adulteration, smuggling, counterfeit products, sabotage, terrorist attacks, as well as the illicit acquisition and use of data. This definition is neat and specific in terms of sources of SCS breaches. In this sense, the definition eliminates unnecessary ambiguity and makes the concept easy to understand and measure. A thorough review of the supply chain security literature, the rules guiding construct definition, and examples of SCS breaches will be provided in detail in the next chapter.

1.2.2 Antecedents of SCSM Mechanisms

While defining SCS has important implications to academics, it is also relevant to understand the antecedents of SCS related mechanisms. The evidence has shown that some firms are very proactive in implementing SCSM mechanisms while others are lagging (Braunscheidel and Suresh, 2009; Kleindorfer and Saad, 2005; Martha and Subbakrishna, 2002; Sheffi, 2007), suggesting that the underlying drivers of implementing SCSM mechanisms demands attention. Drawing on the institutional theory (DiMaggio and Powell, 1983; Meyer and Rowan, 1977; Powell, 1991; Scott and Meyer, 1983; Scott, 1987; Zucker 1987), this study proposes five underlying drivers that can induce the adoption of SCSM mechanisms, including government, customer, peer, normative, and performance.

From an institutional perspective, firms operate within a framework of rules, values, and taken-for-granted assumptions about what represents acceptable and appropriate social behaviors. The institutional view suggests that the drivers of organizational behaviors go beyond rational optimization (e.g., profit maximization) to social justifications and obligations (Zukin and DiMaggio, 1990). Organizations are assumed to be recognition seeking, subject to social influences and relatively intractable creatures of habits and traditions (Scott, 2001; Zucker, 1987). Conformity to social expectations (dubbed as legitimacy) contributes to firm success and survival because legitimate firms are more likely to gain social acceptance and thus reap societal resources (Baum and Oliver, 1991; Carroll and Hannan, 1989; DiMaggio and Powell, 1983; Oliver, 1991). Hence, in order to garner legitimacy firms are prone to adopt publically promoted practices (coined as isomorphism process), such as SCSM mechanisms in this case, even in the absence of empirical evidence demonstrating their financial soundness (Powell, 1991; Selznick, 1957; Suchman, 1995).

The classical institutional theory and recent studies suggest four types of isomorphism pressures: coercive, mimetic, normative, and performance (Deephouse and Suchman, 2008; DiMaggio and Powell, 1983; Heugens and Lander, 2009; Meyer and Rowan, 1977; Powell, 1991; Scott and Meyer, 1983; Scott, 1987; Zucker 1987). Coercive pressure results from both formal and informal pressures exerted on organizations by agencies which they are dependent upon. Coercive pressure may institutionalize strategies and practices where their appropriateness is taken-for-granted (Berger and Luckman, 1966) irrespective of their efficacy (e.g., the 10+2 rule issued by

the US Customs and Border Patrol in January 2009 for all importers to meet supply chain security requirements). In the context of SCS, coercive pressure is mainly manifested by government and customer demands to improve SCS.

Mimetic pressure primarily derives from the uncertain nature of business (DiMaggio and Powell, 1983; Scott, 2001). Due to the inherent uncertainty of the business world, organizations are inclined to model after other organizations in order to avoid liability. Firms also imitate their competitors in order to provide similar services to customers and/or gain similar benefits that their rivals have experienced. This isomorphic pressure is mainly denoted as peer pressure and can motivate the adoption of SCSM mechanisms.

Normative pressure stems from cultural expectations and professionalism which in turn guide decision-making (DiMaggio and Powell, 1983; Khalifa and Davison, 2006). In essence, this argument posits that organizational choices are influenced by professional rules and moral and ethical obligations (Scott, 2001). These pressures usually result in "rules of thumb," standard operating procedures, and occupational standards (Hoffman, 1999) and are typically reflected by professional, industry, and cultural norms. Though the pressure to comply can be subtle, firms understand that there is a need to conform to such norms.

Finally, recent studies have illustrated that the need for better performance also generates isomorphic pressure (Deephouse and Suchman, 2008; Heugens and Lander, 2009; Ketokivi and Schroeder, 2004). The cautionary note here is that institutional theorists rarely make an effort to disentangle institutional isomorphism from competitive

isomorphism. Compared to the classical institutional isomorphism processes (i.e., coercive, mimetic, and normative isomorphism), competitive isomorphism is more acceptable to economists and organizational sociologists alike. It emphasizes that market competition weeds out less efficient practices in favor of more efficient ones (Heugens and Lander, 2009; Scott, 2001). Its focus is notably clear on operational efficiency. In other words, the "performance pressure" argument suggests that firms may adopt SCSM mechanisms because they truly believe that such an adoption can improve efficiency and effectiveness, leading to competitive advantage or operational benefits.

From these perspectives, the institutional theory can explain the adoption of SCSM mechanisms. Therefore, this thesis utilizes the institutional theory as a theoretical base and suggests that firms are prone to adopt SCSM mechanisms in order to gain legitimacy and improve performance.

1.2.3 Taxonomy of SCSM Mechanisms

To better understand the SCSM mechanisms, this study uses the principles of the human immune system as a metaphor to categorize SCSM mechanisms into four classes. The SCSM system and the human immune system are very similar. First of all, both systems are designed to protect the wellbeing of the organization. The immune system defends the body from invasions by outside organisms. The SCSM system defends the supply chain and its operations from SCS breaches. Second, both systems are complex and have a multi-layered architecture. The immune system has multiple layers of keratinized cells, with defenses at many levels. The SCSM system holds a clear

hierarchy where at each level (e.g., individual, team, firm, or supply chain level) there can be responses to SCS breaches. Third, both systems need to be tolerant. The immune system has a mechanism to tolerate itself (i.e., does not attack self—elements of the body). The SCSM system, while improving security, has to give considerations to efficiency such that SCS activities (e.g., additional inspections) would not impede normal operations. Fourth, malfunctions of both systems can have devastating consequences. A malfunctioning or a weakened human immune system makes the body vulnerable to attacks and thus the body may suffer serious and dire consequences. Similarly, if the SCSM system cannot respond to SCS breaches effectively, severe economic losses are likely to ensue. In a nutshell, these parallels make it appropriate and reasonable to use the human immune system as a metaphor of the SCSM system.

The human immune system responses to pathogen invasions can be grouped into four classes: prevention, detection, reaction, and restoration (Kaufmann et al., 2004, Playfair and Bancroft, 2004; Segel and Cohen, 2001). The skin is the first line of defense against infection. It forms a tough impenetrable barrier of epithelium protected by keratinized cells. It prevents pathogens from entering the human body. However, if pathogens pass the first line of defense, then certain types of cells (e.g., lymphocytes; one type of white blood cells) can detect pathogens via their antennae. Once the intruders are detected, the immune system produces antimicrobial peptides that kill bacteria, fungi, and enveloped viruses. Finally, if these "intruders" do cause damage, the fluid layer of the immune system, which contains glycoproteins, proteoglycans, and enzymes starts the recovery process of internal tissues. In a similar vein, SCSM

mechanisms can also be grouped into these four classes. For instance, firms can prevent SCS breaches by putting safeguards at the entrances of manufacturing facilities. They can deploy detection mechanisms and utilize advanced technologies (e.g., GPS based tracking devices) to detect existing and potential SCS glitches. Moreover, firms can coordinate with supply chain partners and train their employees so that they can react to SCS breaches timely and effectively. Finally, firms utilize crisis management and disaster recovery plans to rehabilitate processes if SCS breaches do cause damage to the supply network.

1.2.4 Boundary Conditions

In addition to understanding how isomorphic drivers motivate SCSM mechanism, it is also theoretically relevant to consider organization traits that can shape the effects of these drivers on organizational activities. The extant conceptual literature has demonstrated that top management commitment toward SCS (TMC for short) and shared SCS perception within a firm (SSP for short) can serve as boundary conditions that impact the implementation of SCSM mechanisms (Autry and Bobbitt, 2008; Closs and McGarrell, 2004; Martens et al., 2011; Quinn, 2003; Sheffi, 2002; Whipple et al, 2009; Williams et al, 2008). Essentially, TMC promotes the allocation of important resources for SCSM. If the top management treats SCS with respect, the firm is likely to adopt and implement SCSM mechanisms. In contrast, SSP mainly reflects the attitude of the employees toward SCS. Firms with high levels of SSP are likely to put security first. Employees are more likely to believe and accept that SCS is the responsibility of

everyone in the organization. They may be more proactive in implementing SCSM mechanisms and resolving related challenges. As a result, top management commitment and shared SCS perception may shape the relationship between isomorphic pressures and SCSM mechanisms such that the relationship is stronger as the level of top management commitment or shared SCS perception increases.

1.2.5 Consequences of SCSM Mechanisms

Finally, this thesis examines the effects of SCSM mechanisms on supply chain performance. Implementing security related strategies and practices is believed to not only improve security performance but also to generate an array of collateral benefits (Rice and Spayd, 2005; Lee and Wolfe, 2003, Lee and Whang, 2005; Sheffi, 2005; Peleg-Gillai et al., 2006). These collateral benefits include reduction in operating costs, supply chain responsiveness, supply chain resilience (the ability to survive, adapt, and grow in the face of turbulent change), and supply chain visibility among others. Yet, little empirical evidence exists to attest to the relationship between SCSM mechanisms and such collateral benefits (Williams et al., 2008). Given the resource constraints within which most firms have to operate today, it is meaningful, if not critical, to develop a good understanding of how SCSM mechanisms can substantively affect supply chain performance. Specifically, the present thesis examines five supply chain performance measures: SCS performance, supply chain cost performance, supply chain responsiveness, supply chain resilience, and supply chain visibility. The empirical evidence will inform the last research question of this study.

1.3 Research Design and Research Methods

The institutional theory and the tenets of the human immune system are well developed in the literature (Heugens and Lander, 2009; Kaufmann, Medzhitov, and Gordon, 2004; Parham, 2005). As such I will test a variance theory model based on mature theories. The data collected needs to be primarily quantitative (Edmondson and McManus, 2007). A survey based research design is thus adopted. In addition, because of the nature of the topic being security, I will also employ a qualitative approach to gather data to (1) help justify the definition of SCS and (2) refine my hypotheses and enhance the research validity. Therefore, the research design and research methods include four tasks: (1) operationalization of constructs, (2) administration of qualitative interviews, (3) survey data collection, (4) tests of substantive hypotheses.

This dissertation deployed existing manifest variables of institutional isomorphic drivers primarily from a recent literature review of the institutional theory by Heugens and Lander (2009) and several classic studies (e.g., DiMaggio and Powell, 1983). The measurement scales of (1) SCSM mechanisms and (2) supply chain performance measures were mainly created and/or adapted based on prior SCS research (e.g., Sheffi 2001, 2005), industry-oriented reports (the IBM special report series of SCS), and a number of SCS programs developed by governments and international organizations (e.g., C-TPAT, AEO, etc.) The boundary condition variables were mainly adapted from the strategic management as well as the SCM literature (e.g., Barret et al., 2005; Closs and McGarrell, 2004; Floyd and Lane, 2000; Gutierrez and Hintsa, 2006; Hambrick and

Mason, 1984; Mangan and Christopher, 2005; Mena et al., 2009; Peleg-Gillai et al., 2006; Rice and Spayd, 2005).

The target population of the survey primarily includes manufacturing firms operating in the United States and Italy. Considering that I might have to test ten variables simultaneously, I need to have about 200 responses. For this, I need to target approximately 2,000 firms assuming an average response rate of 10% (which is normal in supply chain security and OM research). Before delivering the survey, I conducted 15 interviews with practitioners and academics in order to gather feedback on the survey questions and make sure the concept of each construct is clear to them (a.k.a., pilot test). The interviewees took the survey and provided their comments. This pre-test validated the survey and resulted in refinements of several questions. Paralleled with the survey administration, I further conducted an array of interviews and field tours based on a qualitative approach. The qualitative data allowed me to refine and clarify my propositions. The use of multiple methods also responds to the continuous calls for cross-validated studies by O&SCM scholars (Singhal and Singhal, 2012).

The classic Q-Sort method (Stephenson, 1953) which has been widely used in the social sciences literature was employed to examine the efficacy of the four class taxonomy I developed. I used forced Q-sorting (i.e., I constrained the number of classes to be five: prevention, detection, reaction, restoration, and a N/A class for items that the Q-sorters believe does not belong to any of the four classes) because (1) unforced Q-sorting provides a lower degree of discrimination and suffers from the Barnum effect (Meehl, 1956); (2) the unforced Q-sorting procedure is not more reliable than the forced

one (Block, 1961); and (3) finally the five-class setting is consistent with the arguments I provided in the second chapter.

Finally I used Structural Equations Modeling (SEM) techniques to assess the measurement models and the structural models. Each construct I proposed included at least three manifest variables and had a reflective indicator orientation. All measurement items were measured on a seven point Likert type scale. The data analyses were performed via Mplus and SPSS. Common method bias, non-respondent bias, validity, and reliability were assessed prior to model testing.

In summary, this chapter (1) identified and discussed five major gaps associated with the extant literature on SCS, (2) discussed the specific approach to address these gaps, and (3) proposed a research model linking all of the relevant constructs and elements. Specifically, building on the institutional theory and the metaphor of the human immune system, I posited that five institutional pressures would affect four classes of SCSM mechanisms and subsequently firm performance. In addition, two organizational traits were hypothesized to shape the effects of institutional pressures on SCSM mechanism. In particular, the two organizational traits were expected to amplify the effects on SCSM mechanisms. Finally the research design and research methods are briefly described.

CHAPTER II

LITERATURE REVIEW AND CASE STUDIES

Chapter I proposed research questions, briefly discussed the key constructs, and described the overall model of this thesis. In this chapter, I provide an extensive review of the supply chain security literature and respond to the first two research questions (i.e., defining supply chain security, and constructing a taxonomy of SCSM mechanisms). I then justify the definition and the taxonomy through four in-depth case studies.

2.1 Review of Supply Chain Security Research

I begin this section with an extensive review of the SCS literature. Because a sizable number of security related papers appears at journals which are dedicated to niche areas (e.g., transportation, physical distribution, product management), constraining the review to only leading Operations and Supply Chain Management (O&SCM) journals seems to be untenable. Therefore, both leading and other notable O&SCM outlets are reviewed. Eight key words—"security", "safety", "supply chain risk", "supply chain disruption", "terrorism", "theft", "smuggling", "adulteration"—are used to help identify relevant papers published between 2000 and 2012. A total of 941 papers were located (Table 1).

Table 1. Reviewed journals

Journal	No. of Papers Identified
Leading O&SCM Journals	
Management Science (MS)	50
Manufacturing & Service Operations Management (MSOM)	3
Journal of Operations Management (JOM)	89
Decision Sciences Journal (DSJ)	76
Production and Operations Management (POM)	67
Other Notable O&SCM Journals	
Journal of Business Logistics (JBL)	46
Journal of Supply Chain Management (JSCM)	69
International Journal of Physical Distribution & Logistics Management (IJPDLM)	123
International Journal of Productions Economies (IJPE)	135
International Journal of Logistics Management (IJLM)	40
International Journal of Operations & Production Management (IJOPM)	99
Practitioner-oriented O&SCM Journals	
Supply Chain Management Review (SCMR)	40
Harvard Business Review (HBR)	57
Sloan Management Review (SMR)	40
California Management Review (CMR)	7
	Total: 941

The use of the eight key words helps to minimize the probability that a relevant study will be excluded in the review. However the large number of key words also inevitably inflates the probability that an irrelevant study will be included. For example, a number of papers regarding financial investment decisions are identified by the key word "security" because "security" is used as a negotiable financial instrument representing financial value (see, Securities Exchange Act of 1934). Several additional criteria are then applied to filter out irrelevant papers.

First, papers without a clear operations/supply chain-oriented focus were discarded. Second, some brief academic notes were also eliminated. These notes are usually very short (typically 2-3 pages) and appear in the format of interview records. These notes are primarily published in practitioner-oriented journals (e.g., Supply Chain

Management Review) and mainly illustrate that SCS is an important issue for practitioners.

Third, SCS breaches represent a special type of supply chain risk. As Autry and Bobbitt (2008) state, supply chain security and risk have conceptual overlap but have different foci. Supply chain risk generally refers to any uncertainty arising from (1) problems of coordinating supply and demand or (2) disruptions to normal activities (Kleindorfer and Saad, 2005). In contrast, supply chain security mainly refers to intentionally generated breaches in the supply chain which may include theft, smuggling, adulteration, counterfeit products, sabotage, illicit acquisition of data, or terrorist attacks (Speier et al., 2011). The focus of this thesis is on SCS breaches.

Fourth, this thesis distinguishes between supply chain security and safety as well. ISO 28000 states that "a supply chain is secure when it can resist, fend off, or withstand unauthorized acts that are designed to cause intentional harm or damage". Supply chain safety, on the other hand, can be affected by both intentional and unintentional acts which can compromise the integrity of a supply chain. For example, the accidental exposure of produce to bacteria through a polluted water source is an unintentional act. On the other hand, terrorists can intentionally introduce harmful pathogens in the supply chain via fresh produce. In both instances, the safety of the food supply chain is compromised. This review only includes studies that explore the processes/strategies to tackle supply chain security issues.

Finally, in addition to academic studies, some relevant government, regional (e.g., the European Union), and international organization reports are also reviewed. A

typical example of this type of study is a Department of Homeland Security (DHS) report or a subsection of the ISO 28000 standard. These reports are not listed in the review table because of the fairly large number of these reports. Nevertheless, citations will be provided in the rest of the dissertation when a specific report is referenced.

As a cross-check against potential subjective bias, a second reviewer who is familiar with the supply chain security literature filtered the 941 identified papers using the same criteria. His comments and suggestions resulted in minor revisions of the author's results. Table 2 presents the 29 papers that will be further discussed next.

This thesis organizes the review chronologically. Such organization allows for a bird's-eye-view of how the supply chain security literature evolved over time. It is also helpful to identify the coherence as well as diversity within the literature and to capture any cumulative patterns.

Table 2. Review of the supply chain security literature

Study	SCSM-performance relation	Drivers of SCSM	Define SCS	Nature of research	Research method	Sample size	Journal
Sheffi (2001)	No	No	No	Conceptual		N/A	IJLM
Lee & Wolfe (2003)	Yes	No	No	Conceptual		N/A	SCMR
Rice & Caniato (2003)	No	No	No	Conceptual		N/A	SCMR
Russell & Saldanha (2003)	No	No	No	Conceptual		N/A	TJ
Closs & McGarrell (2004)	Yes	No	No	Conceptual		N/A	Industry Report
Prokop (2004)	No	No	No	Analytical / descriptive	Quantitative / game theory modeling		IJLM
Kleindorfer & Saad (2005)	No	No	No	Conceptual		N/A	POM
Lee & Whang (2005)	Yes	No	No	Mixed	Quantitative model + 1 case study	1	IJPE
Rice & Spayd (2005)	Yes	No	No	Conceptual		N/A	Industry Report
Peleg-Gillai et al. (2006)	Yes	N/A	No	Empirical / descriptive	Quantitative / survey	14	Industry Report

Table 2. continued

Sarathy (2006)	No	No	No	Conceptual		N/A	TJ
Sheu et al. (2006)	Yes	No	No	Empirical / descriptive	Mixed	5 cases	SCM: a IJ
Thibault et al. (2006)	Yes	No	No	Empirical / descriptive	Qualitative / interviews	24[a]	TS
Autry & Bobbitt (2008)	Yes	N/A	No	Empirical / descriptive	Qualitative / structured interviews	31[a]	IJLM
Closs et al. (2008)	No	No	No	Conceptual		N/A	SCMR
Chao & Lin (2009)	No	No	No	Empirical / explanatory	Quantitative / survey	161	IJPE
Ekwall (2009)	No	No	No	Empirical / explanatory?	Mixed	6 interviews; 4 survey responses	IJPDLM
Reade (2009)	No	No	No	Empirical / descriptive	Quantitative / survey	898	IJPDLM
Voss et al. (2009a)	No	No	No	Empirical / descriptive	Quantitative / survey	107	JBL
Voss et al. (2009b)	No	No	No	Empirical / descriptive	Mixed	199	TS
Whipple et al. (2009)	No	No	No	Empirical / descriptive	Mixed	50 interviews w/ 15 firms; 195 survey responses	IJPDLM
Williams et al. (2009a)	No	Yes	No	Empirical / descriptive	Qualitative / interviews	17[a]	IJPDLM
Williams et al. (2009b)	No	No	No	Empirical / descriptive	Quantitative / survey	n_1=62 (pretest) n_2=102	IJLM
Atwater et al. (2010)	Yes	N/A	No	Empirical / descriptive	Quantitative / panel data	270	JBL
Bakshi & Gans (2010)	No	No	No	Analytical / explanatory	Quantitative / game theory modeling	N/A	MS
Bakshi et al. (2011)	No	No	No	Analytical / explanatory	Quantitative / queuing simulation	N/A	MS
Martens et al. (2011)	Yes	No	No	Empirical / explanatory	Quantitative / survey	69	JBL
Marucheck et al. (2011)	No	No	No	Conceptual		N/A	JOM
Speier et al. (2011)	Yes	No	No	Empirical / explanatory	Mixed	75 interviews; 199 survey responses	JOM

[a]: It refers to the number of interviews conducted. The authors did not report the number of firms involved.

Table 3. Rethinking supply chain security

	Before 9/11terrorist attacks	After 9/11terrorist attacks
The changes in scale and scope of SCS challenges	SCS is tasked to avert taking things "out of" the supply chain. e.g., employee theft.	SCS also needs to prevent things from getting "into" the supply chain. e.g., weapon smuggling or drug smuggling
	The SCS war is a war against business organizations	The SCS war is a war against the government, the people, and the business organizations
	SCS needs intensive attention from the focal firms	SCS needs not only intensive attention from the focal firms but also intensive collaboration between public and private sectors
	The SCS war is fought by professionals (policemen or guards)	The SCS war is fought by all affected parties (government, public and private firms, and even citizens), but most efforts are undertaken by private firms
	Security can be lax since its potential impact is limited.	Security cannot be compromised because it impacts human lives as well as financial performance

The early studies are primarily conceptual in nature and suggest that SCS is both important and relevant. Many early studies are exploratory and their perspective is broad. These papers are mainly motivated by a number of SCS breaches such as the 9/11 terrorist attacks of the early 2000s'. They suggest that the scale and scope of SCS challenges have fundamentally changed (Table 3). Better SCS requires not only the extensive efforts from the focal firms but also collaboration among all related parties across the supply network.

According to Sheffi (2001), the threat of terrorism is a continuous danger. The war against terrorists would be fought primarily *not* by a professional army *but* by business organizations and normal citizens. The importance of winning this battle goes beyond plain costs to human life. Consequently, to be actively prepared for the next attack firms would have to rethink their supply chain operations, adapting to increasing supply chain uncertainties, and building up public-private collaboration.

The business value of better SCS is also relevant. Rice and Caniato (2003) propose that global supply chains are inherently vulnerable to disruptions. The economic losses emanating from these disruptions are considerable and sometimes devastating (Hendricks and Singhal, 2003, 2005). To build a secure and resilient supply network, Russell and Saldanha (2003) discuss several tenets of security-sensitive logistics systems with the focus on partnership development and flexibility building.

Adding to these studies, Lee and Wolfe (2003) and Lee and Whang (2005) explore the potential relationship between the Total Quality Management (TQM) philosophy and SCS. They view SCS breaches as analogous to quality defects. They suggest that the SCS purview no longer merely includes issues such as theft and contraband (of illegal drugs, illegal immigrants, and export of stolen goods). It also includes the protection of a supply chain against the threat of terrorist attacks. Governments and industry need to work with each other to build confidence—ensuring public safety while maintaining smooth flows of goods and services in the global supply system. One possible way to generate confidence is to apply the TQM principles in designing and operating supply chains to assure SCS. Several strategies, such as building the ability to detect a SCS breach as soon as it occurs, are suggested (Lee and Wolfe, 2003) and a quantitative model is put forward to show that firms can achieve higher levels of SCS at lower cost (Lee and Whang, 2005).

While no formal definition of supply chain security is provided, the early studies do provide innovative thinking and mixed evidence which are ample to motivate future research. Prokop (2004) constructs a game between shippers and carriers in the context

of inbound cargo security based on rules issued by the U.S. Customs and Border Protection (CBP). The results imply that both players (i.e., the shipper and the buyer) may be active and take the first move depending on the requirements of the rules. For instance, the shippers will make the first move when the rule is compulsory (such as the Container Security Initiative (CSI)) because they have little choice but to comply. But when the rule is optional (such as FAST), both parties may become the first mover.

Thibault et al. (2006) study the response of the U.S. maritime industry regarding the Container Security Initiative. The findings show that the regulation fostered a cooperative relationship between industry and government as it relates to supply chain security. This study seems to suggest that firms which are active in enhancing SCS and the adoption of SCSM mechanisms do garner collateral benefits such as sturdy industry-government relationships. However, Sheu et al. (2006) demonstrate that because a given SCSM initiative (i.e., C-TPAT program in their study) is a means rather than an end, its value to SCS is, in fact, not clear.

While it is possible that the short-term cost of SCSM mechanisms could be balanced out by long-term gains from improved supply chain performance (Sarathy, 2006), what benefits firms can actually generate from better security is unclear. The exploration of firm strategies and actions targeting SCS breaches is also scant in these early studies. As Sarathy (2006) argues, firms should design security into the supply chain rather than seek solutions on the aftermath of SCS breaches. However, prior to investing in supply chain security, organizational actors need to justify their decisions.

Several industry-initiated and practitioner-oriented reports help address the concerns regarding benefits that can be generated via the implementation of SCSM mechanisms. The collateral benefits and implementation issues of SCSM mechanisms are the foci of these reports. Three reports (i.e., Closs and McGarrell, 2004; Rice and Spayd, 2005; and Peleg-Gillai et al., 2006) from the Special Report Series—Supply Chain Security, sponsored by the IBM Center for the Business of Government, are carefully reviewed here.

In contrast to the early studies (published between 2001 and 2004), the perspective of these reports is exclusively practitioner-oriented. The questions these reports attempt to answer are (1) how can firms effectively implement SCSM mechanisms? (2) are these SCSM mechanisms really beneficial to firms?

Closs and McGarrell (2004) argue that firms have to understand the key challenges (i.e., the five "Vs": velocity, variability, value, vulnerability, and visibility) of supply chain security in order to effectively implement SCSM mechanisms. Building on prior research (e.g., Lee and Wolfe, 2003; Russell and Saldanha, 2003), Closs and McGarrel put forward several criteria that help to gauge the implementation of SCSM mechanisms. For instance, firms can assess their supply chain vulnerability in several ways. The authors suggest that a measure such as "report self-assessments of vulnerability" is an indicator of regular (i.e., low level) security evaluation, while a measure such as "performing unannounced inspections or validation by third parties firms to detect vulnerability" is an indicator of high level of security evaluation. These

criteria serve as a "checklist" that allows firms to assess their current SCS level and set up future SCS targets.

Yet, the specific mechanics of implementing SCSM mechanisms is not the only concern of practitioners. Rice and Spayd (2005) address the industry wide concern that government actions to impose tougher security-related standards and processes erode trade efficiency by adding cost and complexity. The authors develop a framework for executives, researchers, and government officers to ask questions, conduct research, and make decisions about how to approach investments in SCS. They argue that there has been a great deal of speculation in this area, but very little data. The framework they provide facilitates communication among all related parties and therefore can lead to better collaboration. The report further illustrates that there is increasing evidence and rationale suggesting that meaningful benefits, including improved SCS performance, reduced overall cost, and improved efficiencies, are created from prudent SCS investments.

Peleg-Gillai et al. (2006) further extend the findings of the first two reports and suggest that better security drives business value. They provide an overview of major existing SCSM initiatives/programs and their respective collateral benefits (Figure 2). In contrast to prior reports, the authors did collect data from both manufacturers and logistics service providers to support their core arguments (i.e., SCS investments are beneficial). Firms participating in the study do grab collateral benefits by implementing SCSM mechanisms. The findings clearly indicate that significant business value accrues from supply chain security investments. However, the limitation is that the sample size

was very small (n=14) and all companies involved were industry leaders. In other words, the findings may be atypical.

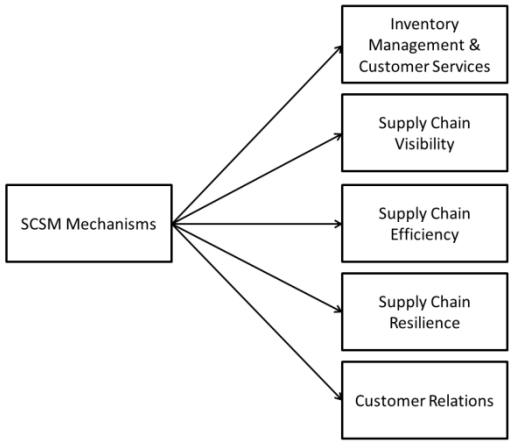

Figure 2. Collateral benefits of SCSM mechanisms

While the endeavors of these reports are primarily to help practitioners, they contribute to the academic literature as well. One of the contributions is that they furnish a set of prototypical measurement scales that help scholars to develop robust SCSM constructs. Another important contribution of these reports is that they offer useful rationale and some empirical evidence to justify the value of SCS investments. Nevertheless, the narrow breadth of these studies undermines the contribution of these reports. For example, the collateral benefits proposed are primarily operational and the link between SCSM mechanism and real financial outcome is not empirically justified.

To address these questions, the recent SCS literature (primarily papers published in 2007-2012) has moved forward to a number of empirical and analytical inquiries.

Compared to the early papers, the recent studies are more quantitative in nature. A number of relations which were conceptually proposed in the early papers are analytically modeled or empirically tested. The interaction between government authorities and business organizations (some authors refer this as public-private sector interaction, see Lee and Whang, 2004) is one of these conceptual relations. When studying the impact of the 100% inspection of U.S.-bound containers policy, Bakshi and Gans (2010) show that the C-TPAT program can shift some of the U.S. Bureau of Customs and Border Protection's (CBP) burdens to trading firms. Their results suggest that that CBP may use strategic delays as an incentive for firms to join the C-TPAT program. The 100% inspection policy has been also critiqued since it is somewhat impractical and may impede global trade. As Bakshi et al. (2011) further highlight, CBP can only handle a small portion of the total load. Based on the data from two large international terminals, a simulation was performed and the results show that an alternative of the 100% inspection policy—a rapid primary scan of all containers, followed by a more careful secondary scan of only a few containers that failed the primary test—is more feasible (Bakshi et al., 2011).

Other mandatory or voluntary government initiated SCSM initiatives also have strong effects on organizational behavior. Atwater et al. (2010) examine a five-year (1999-2003) panel data set and illustrate that almost 40% of motor carriers altered their strategies after 9/11 due to the changes of highway security requirements. Their analysis demonstrates that while both changed and non-changed firms suffered declines in operating income after 9/11, the non-changed group experienced a much steeper decline.

The impact of heightened SCS needs has generated a spillover effect on supply chain partners as well. Voss et al. (2009a) examined SCS related supplier selection criteria in the food industry. The authors argue that there are tradeoffs between SCS and other performance dimensions, such as delivery reliability. Their simulation results show that under some conditions (e.g., sourcing domestically) food processing firms are not willing to trade off operational benefits (e.g., delivery reliability) for better SCS when it comes to supplier selection.

While acknowledging that external parties (e.g., government, customer) can shape a firm's SCSM activities, some scholars have also paid great attention to internal factors that affect security-related organizational behaviors. Chao and Lin (2009) show that a firm's attitude toward SCS has a significant impact on the intention to adopt container security services (i.e., hire a third party to secure containers). Voss et al. (2009b) demonstrate that firms that place a high strategic priority on SCS generally have a greater ability to detect and recover from SCS breaches compared to firms that place a low strategic priority on SCS. Similarly, Whipple et al. (2009) illustrate that firms operating globally placed more importance on SCS than firms operating domestically. These global firms are more likely to assess the SCSM procedures of their supply chain partners, and thus achieve better SCS performance. Their cluster analysis further validates the findings as the high performance group is dominated by international firms.

Reade (2009) further moved the analysis from the firm level to the individual level. He suggests that SCS is also a concern of common employees. He examines the relationship between employee sensitivity to terrorism and attitude of employees toward

their job and organization in Sri Lanka, where terrorism is a societal problem. The author used correlation analysis to examine the proposed relationship and found a statistically significant negative correlation, indicating that the threat of terrorist attacks eroded the employees' commitment to their organization.

Results based on the aforementioned studies have enriched the supply chain security literature by providing analytical and empirical evidence. In the meanwhile, other scholars have recognized the lack of theoretical and conceptual development of the supply chain security research (Closs et al., 2008). The scope of SCS is broad and different aspects of SCS are rather scattered. For example, there is an abundance of "best" strategies and practices but few frameworks that link these strategies and practices together exist (Closs et al., 2008). In response to this, Autry and Bobbitt (2008) developed a framework of what the authors called supply chain security orientation (SCSO, "a firm-level construct addressing companies' multiple approaches toward mitigation of supply chain security breaches and supply chain risk management", p. 42) to categorize a firm's SCSM efforts. Based on several interviews, they suggest that SCSO includes four dimensions: preparation and planning initiatives, supply chain security-related partnerships, organizational adaptation, and security-focused communications and technology.

Speier et al. (2011) integrate three theoretical perspectives (i.e., normal accident theory, high reliability theory, and situational crime prevention) to develop a framework that examines the threat of potential disruptions on supply chain processes. Data collected from the food industry suggests that the depth and breadth of SCSM

mechanisms implemented depend on top management mindfulness (i.e., perception of the need of SCS), operational complexity, product risk, and coupling (i.e., complex interdependency). Nevertheless, Speier et al. (2011) discuss both safety and security in their study.

In addition to the aforementioned papers, the literature has also seen the efforts to develop and validate the measurement scales of SCS-oriented culture (Williams et al., 2009b); apply the crime displacement theory to explain why cargo theft continued to be a significant problem despite the implementation of various countermeasures (Ekwall, 2009); and identify the antecedents of SCS effectiveness (Martens et al., 2011). Indeed, Marucheck et al. (2011) published an editorial essay which focuses on how the field of O&SCM can offer fresh insights to address supply chain safety and security challenges. Based on the examination of safety and security issues in five industries, they describe four areas where innovative solutions could be provided in addressing these problems: regulation and standards, product lifecycle management, traceability and recall management, and supplier relationships. Nevertheless, the authors do not formally distinguish safety from security in their work.

One important observation in the literature is that the antecedents of SCSM mechanisms are by and large ignored. The only exception is Williams et al. (2009a). Based on 19 interviews, Williams and colleagues concluded that four drivers exist: government, customers, competitors, and society. However, they do not compare the relative power of these drivers nor do they include performance pressure as a potential and critical driver; both are major concerns of this thesis.

Another and probably more important observation is that the foci of the supply chain security studies appear to be very scattered. The concept of SCS seems to be very broad, and thereby unclear and hard to use. The absence of a formal definition of SCS may greatly jeopardize the development of this stream of research. Therefore this thesis moves forward to conceptualize SCS next.

2.2 Conceptualization of Supply Chain Security

2.2.1 A Review of the Concept of Security in Different Disciplines

The ambiguity of the term supply chain security perhaps stems from the ambiguity of the term security, which has a wide range of meanings. Studies from multiple disciplines have suggested that security is multidimensional in nature and diverse in practice (Brooks, 2010).

In the sociological literature where the concept of security originates, Fischer and Green (2004, p.21) suggest that security "implies a stable, relatively predictable environment in which an individual or group may pursue its ends without disruption or harm and without fear of disturbance or inquiry." A more traditional and narrow definition conceptualizes security as the protection of information, assets, and people for individual safety and community wellness (Craighead, 2003). Some scholars also suggest that security may be considered as the prevention of undesirable, unauthorized, and detrimental loss to an organization's or individual's assets (Post and Kingsbury, 1991). Those definitions portray security as a private and/or commercial need as individuals and/or business assets are the subjects that need to be secured. However, the

sociology literature also expands to consider security at the national level. In this line of studies, security is linked to the defense of a nation through armed forces (Walt, 1991). Security is also associated with public policing and the use of armed forces to protect (sometimes even control) the citizens (Jones and Newburn, 1998). In all of those conceptualizations, security is described as either an ideal status (i.e., being secured) or a means to achieve that status, despite that the specific meaning of security may vary given the time, place, and context (Davidson, 2005).

In the criminology literature, security is connected with the concept of law and order. Security emphasizes unlawful and anti-social events and their causes and consequences. A belief shared by many criminology scholars is that crime prevention and security always go together (Manunta, 1999). Security is desired, as it impedes crime. Security is valued for the role it plays to maintain the stability of the society. Some other scholars, however, argue that security is not always for the best and should not be considered free of dangers. The unconstrained achievement of one's security may actually jeopardize that of others, by threatening them or by transferring threats onto them (Dillon, 1996). In this sense, security is driven by not law-abiding motives but self-utility. On the whole in the criminology studies, security is either the means which helps to ensure law (or achieve self-utility) or the resulting condition. Nevertheless, a review by Zedner (2003) suggests that security is better considered a "state of being". According to Zedner, the purported security ends are "either objective freedom from risk (protection, guard, or defense) or the subjective feeling of safety (or absence of fear or apprehension) (p.155)"; even some researchers propose that security could be the means

to that purported ends, “the pursuit of security may be something like an end in itself” (p.157).

In the management literature, most scholars tend to treat security as an operational tool to prevent or reduce risks which cannot be accepted or transferred (Broder, 1984). This understanding is derived from the assumption that risks cannot be totally removed and therefore losses will anyway be suffered. In other words, the core idea is that reduction (of risks) is more important than removal. Therefore, security is usually defined by a standard (e.g., the acceptable level of losses) and the cost effectiveness of security measures which is to be judged against that standard. Under this condition, security and loss reduction are interchangeable. Nevertheless, some scholars believe that security is in principle risk-averse. Confining security to an acceptable level of losses makes it hard to explain voluntary risk-taking in practice. An alternative explanation is that some minor risks should be tolerated as scarce resources need to be channeled toward more important ones. By evaluating potential risks, limited resources can be used to achieve the best possible results. As such, the concept of security is broader than just loss prevention.

In summary, the concept of security is capacious, dangerously capable of meaning quite a few things to different constituents.

2.2.2 Supply Chain Security

While the concept of security may be too broad to be practicable (Manunta and Manunta, 2006), meaningful definition could still be achieved when that definition is

dependent on a specific applied context (Brooks, 2010). The context of supply chain management thus allows me to provide a precise enough but yet practically applicable definition of supply chain security.

2.2.2.1 Supply Chain Risk and Supply Chain Security

Supply chain security issues are considered a special type of risk embedded in the supply chains; the supply chain management literature has a long history to deal with supply chain risks. Is it possible, however, for SCS to be effectively defined in terms of the classic risk notions of (1) the probability of a risk and (2) the magnitude losses related to that risk (Shavell, 1984; Saad and Kleindofer, 2005)? The answer is probably no. The probabilistic concept of risk is built upon the daring assumption that decision makers can possibly make informed choices about future events whose likelihood and outcomes are known, or at least assessable with a reasonable degree of reliability. The approach of utilizing event consequences and their associated probability to manage risk is widely endorsed for two reasons: its formal simplicity and its aid to rational decision-making (Manunta, 2002). However, both reasons seem unsustainable for SCS.

First, the analysis of SCS breaches cannot be reduced to simple mathematical formulas. SCS breaches are more complex than general supply chain risks, such as supply shortage and demand uncertainty. SCS breaches are very often characterized by their irregularity. They may occur suddenly and simultaneously; their outcomes are uncertain or even unthinkable (unknown probability from a mathematical perspective); they are sensitive to time, people, and environment; and finally they go beyond monetary

considerations to human lives. SCS breaches depend on human actions (people who intentionally cause SCS problems), which should not be considered as errors, and reactions made by people in response to SCS breaches may prove right in some cases but wrong in others. Both conditions violate the basic assumptions made by mathematicians such as Bayes, von Leibniz, and Laplace, invalidating the statistical value of prediction.

Second, the SCS assessment based on the probability approach may not provide a reliable account of reality. The probabilities associated with SCS breaches could be very subjective and thus are somewhat far away from objectivity and accuracy. As Kahneman and Tversky (1979) suggest, decision makers tend to use their perceptions rather than "reliable numbers" to make choice. The fear of the so-called mad cow disease is an excellent example: extremely low probabilities of the most feared negative results—one person per year in the U.K. contracts the human-variant degenerative neurological disorder—outweigh much higher probabilities of less feared ones (e.g., poison outbreak, affecting one in 3,000 people per year) (Oxford statistics, 2001). In the SCS area, the fear of SCS disasters, such as the 9/11 terrorist attacks, may lead to highly subjective and overestimated probabilities. As such, the probabilistic approach is hardly reliable in the SCS area and barely helpful in rational decision-making.

Taken together, the arguments of simplicity and rationality hold little water when it comes to SCSM. The use of the classic risk notions to define SCS seems to be untenable. While SCS involves about a sub-group of supply chain risks, its unique attributes make it hard to be defined using general and simple risk management languages.

2.2.2.2 Supply Chain Safety and Supply Chain Security

Supply chain safety and supply chain security are sometimes used interchangeably in the literature (Speier et al., 2011). The reason of this use is apparent and understandable. Both safety and security encompass the meaning of protection, harmlessness, reliability, free of danger, etc. Under the arena of supply chain management, both of them imply that the supply chain network has procedures to protect the supply chain assets from theft, damage, or terrorism. However, despite their conceptual overlaps, some scholars suggest that the two concepts are different. For example, supply chain safety leads to better product safety which refers to "the reduction in the probability that use of a product will result in illness, injury, death or negative consequences to people, property or equipment" (Marucheck et al., 2011, p. 708). Supply chain security, on the other hand, implies the delivery of a product is uncompromised within the supply chain (Marucheck et al., 2011). In this sense, improving SCS is one way to enhance supply chain safety. Safety is a broader concept with security embedded in it. Nevertheless, if safety comprises security, then anything that is safe must also be secure. Yet this is not always the case: a warehouse can be safe (i.e., no one wants to attack or steal from it) but not secure (e.g., not equipped with anti-theft devices).

Another view, which helps to remedy the aforementioned conflict, is that supply chain safety and security can be distinguished based on the intention of the source of the problems. Safety is concerned more with unintentional structural failures and "acts of God", while security is dealing with intentional behaviors which result in harm or

damage (Zedner, 2003). This view is in line with the ISO-28000 standard, which states that "a supply chain is secure when it can resist, fend off, or withstand unauthorized acts that are designed to cause intentional harm or damage". In this sense, SCS entails the efforts to avoid and respond to intentional acts, while supply chain safety concerns both intentional and unintentional acts which may compromise the integrity of a supply chain. For example, the accidental exposure of produce to bacteria through a polluted water source is an unintentional act (i.e., a supply chain safety issue). On the other hand, terrorists can intentionally introduce harmful pathogens in the supply chain via fresh produce (i.e., a supply chain security issue). In both instances, the integrity of a supply chain is compromised. This view is adopted in this thesis as it provides the opportunity to effectively differentiate supply chain security from supply chain safety, and therefore to accurately define SCS.

2.2.2.3 Supply Chain Security: A Means or an End?

In supply chain management, security is usually associated with negative nuances, a distinguishing feature of the criminology literature. SCS breaches such as theft, product adulteration, and smuggling imply the failure of anti-crime processes and/or the failure of penalties associated with those criminal and unethical activities (as specified in supply contracts). Given this negative connotation, it is hardly surprising that it is perhaps insecurity and the demand for better security that drive reactions to SCS breaches. Demands for better security against crimes reflect a managers' subjective feeling of insecurity, regardless of whether this sense of insecurity is or is not well

founded in practice. Under such circumstances, SCS communicates an ideal status, absence of negative events. As Spitzer observed, "security…is said to exist when something does not occur rather than when it does…when stores are not robbed, pedestrians are not molested" (1996, p. 43). In other words, SCS should be portrayed as the expected outcome of an organization's SCSM efforts.

This end view is adopted by most SCS researchers. From this perspective, SCS refers to the extent to which the supply network can prevent (or withstand) any kind of SCS breaches. For example, by describing supply chain security management as "the application of policies, procedures, and technology to protect supply chain assets (product, facilities, equipment, information, and personnel) from theft, damage, or terrorism and to prevent the introduction of unauthorized contraband, people or weapons of mass destruction into the supply chain (2004, p.8)", Closs and McGarrell indirectly imply that SCS is the outcome of an array of security related activities and mechanisms.

Other researchers, however, suggest that SCS could be the means (actual activities and efforts) that aims at achieving high levels of security performance. For example, Sarathy (2006) argues that firms should design security into the supply chains, indicating that SCS is embedded within supply chain operations and processes. SCS combines traditional supply chain management practices with new security requirements. As Williams et al. conclude, supply chain security "is a means to regulate the movement of conflict goods (i.e., profitable but illegal products such as weapons) and the people associated with them." (2008, p. 267)

While both views have their rationales, the end perspective is preferred. Under the means perspective, the broad scope of SCS activities has made the definition of SCS imprecise at best as the definition cannot capture all of the important SCSM measures. The imprecision not only means many divergent measures can be justified under the name of supply chain security, but also gives license to potential unusual measures that may otherwise appear indefensible. The expected outcome (the end) of these security means is, however, identical and consistent (i.e., better security). This end view is also consistent with the preferred criminological definitions of security as we reviewed in the previous section.

2.2.2.4 Defining Supply Chain Security

Having distinguished security from general risk and safety and proposed supply chain security as an end of SCSM efforts, I move to discuss the criteria of developing a good definition. Many scholars have provided several criteria of what constitutes a "good" definition (Kaplan, 1964; Dubin, 1978; Hunt, 1991). In general, their suggestions are similar to Hempel's (1970) statement that "good conceptual definitions should exhibit inclusivity, exclusivity, differentiability, clarity, communicability, consistency, and parsimony" (p. 654). However, recent studies have argued that these suggestions are too abstract and do not provide examples of how they can be applied (Wacker, 2004). Instead, Wacker (2004) provides several specific rules of constructing a good definition which are tailored for the O&SCM research. This study follows these rules to conceptualize SCS. Nevertheless, one important note here is that not all rules Wacker

proposed are applicable in this study. For example, Wacker assumes that the concept which is to be formally defined has been somewhat developed in the literature, and therefore he suggests that the definition "should be as similar as possible between studies" (rule 5 in table 2, p. 638). In the context of my study, supply chain security research is however still in its infancy. As table 2 suggests, there are no existing studies, which provide the definition of supply chain security, to be consistent with.

Six specific rules are then followed to define supply chain security (Wacker, 2004, p. 634-637): (1) the concept is defined using primitive terms which are assumed to be known by the readers; (2) the definition should exclude shared terms with other definitions to reduce confusion; (3) the definitions should not use vague or ambiguous terms; (4) the definition should have as few as possible terms (i.e., parsimony); (5) the definition should not make any term broader (i.e., expanding the domain); (6) the definitions should not introduce any new hypotheses.

Based on the review of the literature and following the rules proposed by Wacker (2004), this study defines supply chain security as the absence of breaches in the supply chain. The sources of breaches include theft, product adulteration, smuggling, counterfeit products, sabotage, terrorist attacks, as well as illicit acquisition and use of data. The definition communicates an ideal status of the supply chain, zero breaches. The definition is neat, parsimonious, and easy to understand (rule 1-4). By inventorying the sources of supply chain breaches it also offers a clear "content domain" to distinguish security from other similar concepts (rule 5). The list of breach sources also helps managers to facilitate the execution of security actions because it lists areas that

need to be dealt with. No hypotheses are introduced (e.g., security means better performance, rule 6). To further justify this definition, we provide examples of each source of breaches below.

Theft is one of the most common SCS breaches. Even well secured supply chains could be the targets of a heist. In a recent example, thieves broke into Eli Lilly and Co.'s warehouse located in Enfield, Connecticut in March, 2010. The thieves waged a high-tech assault as they cut a hole in the roof, rappelled inside, disabled the alarms, and removed enough drugs to fill a tractor trailer. They made away with approximately $75 million worth of prescription drugs (ABC News, 2010). As for product adulteration, one recent example is the failure of the gigantic Chinese milk producer Sanlu in 2008. The company failed to detect the use of melamine by its suppliers. The tainted product processed by Sanlu lead to the death of three babies and more than a thousand ill infants. The company went bankrupt and the milk industry lost approximately $5 billion in sales (A.T. Kearney Analysis, 2010).

Smuggling has been a big concern to nations and firms for a long time. It includes not only smuggling of people and weapons, but also smuggling of high value illegal substances such as cocaine. Recently, police in Spain have recovered 162 kilos of cocaine with a street value of approximately $20 million, hidden inside plastic bananas. They were concealed in a 22-ton shipment of real fruit that arrived from Ecuador, “the imitated bananas, which were very similar to real bananas, were hidden amongst a shipment of real fruit,” the interior ministry said on Jan 13, 2011 (kyero.com, 2011).

Counterfeit products also present serious SCS challenges. For instance, while the Chinese authorities investigated 480,000 cases of counterfeit drugs worth $57 million and closed 1,300 factories in 2001, 192,000 deaths were attributed to counterfeit drugs in China in the same year (Wellcome Trust report, 2009). Accounts of counterfeit products abound (e.g., eggs, gum, airbags, etc.) Sabotage can generate serious consequences as well. For example, Disney recalled 3.4 million videos of the animated film "The Rescuers" in 1999 because one "angry" employee tampered the video release versions by adding an obscene photograph in two frames (The New York Times, 1999). In another example of sabotage, Forbes' New York operations were shut down for two days as a former employee crashed five of the company's eight servers after being fired from a temporary position.

Acts of terrorism can also be rather consequential and unfortunately there are many means that terrorists can use to inflict pain. Food poisoning could be one of the easiest and economically and psychologically most devastating. For example, in 1984, members of an Oregon religious commune tried to influence a local election by poisoning salad bars with salmonella bacteria to sicken voters. Although no one died, 751 people became ill (Homeland Security Report, 2006). Lastly, SONY's 2011 data breach is the most recent example of illicit use of data. The attack launched by a hacker cost the company approximately $171.4 million due to the theft of 77 million customer records. The company had to temporarily terminate its online services in order to locate the security breach.

The list of possible sources of SCS breaches is current and rather exhaustive as it is based on a comprehensive review of the academic and practitioner literature. This thesis acknowledges however that the number of SCS breaches may increase in the future. Therefore, the definition is subject to refinements. Nevertheless Wacker (2004) and several other scholars (e.g., Hunt, 1991) suggest that definitions need to be improved as time passes by. In this sense, the proposed definition is advantageous because it can be easily expanded via adding new sources of SCS breaches.

2.2.2.5 Supply Chain Security Management

Beyond defining SCS, it is also critical that I define supply chain security management (SCSM). With SCS being defined as the outcome of security related activities, this thesis further defines SCSM as the collection of mechanisms organizations deploy to avert, cope, react to, and restore from breaches. The literature review has illustrated that the mechanisms deployed to improve supply chain security span the spectrum of O&SCM subareas—spanning from inventory management to customer relationships, from shipment management to organizational culture. Table 4 summarizes these security efforts that have been explored in the supply chain security literature.

Table 4. Scope of SCSM

Study	Cargo, Terminal, & Port Security	Crisis Mgmt & Disaster Recovery	Customer Relationship Mgmt	Freight/Logistics Security & Carrier mgmt	Information Security	Inventory Security & Anti-theft	Process Technology	Mgmt Support/Education	Organizational culture & Security Awareness	Personal Security & Human Resource Mgmt	Physical Security	Public-private collaboration	Quality Control	Resiliency Development	Security Planning	Supplier Relationship	Third-party Security Service
Atwater et al. (2010)																	
Autry & Bobbitt (2008)					√		√		√						√	√	
Bakshi & Gans (2010)	√			√													
Bakshi et al. (2011)	√			√													
Chao & Lin (2009)				√													√
Closs & McGarrell (2004)	√	√	√	√	√	√		√		√	√		√			√	
Closs et al. (2008)							√					√					
Ekwall (2009)	√					√											
Lee & Whang (2005)												√	√				
Lee & Wolfe (2003)													√				
Martens et al. (2011)															√		
Marucheck et al. (2011)												√				√	
Peleg-Gillai et al. (2006)			√	√		√					√		√				
Prokop (2004)				√													
Reade (2009)										√							
Rice & Caniato (2003)	√			√	√						√			√			
Rice & Spayd (2005)	√	√	√	√	√	√		√	√	√	√		√	√	√	√	
Russell & Saldanha (2003)				√	√							√		√		√	
Sarathy (2006)												√				√	
Sheffi (2001)												√				√	
Sheu et al. (2006)				√								√				√	

Table 4. continued

Speier et al. (2011)								√									
Thibault et al. (2006)				√								√					
Voss et al. (2009a)																√	
Voss et al. (2009b)		√						√								√	
Whipple et al. (2009)								√								√	
Williams et al. (2009a)												√					
Williams et al. (2009b)									√								

Given the large scope of SCSM mechanisms, the definitions of SCS and SCSM alone may not be sufficient to help managers effectively organize their SCS related activities and implement appropriate SCS programs. For instance, the literature, industry reports, and professional standards (e.g., ISO 28000) have suggested a rather large number of SCSM mechanisms. These mechanisms sometimes require different levels of resources and varying managerial attention. For instance, additional security inspections could be easily achieved by adding technological devices and security staff, but the development of a security-oriented culture may demand intimate involvement from top management's years of nurturing. As a result, managers may still have trouble about how to move forward with a comprehensive SCS plan given that clear definitions of SCS and SCSM are in place. A taxonomy of SCSM mechanisms can be instrumental in this regard: a taxonomy helps organize SCSM mechanisms into different classes such that managers may have a clear focus (e.g., implement one class of practices at a time) when it comes to SCS. A taxonomy would also benefit the academic community because

it allows for tests and comparisons of the effects of different classes of SCSM mechanism. Hence, I next propose an approach to develop a taxonomy of SCSM mechanisms. The fundamental rationale of this taxonomy lies in the similarities between a SCSM system and a human immune system. I start with a brief introduction of the human immune system.

2.3 Linking the SCSM System to the Human Immune System: A Taxonomy

This section provides a succinct account of the human immune system and its responses to infection caused by pathogens, bacteria, fungi, and other sources. The purpose of this section is to draw parallels between the human immune system and the SCSM system, and thus justify the use of the human immune system as a metaphor for the SCSM system. The review is by no means exhaustive. For more details about the human immune system, I refer the readers to Kaufmann, Medzhitov, and Gordon (2004), Parham (2005), Playfair and Bancroft (2004), and Segel and Cohen (2001).

2.3.1 The Basics of the Human Immune System

Immunology studies the physiological mechanisms that the human body uses to defend itself from invasion by other organisms. The immune system protects the body from threats (posed by, for example, pathogens) in a fashion that minimizes harm to the body and ensures its continued functioning. The origins of immunology studies reside in the practice of medicine and in historical observations that people who have survived the ravages of epidemic disease had become immune to infection. The human immune

system includes the innate immune system (part of the immune system which people are born with; it does not adapt to specific pathogens) and the adaptive immune system (part of the immune system that "learns" or adapts to recognize specific kinds of pathogens, and retains a "memory" of them to speed up future responses). The immune system is crucial to human survival. In the absence of a working immune system, even a grain of dust in the air can prove fatal.

The human immune system and the SCSM system are alike. First of all, both systems are designed to secure the wellbeing of the entity that owns the system. The immune system defends the body from invasions by organisms. The SCSM system defends the supply chain and its operations from SCS breaches. Second, both systems are complex and display a multi-layered architecture. For instance, the immune system has multiple layers of keratinized cells, with defenses at many levels. The SCSM system holds a clear hierarchy where at each level (e.g., individual, team, firm, or chain level) there can be different responses to SCS breaches. Third, the two systems need to be tolerant. The immune system has a mechanism to tolerate itself (i.e., does not attack self—elements of the body). The SCSM system, while improving security, has to give considerations to efficiency such that SCSM mechanisms would not impede normal operations. Fourth, malfunctions of both systems can result in devastating consequences. A failure of the immune system can result in serious health problems and even death. Similarly if the SCSM system fails to respond to SCS breaches, severe operational and economic losses may ensue. Table 5 summarizes these similarities along with some other parallels between the human immune system and the SCSM system.

Table 5. Similarities between human immune system and SCSM system

Similarities	Human immune system	SCSM system
Purpose	Defends the body from an invasion by other organisms.	Defends the supply chain from disruptions caused by SCS breaches.
Complexity	The human immune system discriminates *self* (elements of the body) against *non-self* (foreign elements). Because there are so many patterns of these elements, the immune system has to distinguish a tremendous amount of patterns in non-self (on the order of 10^{16}) to self patterns (on the order of 10^{6}).	Firms sometimes have limited understanding of their own operations, let alone their supply chain. One firm usually serves multiple customers and connects with a huge number of suppliers. For example, HEB (the 7th largest grocery store chain in the U.S.) had more than 6,000 first-tier suppliers in 2012.
Multi-layered	The immune system has a multi-layered architecture, with defenses at many levels.	Firms have a multi-layered architecture (i.e., individual, team, firm, or even supply chain level). Actions can be undertaken at each level.
Tolerance	The immune system has a mechanism to tolerate itself (i.e., does not attack self).	Firms develop mechanisms such that SCSM mechanisms would not hurt the efficiency of operations.
Severity	Deficiencies of immune system can cause serious health problems and even death.	SCS breaches can result in severe economic and operational losses. Some breaches may result in catastrophic failure.
Learning & Memory	The immune system can learn the structures of pathogens, and remember those structures, so that future responses to pathogens can be more efficient.	Firms learn from previous experiences. They document how SCS breaches are detected and resolved such that they can react to similar breaches more effectively in the future.
Swiftness	The immune system must eliminate pathogens as quickly as possible so that the pathogens will not be able to replicate themselves and cause harm. Responses to new pathogens are slow, but to previous ones are fast.	Firms have to resolve SCS breaches as soon as possible to ensure the business continuity and minimize potential economic losses. Responses to new challenges are slow, but to old ones are swift.
"Intra-" issues	Some pathogens live inside host cells and are not visible to white blood cells. The cells can collect fragments of proteins contained within the cell and transport them to the surface so that they are visible to the rest of the body.	Firms promote management mechanisms such that "hidden", internal security gaps such as employee sabotage can be prevented.

In addition, the two systems are also akin to each other in terms of how they operate.

2.3.1.1 Prevention

First, the immune system is tailored to prevent invasion by foreign microorganisms. It generates a hostile environment, both physically and chemically, to deny access to most foreign microorganisms. For example, the skin can block most pathogens. If the pathogens break through the surface of the skin, layers of keratinized

cells under the surface of the skin form a tough impenetrable barrier of epithelium. In addition, physiological conditions, such as temperature, make the bodily environment notably hostile for "intruders." These defensive actions are preventive in nature. The human immune system builds obstacles to prevent entry of outside microorganisms and thus inhibits bodily damage. Likewise, the SCSM system includes a number of preventive SCSM mechanisms to protect the supply chain. Firms hire guards and build fences around the facilities. They do background checks before hiring employees to assure that potential security glitches are minimized from the very beginning. They develop and publicize deterrence mechanisms whereby employees, supply chain partners, and the public at large may consider before they attempt to compromise the security of a supply chain system. In a nutshell, firms equip themselves with various preventive mechanisms in order to avert SCS breaches from emerging.

2.3.1.2 Detection

Second, the immune system actively detects "intruders" when toxic substances or pathogens evade the first layer of protection (i.e., prevention). The detection process is usually described as that of distinguishing "self" (elements of the body) from "nonself" (foreign microorganisms such as pathogens). Both the innate and adaptive immune systems can detect foreign microorganisms. The innate immune system consists of primarily a chemical response system called complement, and a phagocytic system involving roaming scavenger cells such as macrophages and phagocytes. These complement molecules and scavenger cells detect extracellular molecules and materials,

and thereby provide a quick response to infections: keep early infection in check. The adaptive immune system mainly consists of certain types of white blood cells (i.e., lymphocytes) which circulate around the body. A lymphocyte has on the order of 105 receptors on its surface, which allow it to detect pathogens. A receptor can bind to pathogens whose epitope (which are locations on the surface of a pathogen) structures are complementary to the structure of the receptor. When the affinity (the strength of the bond between a receptor and an epitope) exceeds some threshold, a lymphocyte will be activated for further reaction (e.g., pathogen elimination). Similarly, the SCSM system must have detection mechanisms that can locate potential and existing SCS breaches, especially those intentionally conducted and carefully executed by, for example, terrorists. Firms may install surveillance equipment (e.g., cameras) at critical locations (e.g., warehouses) to detect illicit activities. They can utilize technologies to track the movement of products and materials. They can also establish a SCS review system such that they can regularly scrutinize the whole supply chain and subsequently detect anomalies. In some cases, firms even develop and cultivate a security-oriented organizational culture whereby employees can treat security as one of the top priorities and proactively detect supply chain security glitches.

2.3.1.3 Reaction

Third, once the invading pathogens, bacteria, and fungi are detected, the human immune system begins to react. For example, complement molecules of the innate immune system can help eliminate bacteria through lysis (the process whereby the

complement ruptures the bacterial membrane, resulting in the destruction of the bacterium) or opsonization (refers to the coating of bacteria with complement, enabling the bacteria to be detected by other cells such as macrophages). Macrophages also have receptors for certain kinds of bacteria and thus they detect and engulf those bacteria. The response of the adaptive system can be induced when the immune system detects a kind of pathogen it never encountered in the past. Once the adaptive immune system has identified an invader, the lymphocytes generate specific responses that are tailored to maximally eliminate the specific pathogens or pathogen infected cells. Specifically, B cells (one type of lymphocyte) respond to pathogens by producing large quantities of antibodies which then neutralize foreign objects. T cells (another type of lymphocyte, including helper T cells and cytotoxic T cells), on the other hand, produce (1) cytokines that direct the immune responses and (2) toxic granules that contain powerful enzymes which induce the death of pathogen infected cells. The innate immune responses are generally faster than adaptive immune responses as the adaptive immune system takes time to recognize "intruders" and organize defense. In the SCSM system, the reaction mechanism will be activated once SCS breaches are detected. Responses to some SCS breaches can be immediate while others may be slow. Responses to "typical" security challenges, such as the detection of illicit material loaded in a cargo container, are generally fast because there are well established procedures that handle cargo inspections. The reaction process is alike to the responses of the innate immune system which responds to pathogens it has seen before. Firms usually hold the cargo and conduct further inspection before releasing the cargo to a proven constituent. Responses

to “atypical” security challenges are, however, complicated. The reaction process to these problems is akin to the reaction of the adaptive immune system. Because these challenges are usually new and atypical to organizations, firms may lack experience and consequently need time to develop an effective response to these challenges. Nevertheless, firms document these SCS breaches such that future responses to similar breaches can be quite fast and effective.

2.3.1.4 Restoration

Lastly, the immune system promotes the restoration of the human body after infections have settled in the body. While detecting and destroying pathogens, components of both the innate and adaptive immune systems also assist other cells to recover from pathogen attacks. For example, the fluid layer of the immune system which contains glycoproteins, proteoglycans, and enzymes can help the internal tissues to recover. One of the functions of cytokines (signal molecules that transmit information between cells; also known as “hormones” of the immune system) is to stimulate the growth of surrounding cells when necessary. Essentially, the immune system responses to foreign microorganisms are developed to restore the normal condition of the human physiological environment and ensure the continued functioning of the human body. Likewise the SCSM system has restoration mechanisms if SCS breaches do cause damage. A typical restoration mechanism is the so called disaster recovery plan which has been popularized in the last decade. For example, due to the terrorist attacks on 9/11, 2001, the US government temporally closed the US-Canada border. Consequently, big

auto makers such as GM and Ford had to shut down some of their assembly lines due to material shortages. Nevertheless, their disaster recovery plans allowed them to quickly restore normal operations: Ford utilized air-freight to replenish inventories. GM, on other hand, shifted production from its Canadian plants to U.S. plants.

Overall, both systems have to prevent, detect, and react to threats they face and help restore the functions to their original states. Yet, these parallels only partly illustrate the similarities between the two systems.

2.3.2 Advanced Similarities between Human Immune System and SCSM System

The human immune system and the SCSM system also share some advanced attributes. For example, both systems are not perfect and they need to evolve (adapt and learn) in order to keep functioning effectively. In addition, both systems do not simply respond to all threats but tend to be more attentive to those threats that can actually cause damage. These advanced similarities are summarized in table 6 and discussed below.

Table 6. Advanced similarities between human immune system and SCSM system

Similarities	**Human immune system**	**SCSM system**
Evolution	The human immune system evolves to generate a new lymphocyte repertoire in order to combat the large number of bacteria	The SCSM system evolves to handle new SCS breaches.
Selective Responses	The human immune system only responds to *harmful* non-self.	The SCSM system tends to respond to SCS breaches that can cause substantive disruptions.
Latent Breaches	Opportunistic pathogens hidden in the human body can cause serious health problems when the body is compromised.	Many SCS breaches are latent and only present themselves under certain circumstances.

2.3.2.1 Evolution

All humans are susceptible to a variety of infectious diseases, especially when young. This is because the immune system takes time to build its strongest responses to invading organisms. Even the strongest immune system cannot guarantee that all invading organisms can be effectively eliminated. Likewise, a supply chain is also always "vulnerable" even when its SCSM system is functioning. Firms generally face new SCS challenges whenever they change their supply chain configurations due to business needs. For example, adding or eliminating a warehouse can result in significant rerouting of shipments. The logistics managers have to consider if the new routes will pass through regions where security is a big threat (e.g., northern Mexico) and consequently prepare to face new SCS challenges. To solve this problem, both systems have to evolve.

The immune system is a highly evolved biological system. Because detection is carried out by binding with foreign molecules, the immune system must have a sufficiently large number of diverse lymphocyte receptors to ensure that at least some lymphocytes bind to any given pathogen. Generating a sufficiently diverse repertoire is however a problem. Tonegawa (1983) has estimated that there are at most 10^8 different varieties of lymphocyte receptors. Yet there can be over 10^{16} different pathogen epitopes. There will be insufficient repertoire diversity to bind to every single possible pathogen. This problem is exacerbated as pathogens are likely to evolve to evade detection from the existing repertoire. For example, there are many cases where pathogens have developed molecules that fool the immune system by binding to

endogenous receptors (Matzinger, 1998). In an attempt to address this problem, the immune system conducts continual turnover of lymphocytes: each day approximately 10^7 new lymphocytes are generated (Osmond, 1993). It takes only 10 days to generate a completely new lymphocyte repertoire. Over time, this turnover of lymphocytes along with immune memory enhances the protection provided by the human immune system.

The SCSM system adapts to changing SCS threats through dynamic protection. Firms usually conduct regular training in order to keep up with the state-of-the-art SCS techniques and knowledge. They also learn from other firms located in the same industry via continuous benchmarking. Professional organizations, such as ISO, and many security service providers, launch guidelines and reports of best SCSM mechanisms. Firms can actively update their SCSM knowledge and skills such that they may effectively respond to SCS breaches they've never met before. Moreover, firms can also document historical security events and maintain a database for learning purposes. These actions allow them to initiate fast responses to SCS breaches if similar breaches have occurred before. Firms are able to "refresh" the SCSM system periodically and thus provide dynamic protection for the supply chain.

2.3.2.2 Selective Responses

The human immune system also responds to threats selectively. In order to eliminate foreign organisms, the immune system must be able to distinguish between foreign molecules (or antigens) and the molecules that constitute self. In immunology, this capability is described through the classic expanded self-nonself (SNS) model

(Janeway, 1989, 1992). The Expanded-SNS model assumes that the immune system is turned outward, responding to exogenous signals that represent one or another form of non-self. However, evidence has been accumulating that many foreign microorganisms are not harmful. The immunology response to eliminate them may actually cause damage to the body (Segel and Cohen, 2001). Under such conditions, it would be healthier *not* to respond. Thereby, it would be more accurate to say that the immune system is actually distinguishing between harmful non-self and everything else. Consequently, a complementary and competing model—the Danger model—was developed. In contrast to the expanded SNS model, the Danger model holds that the immune system is governed from within, responding to endogenous signals that originate from stressed or injured cells (Matzinger, 1994, 1998). In other words, the Danger model assumes that what really matters, from an evolutionary point of view, is whether the entity causes damage or not.

In some cases, the Danger model can effectively explain certain phenomena that the Expanded-SNS model cannot. For example, the Expanded-SNS model predicts that all foreign organisms will be eliminated by the human immune system. In reality, for example, transplants are usually rejected (by the human immune system) while tumors are not. A skin graft administered to a burn patient, for example, is an attempt to help, not cause injury. However, the injury is unavoidable. The process of transplanting a tissue involves surgical procedures that result in tissue damage and ischemic cell death and such damage will generate alarm signals that activate immune responses. Tumors,

on the other hand, do not cause damage (at least in the short term), and thus are tolerated by the body.

This logic also applies in the SCSM arena. The general purpose of SCSM mechanisms is to deny all kinds of SCS breaches. But some breaches, while hurtful, may not really affect firm performance—materially cause "damage". For example, firms purchase insurance policies to protect their assets. When damaged assets are insured, firms barely suffer losses. Launching SCS initiatives to respond to these breaches may actually cost them more. Consequently, it is more efficient *not* to respond. This logic is further supported when I interviewed a supply chain manager from a Fortune 500 electronics manufacturer: "We know that some of our trucks were stolen in Mexico. But the insurance covers these losses. As long as the number of lost trucks is below a certain number, we do nothing and let it go." In other words, the SCSM system (in many cases) is designed to respond to only threats that can cause substantive damage.

2.3.2.3 Sleeping and Latent Breaches

While the human immune system proactively detects threats, certain types of pathogens can actively avoid detection and elimination because they are conditionally harmless. For example, some pathogens do not harm its host (e.g., the human body) under normal conditions but can cause illness when the host's resistance is low. These pathogens are called *opportunistic pathogens* because a compromised human immune system presents "opportunities" for these pathogens to infect. Examples of opportunistic pathogens include candida albicans, staphylococcus aureus, and pseudomonas

aeruginosa. They are analogous to "sleeping bombs." If a healthy host becomes sick, these opportunistic pathogens can be triggered and worsen the health problem the host faces. In a similar vein, some SCSM breaches are "sleeping" and only present themselves under certain circumstances. For example, a theft of a truckload of raw material may cause temporal disruption of material supplies. When firms operate under normal conditions, they usually have inventory buffers and thus they may not even acknowledge the seriousness of these temporal SCS breaches due to the minor impact these breaches have. When the inventory level is low or the manufacturing system is lumpish (i.e., low flexibility), however, these SCS breaches may cause devastating results, leading to shortages of major products during their growth windows (Norrman and Jansson, 2004).

Some other types of pathogens, on the other hand, are able to actively hide themselves. These pathogens are intracellular pathogens which live *inside* the host cells. They are not "visible" to lymphocyte B cells because all that the B cells can observe is the outside of the host cell. The intracellular pathogens force the human immune system to look inside host cells through MHC molecules (which function like transporters that can carry the fragments of viral proteins to the cell surface). Likewise, the SCSM system also faces several hidden SCS breaches and needs to look inside. For example, most thieves are either employees or conspire with employees (Walsh, 2000). Those employees are usually familiar with their firms' security systems thereby may be able to cover their crimes effectively. In short, both the human immune system and the SCSM

system face latent threats which are difficult to detect and identify. These threats may be harmless in normal conditions but can potentially generate serious problems.

Admittedly, I cannot illustrate all aspects of the two systems in detail. The human immune system is vastly more complex than portrayed so far. So is the SCSM system. Nevertheless their similarities are apparent. Both systems have the same goal and share the same responding and operating principles. Therefore, it is safe to bring the classification of immunological responses (Kaufmann, Medzhitov, and Gordon, 2004; Parham, 2005; Playfair and Bancroft, 2004) to the purview of SCSM. This study thereby proposes a taxonomy of SCSM mechanisms that apportions these mechanisms into four classes: prevention, detection, reaction, and restoration (Figure 3).

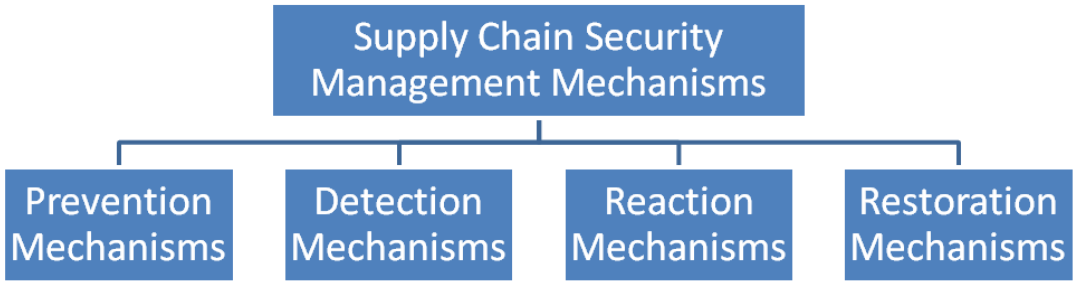

Figure 3. A taxonomy of SCSM mechanisms

One caveat worth noting is that these four classes of SCSM mechanism are not independent. Rather, they are highly intertwined and function simultaneously. For example, while *detecting* and *eliminating (i.e., reacting)* foreign microorganisms, the innate immune system also produces certain proteins, called interferons, to inhibit viral

replication, which is a typical *preventive* action. Likewise, in the SCSM system, the employee who *detects* a SCS breach could also be the first one who *reacts* to that breach. The taxonomy proposed here is one of the possible ways to organize SCSM mechanisms. Nevertheless, this four-class taxonomy appears to be a valid and efficient approach to categorize the scattered SCSM mechanisms. It allows the thesis to develop a set of testable hypotheses that address the rest of the research questions which may eventually advance our understanding and help managers resolve SCS breaches.

2.4 Four Cases Studies

In order to further justify the definition of SCS and the taxonomy of SCSM mechanisms, four in-depth case studies were undertaken. The four case studies allowed me to learn, from a practitioner's perspective, what SCS meant and whether or not the proposed taxonomy was a valid representation. These case studies also enabled me to build a better understanding of what SCSM mechanisms firms implement to prevent (detect, react to, or restore from) SCS breaches and what performance dimensions firms cared about most. The findings of the case studies were used to help develop testable hypotheses in the next chapter.

2.4.1 Sampling, Data Collection, and Analysis

This dissertation adopted a grounded theory building approach (Strauss and Corbin, 1990). Specifically, the principles of theory building based on case studies were adopted (Eisenhardt, 1989; McCutcheon and Meridith, 1993; Yin, 1994). Case studies

are appropriate as supply chain security is a relatively new research area (McCutcheon and Meridith, 1993; Yin, 1994).

I took a theoretical sampling approach to identify companies for this study. The initial list included companies from four different industries: Food and Beverage, IT & Electronics, Manufacturing, and Retailing. Food and Beverage producers may be quite sensitive to SCS breaches because their products can directly affect the public health. The retailing industry is also of interest because firms in this industry directly interact with consumers. IT & Electronics companies signify the high-tech industry while manufacturing companies represent firms in the traditional manufacturing sectors. Such selection of firms was meant to go beyond the analysis of "low hanging fruit" (i.e., something that everyone does; Walley and Whiehead, 1994) and acknowledge that companies in certain industries are more vulnerable to different SCS breaches than others and, therefore, those companies may have implemented SCSM mechanisms at greater levels. In addition, selecting firms across various industries helped me to create a more representative sample from which I can generalize findings. The literature also suggests that firm size may have rather strong effects on organizational behaviors (e.g., Pagell et al., 2004). Therefore, I purposefully selected companies with various sizes. The sample includes large multinational companies with global supply chains and small/middle size local companies. This mix allowed me to examine the research questions from a broad spectrum of settings.

Ten companies were initially invited to participate in this study. Not all of them agreed to participate in part because security matters are considered confidential and

their policies do not allow employees to divulge any useful information. Nevertheless, I secured one company from each of the four industries to participate in the study. Data from the four companies were eventually collected and analyzed. One additional company was willing to provide us access and in fact we conducted interviews with several executives. However, that company is a logistics security service provider and does not do any production itself. Therefore, I opted not to include the findings in this study as the company may not be comparable to the rest of the participants.

Eisenhardt (1989) suggested that neither too few nor too many cases were conducive to good qualitative research. A number of four to ten companies is generally appropriate. A sample of four companies allows me to generalize the findings while keeping the data analysis cognitively manageable. Table 7 provides the profiles of participating companies. At the request of the participants, I used fictitious names to assure anonymity. Data were collected during 2011 and 2013.

Table 7. Sampled companies

Company	Industry	Interviewee	Size	Ownership	Major Business
Master Baker	Food & Beverage	General manager & quality assurance manager	Small	Private	Produces bakery items for over 2,500 fast food outlets
Seal Maker	Manufacturing	Plant manager	Medium	Public	Manufactures remote seals for the oil and gas industry
Electronics Savvy	IT & Electronics	Global supply chain security manager	Very Large	Public	Manufactures electronic products for the consumer market
Retail Guru	Retailing	A group of eight managers/directors	Large	Private	Sells national brand and private label products to consumers

To answer the research questions, a semi-structured interview protocol was developed (see Appendix A). The protocol called for multiple respondents who had responsibility of SCS from multiple functional areas. Therefore, whenever possible, a group of managers were interviewed. Interviewing multiple respondents allowed me to triangulate the data. In general, each interview lasted about 2-3 hours. To understand the role of institutional pressures to adopt SCSM mechanisms, I examined relevant legislation regarding SCS for each industry I investigated. I also gathered information about the history as well as the evolution of SCSM in these companies. The information I collected shed light on managerial motives and company strategy. Interviewees were asked, whenever possible, to provide real examples regarding SCSM in their companies.

Data were collected by at least two researchers at all four companies (two at Seal Maker and Electronics Savvy; three at Master Baker and Retail Guru). Except for the Master Baker, the interviews were recorded and later transcribed. While Master Baker's policy did not all me to record the interviews, detailed notes were taken by three researchers. I also collected archival data from company websites and reports published by government agencies such as the Food and Drug Administration. Data collection did not stop until I reached a saturation point where additional data would not help answer the research questions (Glaser and Strauss, 1967; Eisenhardt, 1989).

I first performed within-case analysis following the procedures advocated by Miles and Huberman (1984). The coding was conducted iteratively. First, all interviewers individually coded the data. We then compared the coded data to assure consistency. Disagreements were identified. Discussions followed in order to resolve

these disagreements. This process led to clarification of the constructs and assured that the inter-rater reliability between the two coders was 100%. The within-case analysis allowed me to gain a broad understanding of the operations of each company's supply chain. I then determined how each company generates revenue and the impact of SCS breaches on their operational/financial performance. I also explored how companies incorporate SCSM mechanisms into their decision-making through within-case analysis. Interviewees were probed specifically about which performance dimensions their company cared about most, when SCS breaches could significantly affect their company's performance, and what benefits their company has experienced by implementing SCSM mechanisms. I further asked managers how they managed trade-offs to make decisions. Analysis of multiple examples provided by managers shed light on decision patterns within each firm. Finally, cross-case analysis was conducted to identify common themes as to how firms handle SCS breaches, evaluate performance, and balance the potentially competing needs to be profitable and secure. The findings are presented in the next section.

2.4.2 Findings

2.4.2.1 The Definition of SCS

Three out of four companies (Seal Maker, Electronics Savvy, and Retail Guru) explicitly state that supply chain security and supply chain safety are different concepts. For them, supply chain safety mainly refers to accidents that are related to Occupational Safety and Health Administration (OSHA) recordables. The safety issue is narrowly

defined as production safety and prevention of injuries. Safety management is primarily about activities which can avert accidents that are proven detrimental to employee health. The fourth company, Master Baker, considers that food security and food safety are highly intertwined with each other. The managers expressed that they implemented practices to improve both food security and food safety. Nonetheless, all managers in my sample share the opinion that the concept of supply chain security is more complicated than supply chain safety.

The Electronics Savvy global supply chain security manager stated that: "in our industry, company from company is different. For some competitors security is nothing but physical security. At Electronics Savvy, we have a chief security officer … within his chief security officer's responsibilities is physical security, IT security, executive protection, and federal security. Here at Electronics Savvy we have to exhibit compliance with all responsibilities. We do the physical aspect of it, which is buildings, processes, and people. The federal security crosses lots of the assurances, quality assurance, the contamination, and our government customer's [requirement of assurance] because we are providing them pretty sophisticated machineries for their, you know, processes. When XXX (the chief security officer) comes here, because he comes from very IT savvy background, we have this IT security…" At Retail Guru, the procurement director of own brand products stated that "in our cases all of the world is adulterated. There is lots of food adulteration, economic adulteration…at Retail Guru, we have food, we have consumer products, that makes it more even challenging to be able to manage both (i.e., food and consumer products) to meet the [legislative]

regulations… we also have thefts and counterfeit products…" Indeed, all managers in the sample concur that SCS is not something that can be easily described.

After soliciting the managers' description of SCS, I also provided my definition and probed their opinions about it. I find that managers acknowledge that they do face various SCS breaches from different sources. There is no single "correct path" for them to deal with all SCS breaches. Instead of extracting common attributes among a variety of SCS breaches in order to decipher what SCS is, borrowing the concept of "zero defects" from Total Quality Management and defining SCS as "zero defense breaches" is efficient and valid to them.

As far as the sources of SCS breaches are concerned, I find that some sources are common to companies irrespective of their industry membership (see table 8). Theft and counterfeit product are common SCS challenges for all companies in the sample. For example, Electronics Savvy had three large cargo thefts recorded in the last 12 months. Master Baker and Seal Maker both experienced employee theft. Retail Master stated that theft was one of the most important reasons of inventory write-off. On the other hand, companies in the sample also experienced unique SCS challenges. For instance, Retail Guru reported that they received adulterated tomato sauce in the past. Investigation of that problem revealed that it was caused by a supplier's double sourcing activity. Seal Maker stated that the company had confidential data stolen in their Beijing branch. Seal Maker also indicated that the company experienced employee sabotage in the past. Companies in the sample never experienced smuggling or terrorist attack problems. But all the managers agree that the two are potential sources of SCS breaches. Three

companies explained that they never encountered a smuggling problem partly because their supply contracts stipulated controls over smuggling. The fourth company, Master Baker, purchased raw materials mainly from local suppliers.

Overall, the analysis demonstrates that the definition of SCS I proposed is valid to practitioners. The sources of SCS breaches are rather comprehensive. All potential sources managers in my sample experienced or they could think of are included in the list of sources I provided.

Table 8. SCS breaches encountered by each company

Company	Theft	Adulteration	Smuggling	Counterfeit products	Sabotage	Terrorist attacks	Illicit data acquisition
Master Baker	√	√	N/A	√	N/A	N/A	N/A
Seal Maker	√	N/A	N/A	√	√	N/A	√
Electronics	√	N/A	N/A	√	N/A	N/A	N/A
Savvy Retailing Guru	√	√	N/A	√	N/A	N/A	N/A

2.4.2.2 The Institutional Antecedents of SCSM Mechanisms

Managers in the sample share the sentiment that their companies have to deal with institutional pressures as it relates to supply chain security. Within-case analysis suggests that an individual firm may not experience all five institutional pressures simultaneously. Cross-case analysis, on the other hand, demonstrates that each institutional pressure is present in at least one of the four cases. The five institutional pressures appear to capture a board spectrum of factors that motivate companies to adopt/implement SCSM mechanisms.

Master Baker

Master Baker states that customer pressure is the most impactful institutional pressure to them. Over 90% of its business comes from a single customer which is a large fast food chain. That customer requires Master Baker to implement a number of SCS related practices in order to protect the entire chain. For example, the Master Baker had to implement *Global Food Security Initiatives* developed by the specific customer by the end of 2012 otherwise the customer would disrupt the relationship which was built for several years. As the general manager of Master Baker put it, "we do whatever they ask us to do." Nevertheless, customer pressure is not the only institutional pressure they experience. The quality assurance manager from Master Baker stated that "Now, almost all firms [in my industry] do pretty much the same thing [as it relates to SCS] because of competition." Master Baker continuously monitors its competitors and implements what the industry labels as "best practices". Legislative requirements issued by government authorities, such as the Food and Drug Administration (FDA) or the U.S. Department of Agriculture (USDA), are also adhered to closely at Master Baker. As the same quality assurance manager stated, "technically, USDA can send an inspector to our facility any time during operations."

Normative pressure appears to be trivial for Master Baker. Master Baker does implement SCSM standards/programs. They developed and implemented a *Food Defense Program* which is an initiative that coordinates all safety and security related activities within the organization. However, this program is not developed based on industry or professional norms but rather is adapted from the major customer's *supplier*

requirements. Master Baker is also concerned about financial/operational performance as it relates to SCS. Yet performance pressure is not a strong motivator for the company to implement SCSM mechanisms. The general manager agreed that SCSM mechanisms may help improve efficiency, but stated: "we usually adopt security related practices because XXX (the major customer) asks for it. We do it even when it will hurt our efficiency."

Seal Maker

Seal Maker faces little institutional pressure. The company was acquired by a large strategic business unit (SBU) of a Fortune 500 company in the early 1990s. Seal Maker used to be a major supplier of that SBU. After acquisition, Seal Maker switched from an external supplier to an internal supplier. All major customers of Seal Maker are 100% owned by the same SBU. While the company still sells products to trade customers, over 90% of its business comes from sister companies. Consequently, Seal Maker has very stable customer demand. The company does not experience strong peer pressure primarily because there is literally no competition at all. In-depth discussions further revealed that the company faces little competition in part because they are one of the two leading companies in that particular industry segment, and in part because a sizeable number of large firms produce remote seals in house, and, therefore, the market demand can only sustain a relatively small number of suppliers.

Customer pressure is relatively weak for Seal Maker. The impact from customers appears to be inconsequential because most customers are internal. The parent company

also coordinates the supply and demand between Seal Maker and its sister companies, which further weakens the customer's ability to impact Seal Maker. The manager at Seal Maker expresses no concern about performance outcomes as well. The parent company entitles Seal Maker to set prices for its products as long as these prices fall into a reasonable range. As mentioned before, there are only a small number of players in the remote seal production segment. Therefore, few norms exist. The only salient institutional pressure for Seal Maker is from government. Nevertheless, the parent company has a well-constructed compliance program and all Seal Maker needs to do is to fulfill those requirements listed in that program. In short, Seal Maker perceives little institutional pressure to improve SCS. This finding is consistent to another finding that the company implemented fewer SCSM mechanisms when compared with other companies in my sample, which will be discussed in section 2.4.2.3 and 2.4.2.4.

Electronics Savvy

Electronics Savvy is one of the largest consumer electronics manufacturers in the world. It produces a variety of consumer electronic devices with global presence. As an industry leader who explores new technologies and manufactures state-of-the-art devices, Electronics Savvy is quite cognizant of legislation regarding supply chain security. Electronics Savvy is one of the first companies who adopted the C-TPAT program when it was introduced in 2001 right after the 9/11 terrorist attacks. It is also among the first companies who earned a C-TPAT tier-3 certification (the highest level). The global SCS manager at Electronics Savvy explained that his company implemented

all necessary practices to assure every single governmental regulation regarding supply chain security was fulfilled.

Electronics Savvy perceives rather strong customer pressure. A large portion of Electronics Savvy's business is government (federal state). These customers require high levels of IT security because a sizable volume of privilege information is stored in their electronic devices. In order to enhance IT security, these customers pressure Electronics Savvy to manage its supply chain to avert potential SCS breaches such as "pre-installation" of phishing software or counterfeit parts. The company has been working closely with its customers to ensure SCS. The global SCS manager explicitly stated that the company had to do a good job in order to satisfy its customers.

While competition in the consumer electronics market is intense, Electronics Savvy surprisingly faces relatively little peer pressure as it relates to SCS. Detailed discussions with the global SCS manager from this company revealed that competition in the consumer electronics market is primarily driven by price and innovation. How peers revamp their SCS related operations is less impactful to the company. Electronics Savvy rarely implements SCSM mechanisms simply because its competitors have done so. As an industry leader, Electronics Savvy is not only a pioneer adopter of occupational standards but also a drafter of those standards. Owing to its active role in developing industry and professional norms, the company does not feel obligated to abide by normative pressure.

The global SCS manager at Electronics Savvy suggests that the company implements SCSM mechanisms in order to reduce losses. The company recorded three

cargo thefts in the last fiscal year. Due to the high average value of its products, any cargo theft can easily cost Electronics Savvy millions of dollars. In order to reduce theft, the company installed advanced tracking devices on its products during shipment. On top of reduction of losses, Electronics Savvy experienced several collateral benefits. For example, those advanced devices can tell exactly how many items in a container were touched by outsiders, if that container was stolen. Electronics Savvy has taken advantage of this technology and shipped a recovered container (about half of the items in that container were gone) to a customer to partly fulfill customer demand.

Retail Guru

Retail Guru is one of the top food/department store chains in the United States. The company has been in operation for more than 100 years. Besides selling national brand products, Retail Guru has more than ten manufacturing plants producing close to 15,000 own brand items. The company also has its own fleet, consisting of hundreds of tractors and trailers. Since a significant volume of business involves food and drugs, the company is very sensitive to SCS breaches. Retail Guru is also one of the earliest adopters of the C-TPAT programs. In 2005, the company earned C-TPAT tier-3 certification. It even has a designated C-TPAT compliance manager who specifically handles issues regarding the implementation of that program. The interviews with eight managers in the company indicate that, owing to its proactive strategy toward compliance, the company does not perceive government pressure as a headache as many other companies do.

Retail Guru's customers are final consumers. These consumers may directly affect Retail Guru's reputation by expressing their opinions through social media (e.g., posting reviews on Facebook about product quality) either in favor of or against the firm. Managers at Retail Guru care about their company's brand equity more than anything else. To them, the company earns its current reputation through more than 100 year's hard work. To protect their brand equity, they deployed very strict SCS standards throughout the supply chain, even when these standards may hurt the delivery performance. As the director of global sourcing stated, the company had delays in cargo shipments every month due to extensive security inspections.

Competition is rather intense in the retail industry because customers can easily find the same or almost identical products from competing retail chains. The profit margin could be as low as 1% and hovers around 2-3%. Owing to such thin margins, Retail Guru never treats supply chain security lightly. For example, if Retail Guru could successfully reduce losses caused by SCS security breaches (e.g., employee theft) by one cent for each dollar of sales, the company would have doubled its profit margin. To demonstrate their SCSM efforts, the sourcing director of own brand products shared with us a long list of detailed SCSM requirements demanded of their suppliers. He further explained that the company was willing to learn from outside sources to improve SCS. Best practices invented by competitors would be introduced to the company periodically. For example, Retail Guru developed an internal, web-based training system called "Retail Guru" University. Employees are required to take training on the system in order to keep their skills up-to-date. Such information suggests that Retail Guru is affected by

both performance pressure and peer pressure. Nevertheless, learning from peers is meant to improve performance at Retail Guru.

Managers at Retail Guru do not perceive norms as a pressure for them to implement SCSM mechanisms. Discussion among several Retail Guru managers demonstrates that because the company has been in operation for more than 100 years, it is well embedded in the environment and adopted various norms in the past. One intriguing finding related to its long history of operation is that the company cares about its reputation so seriously such that the company sometimes sacrifices its profit to enhance SCS. One example was provided by the director of global sourcing. A shipping container of Retail Guru's branded ketchup usually costs the company less than $5,000. It is not financially justified to install any form of security device to protect such products. However, the company employs advanced tracking devices on all shipments of such products simply because such items are vulnerable to a variety of SCS breaches which can be rather consequential to the brand equity of the firm. This finding indicates that Retail Guru believes SCS is critical to the company's sustainability, which is usually considered as a performance measure from a long term perspective.

2.4.2.3 The Taxonomy of SCSM Mechanisms

The managers from all four companies agree that a taxonomy is a novel tool to help manage SCS breaches and believe the taxonomy I proposed provides them with a new perspective to review their SCSM efforts. Having said that, managers in my sample rarely thought about which taxon a given SCSM mechanism should be attributed to.

Therefore, clarification questions were asked when discussing specific SCSM mechanisms in order to ensure that the researchers and the managers share the same opinion with respect to a given mechanism's ascription.

In addition, many SCSM mechanisms were embedded in higher level SCSM programs (e.g., the *Global Food Security Initiatives* at Master Baker) and managers tended to communicate their SCSM efforts through these programs rather than specific mechanisms. In order to uncover which SCSM mechanism was implemented at each firm and thus allow for cross-case analysis, I prepared a list of SCSM mechanisms extracted from the literature (Lee and Whang, 2005; Mena et al., 2009; Williams et al., 2009a), industry reports (Closs and McGarrell, 2004; Peleg-Gillai and Bhat, 2006; Rice and Spay, 2005), and professional certifications (e.g., ISO 2800; ISO 31000). Whenever I felt a mechanism listed was implemented by a firm but the manager(s) from that firm never mentioned it, I would point it out in order to attain clarification. Such list was deemed helpful. Typical responses after my question were: "Yes, we did it. It (the practice) is part of our XXX program/initiative." or "We did not do the same thing, but it is very similar to our XXX."

Table 9 summarizes the SCSM mechanisms the four companies have implemented organized by class. I find that neither do companies treat all SCSM mechanisms equally nor do those SCSM mechanisms contribute to performance equally. Each company has its own focus regarding the implementation of SCSM mechanisms. These SCSM mechanisms are discussed below.

Table 9. SCSM mechanisms implemented by the four companies

	Master Baker	Seal Maker	Electronics Savvy	Retail Guru
Prevention	Developed a proactive strategy Selected only pre-approved suppliers Secured containers at manufacturing area	Selected only pre-approved suppliers	Developed a proactive strategy Selected qualified suppliers Conducted background checks before hiring employees	Developed a proactive strategy Selected qualified suppliers Conducted background checks before hiring employees Developed supplier code of conduct with respect to SCS
Detection	Monitored loading/unloading process Conducted processes to notify supply chain partners in times of crisis	Notified supply chain partners about SCS breaches Developed internal quality management standards	Installed surveillance systems Notified supply chain partners about SCS breaches Used sophisticated detection technologies Conducted periodic assessment of suppliers	Monitored loading/unloading process Installed a surveillance system Monitored suppliers across tiers Notified supply chain partners about SCS breaches Synthesized information regarding SCS breaches Conducted periodic assessments of suppliers
Reaction	Cross-trained employees Established communication channels with suppliers	Maintained backup machines and inventories (primarily raw material)	Cross-trained employees Developed multiple supply sources Established communication channels with suppliers and 3rd party security service providers Designated a quick reaction force for SCS breaches Used interchangeable parts as a strategy to deal with SCS breaches Designed flexible contracts with suppliers	Cross-trained employees Developed multiple supply sources Specified reaction code when a SCS crisis emerges Established communication channels with suppliers and 3rd party security service providers Designated top manager(s) / a group of employees to manage SCS breaches Cultivated a culture that rewards SCSM efforts
Restoration	Maintained strategic inventory (primarily raw material) Learned from mistakes Developed a recovery plan for potential SCS breaches	[The parent company] developed a recovery plan for potential SCS breaches	Developed a recovery plan for potential SCS breaches Developed a business continuity plan Pre-arranged restoration processes Utilized alternative supply sources Used standard parts	Developed a recovery plan for potential SCS breaches Pre-arranged restoration processes Utilized alternative supply sources

Note: Information sources: interviews and archive data.

At Master Baker, the company has a very proactive strategy toward SCS breaches. The general manager at Master Baker possesses a rather strong perception that

"security (i.e., raw material/product protection) overrides quality (i.e., taste of the product)." He has been working with the company for 30 years and he claimed "we cannot afford security problems anymore." He led the implementation of the *Food Defense Program* initiative at Master Baker which coordinates almost all SCS related activities. Under this proactive strategy, Master Baker has deployed a very strict supplier selection system that allows them to select only qualified suppliers, which averts the company sourcing from unreliable material sources. Master Baker requires staff to have security codes in order to access its manufacturing/warehousing facilities. The company also has surveillance systems and actively monitors the entire manufacturing and warehousing area. Outsiders (e.g., representatives from suppliers) have to wear red hats such that they can be easily identified. In order to effectively react to SCS breaches, Master Baker cross-trains its employees so that they can operate different machines for different product lines. The company also established a communication system to ensure commands/instructions from the top are clear when a crisis emerges. Master Baker maintains a 3.5 million dollar strategic inventory of raw materials. It allows the company to restore operations on the aftermath of a SCS disruption. Learning from previous SCS breaches enhances the company's ability to reinstate operations as well.

Seal Maker considers material quality management the most critical component of their SCSM system. Defective raw material is the only reason that the company suffered from substantive losses in the last few years. While defective parts were not exclusively caused by SCS breaches such as counterfeit products, Seal Maker established very strict supplier selection criteria and performed material screening

processes to ensure all materials received were authentic. The company also installed redundant equipment as a mechanism to deal with supply chain disruptions caused by SCS breaches. Nevertheless, due to little perceived institutional pressure and few SCS breaches encountered in the past, Seal Maker has implemented a very limited set of SCSM mechanisms as compared to the other companies I studied.

Electronics Savvy is well-known in the industry owing to its very success on inventory management. However, this does not imply that the company is immune from losses caused by SCS breaches such as cargo theft. Electronics Savvy has a well-established surveillance system installed around its plants and warehouses. Advanced technologies, such as metal detectors, are also installed at entries and exits of manufacturing facilities. Tracking devices are also installed on all cargo shipments. Electronics Savvy is aiming to detect SCS breaches effectively but also to deter them.

In order to react to SCS breaches, communication is vital for Electronics Savvy. A SCS breach must be reported to a responsible regional SCS manager within an hour. That manager will then provide a brief report to the global security officer within four hours. After that, a final and formal report will be prepared by both the global SCS manager and other parties involved in that SCS breach. The final report must be submitted within 24 hours along with detailed damage estimation and activities undertaken to deal with the SCS breach. Such communication mechanism allows Electronics Savvy to swiftly respond to SCS breaches and mitigate potential losses. The company also develops multiple supply sources and uses interchangeable parts as a strategy to deal with SCS breaches. The flexible contracts between Electronics Savvy

and its suppliers ensure the company can reinstate operations quickly if a SCS breach emerges.

Retail Guru primarily sells food and drug store products. The company believes it is a big challenge to protect its supply chain from SCS breaches. Every day there is a recorded disruption somehow in their supply chain. All managers I interviewed stated that they needed to know more about their suppliers across tiers. The procurement director of own brand products stated that "we see the need to be able to know more about our supply chain, and much further down the supply chain than we have been before. Just a challenge of doing that with a hundred thousand products and thousands of suppliers." Their top leaders shared the same opinion and provided full support for their SCSM efforts. As one manager stated, "my boss is there from day one." All Retail Guru suppliers must develop their own product security plan utilizing the *FDA Food Security Preventive Measures Guidelines*. International suppliers must develop a global SCS plan utilizing the *U.S. Customs & Border Patrol Guidelines*. International suppliers must also participate in and collaborate with Retail Guru's C-TPAT compliance. Retail Guru has more than six thousand suppliers. Yet the company reviews every single supplier's product defense and facility security plan at least once a year. Even for suppliers who have worked with the company for decades, they still conduct the reviews and verify the integrity of their processes and products. When talking about their supplier management with respect to security, one manager stated "[our policy is to ensure] they (suppliers) do what they said they will do."

Retail Guru has a designated chief security officer and an emergency reaction team. The company also has a "war room" where pertinent people/parties can meet in response to a SCS breach. After each SCS breach, corrective action procedures are recorded and knowledge is preserved for the future. In-house training and online courses are offered to employees. Instead of using third party logistics service providers, the company also maintains its own fleet. Those endeavors help Retail Guru successfully respond to SCS breaches effectively.

The key and commonly shared tenets of SCSM mechanisms implemented by the companies are further extracted and presented in table 10. Because two SCSM mechanisms could be essentially referring to the same task but named differently by different companies (e.g., "we only use pre-approved suppliers" v.s. "we only use qualified suppliers"), I use general statements to describe those tenets. Such tenets allow me to select the most representative SCSM mechanisms for hypotheses testing in chapter IV.

Table 10. Key SCSM tenets by class

	Key SCSM tenets
Prevention	Develops a proactive strategy to deal with SCS breaches Holds suppliers accountable for SCS breaches Educates employees/suppliers about SCS breaches Selects only qualified suppliers Secures physical locations (e.g., manufacturing facilities and warehouses) Sets high priority for SCS
Detection	Monitors physical movement of raw materials and products Detects existing SCS breaches and near SCS breaches Synthesizes information regarding SCS breaches Monitors supply network instead of focusing only on first tier suppliers Conducts periodic reviews both internally and externally about SCS Notifies supply chain partners about SCS breaches
Reaction	Cross-trains employees Builds backup processes Designates a group of employees as the first respondents to SCS breaches Develops flexible contracts with suppliers Develops a clear chain of command Establishes effective communication channels with both suppliers and internal security staff Utilizes product design to react to SCS breaches
Restoration	Develops recovery plans Develops alternative material sources Maintains redundancy (e.g., strategic inventory of raw materials, machinery, etc.) Learns from mistakes

2.4.2.4 The Outcomes of SCSM Mechanisms

Overall, the managers I interviewed agree that their respective company benefits from SCSM mechanisms. However, the magnitude of benefit is hard to estimate as managers also agree that it is not easy to quantify losses that have been prevented. The global supply chain security manager at Electronics Savvy explicitly stated: “it is very hard to calculate the gains.” Sometimes the process of managing SCS breaches is like “peeling an onion”, in the process of addressing one SCS breach, additional, unexpected ones come up. Essentially, “what I do is to save money [from improved SCS] to re-spend them [for better SCS].” At Electronics Savvy, managers understand the importance of SCS but they expect that there is little consensus as to how the benefits

can be systematically estimated. Such an idea was embraced by managers from Retail Guru as well. Although Retail Guru records inventory shrinkage due to employee theft or cargo theft, these "hard" numbers shed little light on the costs associated with their SCSM inputs. The "net return" is unclear to the managers. One director put it, "We do not have 'soft' numbers to measure cost. How many hours I spent should be billed toward SCSM? I do lots of work and it [security management] is just part of my job."

The findings from the four cases suggest that companies only look at overall cost but do not have a well-established matrix to measure the value of SCSM mechanisms. It is surprising that managers in my sample concur that SCSM mechanisms may result in collateral benefits (e.g., better supply chain visibility), but none of them use these collateral benefits as a measure of SCSM success. Nonetheless, due to the limited understanding about the value of SCSM mechanisms, it is highly warranted to empirically examine the effects of SCSM mechanisms on various performance dimensions as this study does.

One intriguing finding is that, while managers agree each class of SCSM mechanisms can affect supply chain performance, they suggest that it is the synergy of the four classes of SCSM mechanisms that actually plays a pivotal role. Theoretically, the four classes of SCSM mechanisms may either enhance each other or sometimes substitute each other. On the one hand, improvement in one class may lead to improvement in another class. For example, high levels of detection ability provide more time for a company to effectively react to SCS breaches. On the other hand, excellence in one class reduces the need of excellence in other classes. For example, superior

prevention ability may avert potential SCS breaches and therefore companies may not have to invest heavily for the other three classes.

However, discussions with managers demonstrate that excellence in only one class of SCSM mechanisms is not sufficient to protect the supply chain. A real example shared by the Retail Guru's supply chain security manager perhaps can help us to better understand the "synergy" idea managers proposed. Retail Guru used to face frequent cargo theft attributed to a gang on the Texas/Mexico border area. At the beginning, Retail Guru focused on reaction and restoration when dealing with the thefts. The company's strategy aimed to reduce overall losses. However, the number of cargo thefts remained high. Having realized that, Retail Guru attempted to solve the problem by shifting its focus toward detection and prevention. They actively detected stolen products. Whenever they found suspect containers that may be used to carry stolen products, they called the police to investigate those containers. If the owner(s) of the containers could not show the receipt of purchase, then police would take possession of these products. In such cases, Retail Guru did not get its lost products back, but the gang did not gain anything either. By doing so, Retail Guru sent out the "*I am watching you*" message in order to deter the gang from stealing its cargo. After that, the gang became more careful and the number of cargo thefts went down dramatically. However, the remaining small number of thefts generated substantive losses to Retail Guru because the company was no longer well-prepared to deal with this type of SCS breach (as it shifted its focus to prevention and reaction). The lessons drove Retail Guru to rethink its SCSM strategy. They balanced their efforts and gave consideration to both prevention

and reaction. The new strategy was deemed successful as the company experienced fewer thefts after that and the overall losses went down significantly.

CHAPTER III

HYPOTHESES DEVELOPMENT

In the previous chapter, I reviewed the literature, defined SCS and SCSM, and categorized SCSM mechanisms into four classes in order to address the first two research questions. In this chapter, I develop a set of testable hypotheses that inform research questions 3-5. Specifically, I adopt an institutional perspective and the tenets of the human immunology research to explore the underpinning logic that explains the effects of institutional pressures on SCSM mechanisms and then SCSM mechanisms on supply chain performance respectively.

3.1 Institutional Theory

The institutional theory (DiMaggio and Powell, 1983; Scott and Meyer, 1983; Scott, 1987; Zucker 1987; Meyer and Rowan, 1977; Powell, 1991) has captured the attention of researchers and scholars across the social sciences. It has been employed to examine systems ranging from micro interpersonal relationships to macro societal frameworks.

> "It considers the processes by which structures, including schemas, rules, norms, and practices, become established as authoritative guidelines for social behaviors… It inquires into how these elements are created, diffused, adopted, and then adapted over time and space; and how they may fall into decline and disuse" (Scott, 2004, p. 460).

In contrast to traditional rational theories (e.g., economic theories), the institutional theory emphasizes social effects rather than just economic outcomes (Zukin and DiMaggio, 1990). Individuals and organizations are assumed to be recognition seeking, subject to social influences and relatively intractable creatures of habits and traditions (Scott, 2001; Zucker, 1987). Conformity to social expectations (dubbed as *legitimacy* by institutional theorists) contributes to firm success and survival because legitimate firms are expected to gain social acceptance, and thus reap societal resources (Baum and Oliver, 1991; Carroll and Hannan, 1989; DiMaggio and Powell, 1983; Oliver, 1991). Hence, in order to garner legitimacy, firms facing similar environmental effects are prone to operate in similar ways and adopt the same practices/strategies, demonstrating the attribute termed as *isomorphism* (DiMaggio and Powell, 1983).

Because recent articles have provided a comprehensive review of the institutional theory literature (see Heugens and Lander, 2009), the present dissertation only reviews papers that are pertinent to the proposed model. I focus on several classic studies which illustrate the mechanisms by which institutional theory can explain the adoption of certain strategies and practices (SCSM mechanisms in my case).

DiMaggio and Powell's (1983) seminal work and recent studies of the institutional theory (Heugens and Lander, 2009; Lounsbury, 2007) propose that four institutional isomorphism pressures explain why firms in the same industry would adopt the same/similar strategies and practices: coercive, mimetic, normative, and performance.

3.1.1 Coercive Pressure

The coercive institutional pressure is forceful in nature. It derives from powerful agencies that can exert pressure on their business partners or related parties. Such pressure may be felt as mandates, as drivers, as persuasions, or even as invitations to join in collusion (DiMaggio and Powell, 1983). For example, according to the Importer Security Filing (ISF) program (a.k.a., the 10+2 rule), importers and international carriers need to report trade data (10 files from the importer and 2 files from the carrier) to the Customs and Border Protection (CBP) for non-bulk cargo shipments arriving into the United States by vessel. The installation of the reporting system (or commercial ISF software) is then institutionalized as a mandatory industry standard. As long as a firm wants to legally operate in the market, it has to have the reporting system in hand. In other words, the existence of coercive pressure affects many aspects of an organization's behaviors such that certain strategies and practices would be adopted irrespective of their efficiency or financial implications. Indeed, the literature suggests that a complex system of laws has profoundly moved the coercive isomorphism forward: the effects of coercive pressure emanating from the government are often applied to the entire population of organizations, thus making the adoption decisions less adaptive and less flexible (Pfeffer and Salancik, 1978).

Coercive isomorphic process is also manifesting outside the governmental arena. Customers (if not specified, customers are mainly referring to buying firms hereafter) can also develop forceful rules for other firms to abide by. Customer pressure is referred to as a force, persuasion, or invitation that is applied both implicitly and explicitly by

customers to which other firms must respond (DiMaggio and Powell, 1983). Customers are the sources of business. In this sense, they may impact their supply chain partners to a great extent. For instance, IBM has embraced the C-TPAT program and expressed coercive pressures for its suppliers to adopt the same program. One memorandum signed by IBM's top procurement officer stated:

> "C-TPAT efforts are underway today. IBM has pledged full cooperation with this initiative. As a C-TPAT participant, IBM is assessing its own security practices. As an IBM supplier, you also have a role to play in ensuring the security of the supply chain…Adherence to the C-TPAT security recommendations is critical to strengthening security for all supply chain members. Your assistance in this endeavor is required…Global Procurement, in conjunction with the IBM Import Compliance office, will be monitoring the supply chain security issue and will advise our suppliers of any new developments in this area." (see, www-03.ibm.com/procurement).

The government and customer pressures are likely to surface in the field of SCS. Nations have a habit of legislating strict SCS requirements in order to protect their countries, their people, and the flow of global commerce. That is why countries, such as the United States of America, require containers be screened by security personnel, machines, or specially trained dogs at international ports or borders to prevent weapon and drug smuggling. Governments request better SCS and they can achieve it partly by imposing specific security requirements on business organizations. Customers also need

better SCS to assure the integrity of their products and protect their intangible assets (e.g., reputation). They implement SCSM standards (e.g., ISO 28000); they benchmark against their peers in term of SCSM strategies; they also adopt "best SCSM practices". However, those effects are likely to be nullified if their supply chain partners are unwilling to invest in SCS as a supply chain is as secure as its weakest link. Thus customers have the motivation to place forceful pressure on their suppliers for better SCS.

3.1.2 Mimetic Pressure

The second institutional isomorphism pressure refers to mimetic pressure. It derives from uncertainty and competition (DiMaggio and Powell, 1983; Scott, 2001). When the technologies are poorly understood, when the goals are ambiguous, or when the environment creates systematic uncertainty, organizations are prone to model themselves after other successful organizations (March and Olsen, 1976). The advantages of mimetic behaviors are considerable; when an organization faces a problem with ambiguous causes or unclear solutions, mimicking may be a viable solution with little expense (Cyert and March, 1963). The "models" may be diffused explicitly by organizations such as consulting firms or industry trade associations, or unintentionally, indirectly through reports from leading firms or employee mobility. One of the most dramatic instances of modeling was the effort of Japanese revolutionaries in the late nineteenth century to model new governmental initiatives on successful western nations (Westney, 1982). Western organizations are now returning the compliment by

implementing Japanese JIT and quality management models to cope with thorny productivity and personnel challenges in their own firms.

The literature suggests that the effects of SCSM mechanisms can be uncertain and thus the mimetic pressure is likely to gain momentum. For example, Sheu et al. (2006) demonstrate that because SCSM initiatives (the C-TPAT program in their study) are a means rather than an end, their value to supply chain security performance is, in fact, not clear. A study by Gutierrez and Hintsa (2006) provides support for this argument. They compare nine SCSM programs and show that no two programs share exactly the same measures, indicating that even leading professional organizations and governments have different perceptions of what constitutes best SCSM practices. The situation gets even worse as SCSM mechanisms are usually supplemented with convoluted regulations. Top managers may neither be confident on how to implement SCSM mechanisms, nor do they understand the expected outcomes of these strategies and practices. Hence mimicking successful peers who are socially praised by industry members may isolate firms from criticism and avoid unnecessary losses (King and Lennox, 2001).

3.1.3 Normative Pressure

The third institutional isomorphism pressure is normative in nature. It stems primarily from professional, cultural, and ethical expectations, which in turn guide decision-making (DiMaggio and Powell, 1983; Khalifa and Davison, 2006; Scott, 2001). It captures the effects of typically less visible social obligations and cultural patterns on

firm activities. The normative pressure usually results in professional, industry, or cultural norms (e.g., rules of thumb, standard operating procedures, occupational standards) (Hoffman, 1999). The normative pressure is able to regulate or mobilize industry wide opinion in favor of, or in opposition to, an organization's operational practices (Sarkis et al., 2010). According to DiMaggio and Powell (1983) normative pressure is primarily diffused through the growth of professionalization. The major recent growth in the profession has been among organizational professionals, particularly managers and specialized staff of large organizations (e.g., Certified Professional in Supply Management, CPSM). While various professionals within an organization may differ from one another, they exhibit much similarity to their professional counterparts in other organizations. These professionals are likely to share the same opinion on how work should be done, what ethics to stick to, how to train future professionals, and how to establish a professional basis for their occupational autonomy. Indeed, it is argued that a pool of almost interchangeable employees (for a specialized job) is created through formal education and professional networks (Scott 1983, 2001). By occupying similar positions across a range of organizations, these professionals who share a similar orientation and disposition override the control mechanisms which shape organizational behaviors (Liang et al., 2007). Consequently, the strategies and practices these professionals and the professional organizations they belong to (e.g., Council of Supply Chain Management Professionals, Institute of Supply Management, etc.) promote are likely to become norms and thus be widely adopted in an industry (Liang et al., 2007).

In reference to SCS, the norms can be formed through several means. For example, trading and professional organizations are not just working with their supply chain partners to improve SCS, they are also promoting common, global SCSM standards. Such standards may reduce the burden of dealing with multiple, potentially conflicting regulations between countries, thus enabling companies to develop internal processes that are truly global (Flitch, 2007). The World Customs Organization (WCO) members have adopted the SAFE framework of standards for securing and facilitating global trade (WCO report, 2007). Many firms around the world have adopted the ISO 28000 standards regarding SCS. Bit by bit, as more and more firms start to adopt these SCSM standards and programs, the strategies and practices involved in these standards and programs gradually become occupational norms that firms would have to comply with. Consequently, firms under normative pressure need to take action to assure they can meet these SCS related professional, industry, or cultural norms.

3.1.4 Competitive Pressure

Lastly, some institutional theory scholars have drawn attention to performance pressure as well. Unlike the first three classic pressures that are dubbed as institutional isomorphism, the effect of performance demands as a pressure mechanism is portrayed as competitive isomorphism. Lounsbury (2007) argued that segregating economic and social logics is problematic, since the distinction between technical and social benefits is itself embedded in institutions (Lounsbury, 2002; Thornton, 2004). The cautionary note here is that institutional theorists rarely make an effort to disentangle institutional

isomorphism from competitive isomorphism. Compared to the classic institutional isomorphic processes (i.e., coercive, mimetic, and normative isomorphism), competitive isomorphism is more acceptable to organizational economists and organizational sociologists alike. It emphasizes that market competition weeds out less efficient strategies and practices in favor of more efficient ones (Heugens and Lander, 2009; Scott, 2001). Its focus is notably favoring performance.

Indeed, institutional theorists have proposed at least three reasons why the adoption of (new) strategies and practices may result in better performance (a practice can be considered new if the firm has never adopted it before, irrespective of its longevity). First, the newly adopted strategies and practices may simply represent a better way of organizing and managing resources than extant alternatives. Pioneers often adopt these strategies and practices because of substantive efficiency and quality gains (Westphal et al., 1997). Second, as the strategies and practices prove themselves (as manifested by pioneers' competitive advantage), late adopters may benefit substantively from adopting them as well: (1) late adopters can learn from early adopters so that the implementation becomes smooth and cost-efficient; (2) late adopters also stand in a good position to gain symbolic benefits since the strategies and practices may have been somewhat institutionalized and thus have legitimacy. Third, resource providers opt for socially acceptable organizations that (1) do not threaten their reputation, (2) have strategies and practices the providers recognize as "rational," and (3) are less likely to fail because of unanticipated events (Baum and Oliver, 1991; Deephouse, 1999). Firms

that adopt socially promising strategies and practices are thus more likely than their non-participating peers to attract resources of higher quality at favorable terms.

The adoption of SCSM mechanisms can lead to performance improvements (Rice and Spayd, 2005; Peleg-Gillai et al., 2006). These performance gains are mainly reflected by collateral benefits such as reduced cost, better supply chain responsiveness, improved supply chain resilience, as well as improved supply chain visibility, (Rice and Spayd, 2005; Closs and McGarrell, 2004; Lee and Whang, 2005; Peleg-Gillai and Bhat, 2006; Mena et al., 2009). For example, due to the highly negative impact that SCS breaches present, customers increasingly value the care that suppliers undertake with their supply chains (Whipple et al., 2009; Goldberg and Herman, 2006). As a consequence, firms well equipped with SCSM mechanisms are likely to gain better reputation than their counterparts. In addition, Kennedy and Fiss (2009) illustrated that organizations are indeed affected by the rationale of both efficiency and legitimacy, because efficiency and legitimacy complement rather than conflict with each other. In other words, the "performance pressure" argument suggests that firms may adopt SCSM mechanisms because they truly believe that such adoptions can improve efficiency and effectiveness, leading to competitive advantage or operational benefits.

3.2 Hypotheses Development

3.2.1 Antecedents of SCSM Mechanisms

Institutional pressures can play an important role regarding the implementation of SCSM mechanisms. Specifically, I argue that all institutional pressures (government,

customer, peer, normative, and performance) would positively affect prevention, detection, reaction, and restoration-oriented SCSM mechanisms respectively.

3.2.1.1 Institutional Pressures → Prevention-oriented SCSM Mechanisms

In regards to SCS, a government holds great responsibility to avert SCS breaches from happening, because the losses resulting from these supply chain incidents can be devastating and may affect the lives of many people. For example, in early 2012 a counterfeit version of the widely used cancer treatment medicine Avastin was found circulating in the United States (USA Today, 2012). About 70 people died because of the use of such counterfeit drugs over that time period (Perrone, 2012). In the same year, hundreds of thousands of counterfeit airbags were found installed in cars in the United States. Those airbags cannot protect passengers during car accidents and can kill them even under normal conditions because they may explode for no apparent reason, putting innocent people's lives at enormous risk (Foxnews, 2012). Governments cannot treat these types of SCS breaches lightly as public health and human life come into play. Meanwhile, there is little a government can do to make up for the damages sustained on the aftermath of SCS breaches. As a result, many countries and regional unions (e.g., the E.U.) have recently undertaken security initiatives and passed laws which demand necessary organizational controls to prevent SCS breaches. Harsh punishments for violating SCS related laws are too high for firms to afford. Under such circumstances, firms have to act preventively when dealing with SCS threats.

Customers also play an important role in the adoption of prevention-oriented SCSM mechanisms. Following the increasing trend of globalization, firms utilize offshore suppliers to mitigate their operational bottlenecks and achieve competitive advantage. When firms work with their offshore suppliers, supply chains become more complex than ever before. However, many SCS issues which could be easily addressed in the past can now generate big headaches as many more parties are involved and the focal firm may not have effective control over them. A recent example is the failure of the gigantic Chinese milk producer Sanlu in 2008. The company failed to prevent its suppliers from using adulterated raw materials. The tainted milk products led to the death of three infants and more than a thousand ill children. The company went bankrupt and the milk industry lost approximately $5 billion in sales due to their damaged public image (A.T. Kearney Analysis, 2010). The costs of a SCS incident that stems from upstream suppliers can be devastating. Thus, customers have strong motivations to educate their suppliers and enforce their suppliers to achieve better SCS by preventing any possible security incidents from happening.

Firms are also subject to peer pressure. Many firms have rankled their peers by offering superior SCS performance with lower costs. While there are many ways to achieve better SCS, the implementation of preventive routines is always one of the best choices. In general, prevention-oriented SCSM mechanisms focus on internal education, organizational collaboration, and supply chain re-configuration in order to identify potential SCS breaches and address them before they materialize. As Lee and Whang (2004) pointed out, investments in preventative mechanisms would pay off handsomely

as the effort required to solve problems on the aftermath of a SCS disruption would be drastically reduced. Consequently, the adoption of preventive mechanisms has become a ubiquitous phenomenon in various industries and is considered an indispensable element of a company's multilayered approach toward mitigation of SCS breaches (Autry and Bobbitt, 2008). As more and more firms across industries begin to realize the importance of SCS and understand the power of a preventative orientation, prevention-oriented mechanisms garner more and more prevalence and legitimacy. Consequently, firms are likely to model after their successful peers and adopt prevention-oriented SCSM mechanisms in order to reap the benefits that their peers have gained and to stand in competition with those peers.

Of great importance to prevention-oriented SCSM mechanisms is normative pressure. Norms generally take the form of rules of thumbs, standard operating procedures, and occupational standards (Hoffman, 1999). Ignoring these norms may lead to being overlooked by other firms in the same industry and may diminish the focal firm's ability to obtain societal resources and avoid questioning (DiMaggio and Powell, 1983). In the context of SCS, the normative pressure is primarily reflected as professional norms. Many professional organizations (e.g., ISO) and international bodies alike have developed SCS standards and programs. The standards and programs help reduce the burden and complexity of dealing with multiple, potentially conflicting, regulations between countries, enabling companies to develop internal processes based on a global basis. As such, those standards and programs are likely to be institutionalized as professional norms and widely embraced by firms across different industries. Typical

examples of these standards and programs include, but are not limited to, Business Alliance for Secure Commerce rules (BASC rules), ISO 22000, ISO 28000, ISO 31000, Transported Asset Protection Association's Trucking Security Requirements (TAPA's TSR), and the WCO-SAFE framework (see table 11). These standards and programs all place high priority on preventive practices such as conducting unannounced security assessments of logistics providers and developing visibility of supplier practices across all tiers. Consequently, the diffusion of these standards and programs has shaped the operating environment and resulted in several preventive-in-nature professional norms that firms need to conform to.

Table 11. Major voluntary security programs facts comparison

Program	Operational since	Geography	Tenets or Key Elements
ISO22000 (ISO standards for food safety)	1993	Any to any, global coverage	States requirements in terms of *results* rather than *means* for SCS. Introduces innovations in (1) Prerequisite programs, (2) Hazard identification and determination of acceptable levels, (3) Selection and assessment of control measures, (4) Evaluation of individual verification results, (5) Analysis of results of verification activities.
ISO28000 (ISO standards for supply chain security)	2008	Any to any, global coverage	Specification for security management systems for the supply chain. Assists in implementing governmental and international customs agency security initiatives, including the WCO's Framework of Standards to Secure and Facilitate Global Trade, the EU AEC Program, the US C-TPAT, and the International Maritime Organization's (IMO) ISPS Code.
ISO31000 (ISO standards for risk management)	2009	Any to any, global coverage	The focus of ISO 31000 programs is centered on: (1) Transferring accountability gaps in enterprise risk management, (2) Aligning objectives of the governance frameworks with ISO 31000, (3) Embedding management system reporting mechanisms, (4) Creating uniform risk criteria and evaluation metrics.
AEO (authorized economic operator, the WCO framework of standards to secure global trade)	2005	Any to any, global coverage	AEO designates the status that customs authorities from European member states should grant to reliable traders established in the European Community. AEO traders will be able to obtain one or both of the following certificates: i) Simplification for Customs procedures ii) Facilitation for security and safety. *European Commission (2005).*

Table 11. continued

TAPA TSR (TAPA's security requirements to fight crime on international highways)	1992	Any to any, global coverage	Specifies the minimum acceptable standards for security throughout supply chains utilizing trucking and associated operations, including the methods to be used in maintaining those standards.
BASC Standards (Business Alliance for Secure Commerce Standards, a set of international business standards created to promote secure international trade)	1996	Region to region (Latin American to North American/Europe)	Examines the entire process of manufacturing and shipping of merchandise, emphasizing the creation of a more security-conscious environment throughout the supply chain.

Finally, performance pressure also drives the adoption of prevention-oriented SCSM mechanisms. The literature suggests that performance improvements can be achieved by implementing preventive SCSM mechanisms (Rice and Spayd, 2005; Peleg-Gillai et al., 2006). These performance gains are mainly reflected by collateral benefits such as reduced cost, better supply chain responsiveness, better supply chain resiliency, and improved supply chain visibility (Rice and Spayd, 2005; Closs and McGarrell, 2004; Lee and Whang, 2005; Peleg-Gillai and Bhat, 2006; Mena et al., 2009). An example of these collateral benefits arising from SCSM mechanisms are the results attributed to the adoption of the concept of the Authorized Economic Operator (AEO). AEOs are parties involved in international trade (such as importers and carriers) that have implemented SCSM standards and preventative practices in order to effectively manage SCS threats. In return for their SCS investments, firms with AEO status do receive benefits from governments such as expedited processing of their goods by customs authorities. In addition, there is strong evidence that active prevention results in lower overall costs in quality management (Lee and Whang, 2005). Many preventive SCSM mechanisms can help firms avoid operational errors and unnecessary accidents. Indeed, a number of

preventive-in-nature SCSM mechanisms share the same concepts with the TQM strategies and practices, which can effectively prevent quality defects (Lee and Whang, 2005). Rice and Spayd (2005) also illustrate that prevention-oriented SCSM mechanisms allow firms to quickly respond to SCS breaches and thus reduce the potential damages caused by these breaches. Therefore, firms driven by their desire to improve substantive performance are likely to implement prevention-orientated SCSM mechanisms.

Overall, all institutional pressures may positively affect the implementation of preventive SCSM mechanisms. Hence,

H1: Institutional pressures are positively related to the level of the deployment of prevention-oriented SCSM mechanisms.

3.2.1.2 Institutional Pressures → Detection-oriented SCSM Mechanisms

The human skin cannot block all pathogens from gaining access to the human body and cannot defeat bacteria that make it pass its layers. Similarly preventive SCSM activities cannot resolve all SCS challenges. As Efrain Perez, a program manager with CBP, said, "patrol officers are vigilant about looking for suspicious behavior (such as smuggling at the U.S.-Mexico borders), but it's impossible to catch every single person." (www.daily-jeff.com, 11 Feb 2012, available at: http://www.daily-jeff.com/ap%20washington/2012/02/11/us-faces-tough-fight-in-cash-smuggling-crackdown). Even when firms have high preventative ability, SCS breaches can still occur because many of them are intentionally designed and are unpredictable (Speier et al., 2011). Therefore, governments require firms to develop the ability to detect potential

security breaches in their supply chains. For instance, the government obliges airlines to keep flying safely and demands that cargo shipments be inspected. Yet achieving smooth implementation of the additional cargo screening measures will require significant resources to build detection capabilities. As Lichtenstein (2010) described, "The only way to achieve that is by ensuring a thorough but efficient detection process that maintains the flow of goods, not just in the United States but around the globe." (available at: www.supplychainquarterly.com/columns/scq201001monetarymatters/). In fact, numerous government-imposed SCS initiatives are composed of detection-oriented practices, such as inspection of cargo shipments and screening of mail packages at international ports. It is rather common that firms pursue detection-oriented SCSM mechanisms due to government pressure.

Detection ability is also pertinent for customers (buying firms). Early detection ability afforded by suppliers offers buying firms significant leeway to analyze potential SCS breaches and thus allows for an effective action to control or even address these breaches before they materialize and cause damage to the supply chain. In addition, various SCS breaches, such as smuggling of cigarettes or people, are intentionally planned and carefully executed and are thus neither visible nor easy to detect. Their direct impact to the firm may be minor as these activities do not necessarily slow down the movement of products or increase operating costs. However, their indirect influence can be overwhelming (e.g., smuggled weapons of mass destruction can be used by terrorists). While the potential negative results are affected by many factors (e.g., how smart the bootleggers are or the extent to which suppliers cooperate with buying firms to

secure the supply chain), final consumers generally hold the buying firms accountable for the consequences. To avert such issues, buying firms need to work closely with their supply chain partners to detect illicit conduct.

In addition, mimicking peers, which demonstrate strong detection ability, may be helpful. In general, firms with better detection ability are likely to be stronger competitors. Early detection implies that firms can either respond to SCS breaches in a timely manner or may have more time to deal with these breaches that may result in supply chain disruptions. The flow of products in the supply chain would thus be expected to be more stable when an effective detection system exists. Stable product flow may lead to operational benefits for both the focal firm and its customers as they face less uncertainty that needs streamlining. Consequently, firms are inclined to mimic detection-oriented SCSM mechanisms from successful companies. Many SCSM programs such as the C-TPAT and CSI (container security initiative) have highlighted the needs as well as the benefits of detection activities. The U.S. government explicitly states that the development and deployment of sophisticated detection technology is essential for SCS (www.cbp.gov/xp/cgov/about/mission/cbp.xml). Leading organizations, such as Walmart, have been using GPS and RFID technologies to detect deviations in their supply networks for many years and have reported substantial gains (Williams, 2004). As a result, firms facing peer pressure to achieve better SCS are motivated to model their actions after firms with superior detection abilities.

Further, detection ability has been gradually normalized in the last decade. The fundamental reason is that detection-oriented SCSM mechanisms not only provide better

SCS performance but also better supply chain visibility that firms need in order to succeed. For example, firms can utilize real time information gathered from detection-based technologies to offer better services to customers. RFID and GPS tracking devices, which are used to detect illicit activities (e.g., theft/misuse of transportation vehicles), also enable firms to provide more accurate delivery schedules and thus improve customer satisfaction. Professional organizations, such as the Transported Asset Protection Association (TAPA), also fuel the formation of these norms. For example, each year TAPA holds three meetings with executives from a variety of industries, which allow these practitioners to share knowledge and develop professional norms. As more and more firms learn and start to take advantage of what detection capabilities offer, buying firms now treat high supply chain visibility as a taken-for-granted benefit that their suppliers should provide. While such changes occur almost imperceptibly, bit by bit, they have become the industry norms (i.e., occupational standards) and thus drive organizational behaviors. In this sense, normative pressure will motivate firms to adopt detection-oriented SCSM mechanisms.

In a similar vein, detection orientated SCSM activities often lead to operational and financial benefits. For example, continuous monitoring enables firms to have a better sense over their key assets, such as high value inventory, and thus may reduce employee theft and inventory shrinkage. Periodic evaluation of suppliers to detect potential security glitches gives firms an opportunity to assess the vulnerabilities of their supply chains. It may also help firms build a sturdy relationship with their suppliers though meaningful communications. The active oversight over supply chain operations

could result in better understanding of the supply chain and thus lead to potential exploitative improvements. In short, detection-oriented SCSM mechanisms may result in improved performance. Hence, the desire to improve performance is likely to be one reason why firms want to adopt detection-oriented SCSM mechanisms. Taken together, I propose:

> *H2: Institutional pressures are positively related to the level of the deployment of detection-oriented SCSM mechanisms.*

3.2.1.3 Institutional Pressures → Reaction-oriented SCSM Mechanisms

When a SCS breach does occur, the government may require firms to react effectively in order to assure that the public is safe. For example, cargo theft in Mexico has increased 20%-40% per year from 2006 to 2010 (Truckinginfo, 2012). Food and drink products were most targeted by cargo thieves. These thefts carry with them great potential to hurt the public, because contaminated food and drink products can easily result in thousands of ill people in a short period of time (Wein and Liu, 2005). Mexico's National Chamber of Freight and Auto Transport has urged firms operating in Mexico to adopt SCSM measures so that they can react to truck thefts more effectively (Truckinginfo, 2012). Another example is the theft of 128,000 vials of Levemir in 2009. Levemir is a long-acting insulin type that requires constant refrigeration to preserve its potency. However, the stolen vials were not kept in cold storage and were sold to clinics. A patient at the M.D. Anderson Cancer Center in Houston used Levemir from the stolen batch and his blood sugar level spiked uncontrollably. Later, the patient died from

cancer-related causes triggered by the use of the tainted Levemir (CNN, 2011). The FDA put out nationwide alerts and made Novo Nordisk (the Levemir manufacturer) accountable to control the spread of the vials. The company quickly sent alerts to all of its authorized distributors and retail pharmacies. Levemir vials which shared the same lot size with the stolen ones were recalled. Additional security measures were also undertaken in order to avoid future thefts. Hence, it is not uncommon that a government would push firms to implement reaction-oriented SCSM mechanisms.

From a customer's perspective, appropriate reaction on the aftermath of SCS events is an imperative. Continuous product flow is critical to buying firms. Consumers cannot wait. Business opportunities will never come back especially when a product is in its growth window. As such, maintaining normal operations or returning to the state quo after a SCS crisis becomes an essential ability that firms must attain. In order to comfort their customers, firms must react to SCS breaches effectively to a point such that the normal operations would not be significantly affected and thus the delivery of products would not be compromised. Otherwise, economic losses are likely to follow. For example, metal theft is a vexing problem for Network Rail, a company that operates Britain's rail infrastructure. In the 2011 financial year, metal theft alone resulted in more than 360 hours of disruptions. Ineffective responses to those thefts lead to numerous supply delays. Network Rail estimated that it spent £689,000 (approximately $882,847), an increase of almost 50 percent compared to the previous year, to compensate customers for the delays (Pol-PRIMETT, 2011; http://www.pol-primett.org/cable-theft-causes-more-360-hours-disruption-north-east-passengers). Later, strong customer

pressure has forced Network Rail to conduct a thorough evaluation of its SCSM system and improve its reaction ability in order to effectively manage SCS disruptions. Customer pressure is rather conducive to reaction-oriented SCSM mechanisms.

Not only do government pressure and customer pressure motivate firms to implement reaction-oriented SCSM mechanisms, firms also model after successful firms as it relates to reaction because of peer pressure. Simply put it, quick reaction to SCS breaches is always preferred over slow reaction in the business world. Through rapid reaction, firms can minimize, contain, or even control the magnitude of damages caused by SCS breaches. As a result, many firms have recently equipped themselves with disaster recovery plans or back up processes that can assist them at times of a SCS crisis (Kleindorfer and Saad, 2005). They pre-position resources and build up "strategic redundancy". Employees are also cross-trained so that they can handle multiple tasks when needed. While these practices are employed to respond to SCS breaches, they also result in an array of collateral benefits such as improved supply chain responsiveness as firms can effectively solve supply chain problems. As such, reactive SCSM mechanisms have generated competitive advantage for the adopting firms. In order to garner these benefits and be competitive, firms are prone to mimic their peers that are successful in reacting to SCS breaches.

Quick reaction is also in line with a firm's social obligations. Effective reaction to SCS breaches is expected by a firm's supply chain partners and its social audience. If a SCS breach cannot be controlled, chances are it will generate serious issues with a potential to put firms along its value chain in trouble. In this sense, the implementation

of reaction-oriented SCSM mechanisms is a social norm that firms would endorse. The adoption of these mechanisms also helps generate positive publicity, rendering adopting firms better positioned to compete. In addition, many reaction-oriented SCSM mechanisms are embedded in professional SCS standards and programs. For instance, the ISO 28000 standards have specific requirements with respect to the development of protocols for communication when a SCS crisis arises. The ISO 28000 standards also set up guidelines regarding the deployment of well-defined contingency plans as well as the collaboration mechanisms among supply chain partners as a response to a SCS crisis. As these professional SCS standards and programs gain popularity, many reaction-oriented SCSM mechanisms gradually become part of the industry/professional norms that firms should follow. In other words, normative pressure is an important reason that firms carry out reactive SCSM mechanisms.

On top of the abovementioned pressures, the need for better performance is always a motive for a firm to put forward a plan for reaction-oriented SCSM mechanisms. Effective reaction to SCS breaches is usually associated with better performance as this action may minimize the potential adverse effects caused by SCS breaches. Active response during a breach reduces the effort needed to solve problems later. On the other hand, sloppy reaction could generate economic seriousness for many companies. For example, when the SONY's PlayStation Network was turned off due to hacker attacks between April 17 and April 19, 2011, the company claimed that it would resume online services within a week (Thorsen, 2011). However, it turned out that SONY was not prepared for that type of SCS breach and overestimated its reaction

capability. It took the company 24 days to get its online services running again. The unsuccessful responses cost the company approximately $171.4 million and the costs to the industry associated with it could be as high as $24 billion dollars (Thorsen, 2011). As reaction-oriented SCSM mechanisms are well accommodated with a firm's need to respond to accidents and enhance performance, it is suggested that firms may adopt reaction-oriented SCSM mechanisms in order to improve performance.

Taken together, I propose:

H3: Institutional pressures are positively related to the level of the deployment of reaction-oriented SCSM mechanisms.

3.2.1.4 Institutional Pressures → Restoration-oriented SCSM Mechanisms

Governments may want firms to recover from SCS breaches as soon as possible such that those breaches won't generate further hardship. The logic here is analogous to the recovery of the human body from diseases. A body which cannot effectively recover from pathogen attacks would remain sick. This in turn provides opportunities for latent threats (e.g., the opportunistic pathogens) to become effective, which may further worsen the situation. Similarly, supply chains which cannot recover quickly from serious SCS breaches may suffer from a compromised SCSM system and therefore bear more risks of being targeted again. Governments are quite sensitive to SCS breaches in this respect. They need to keep a close eye on the aftermath of a SCS crisis. For example, the U.S. government has been actively involved in helping airlines to recover and rebuild their security management systems such that passenger aircrafts won't be used again to

create another 9/11 attack. In other words, governments are likely to require firms to have well established restoration plans.

Similarly, customers also need their supply chain partners to have disaster recovery plans in order to reinstate operations efficiently. Buying firms are aware that uncertainty can never be completely eliminated. Thus, they invest toward recovery mechanisms. Generally, buying firms can handle temporary supply shortages from their major suppliers by (1) purchasing from high cost alternative suppliers, (2) building up safety inventories, or (3) utilizing express shipments via more efficient transportation mediums such as airfreight. However, these short term solutions may not be viable at the time of a SCS crisis as many suppliers could be impacted by the same crisis simultaneously. In addition, the alternative suppliers may have capacity constraints at the time of a crisis and not be able to fulfill customer needs even when a premium price is paid. Moreover, even when capacity is not an issue, these urgent orders usually come with a stiff price to the buyers. Buying firms still need their major suppliers to recover quickly. In some cases, buying firms practice single-sourcing (e.g. purchasing CPUs only from Intel). Under such circumstances, they have no choice by rely on the supplier to restore its operations. In this sense, buying firms will push their major suppliers to build up necessary restoration ability.

Restoration on the aftermath of a SCS crisis is also associated with peer pressure. Firms are expected to benchmark and learn from others in order to build restoration ability. Usually, firms may encounter ongoing and obtrusive attention from the authorities (e.g., regulators) and the media (e.g., the newspapers) after a major crisis

(Sutton and Galunic, 1996). Firms that cannot swiftly restore operations are thus likely to be considered as incapable to handle SCS breaches. Such "lack of capability" hurts not only a firm's immediate market share but also could significantly jeopardize its future business as the firm's reputation is eroded. In this sense, effective restoration from SCS breaches has great performance implications. Rapid and efficient restoration may allow firms to outmaneuver their peers and create competitive advantage. As such, companies are likely to model after their successful peers who have exhibited excellence in restoration ability.

Restorative SCSM mechanisms are associated with SCS norms as well. Before the emergence of serious SCS breaches in recent years, firms used to overlook their supply chain restoration ability. Some of them only had a very brief and crude plan and most of them did not even have an executive officer dedicated to restoration/recovery management. Disaster recovery, however, began to gain currency in recent years and became an industry norm due to an array of natural and man-made disasters (Knemeyer et al., 2009). A few organizations started to pay attention to SCS breaches such that they created a dedicated office for SCSM and developed a clear chain of command to make sure effective restoration will be in place when SCS breaches occur. Many SCSM programs, including the Free and Secure Trade program (FAST), Internal Security Assessor (ISA) program, and the C-TPAT program, have clear focus on strategies and practices that aim to provide quick recovery after SCS breaches. Consequently, restoration ability has become a "must-meet" norm as perceived by firms across industries.

Finally, post-incident restoration is also critical as some SCS incidents (e.g., the 9/11 terrorist attacks) may have significant and long lasting effects on global supply chains. Successful restoration may help firms avoid continuous public scrutiny on the aftermath of a SCS breach and thus lower the administration cost to manage public relations. In addition, it is in their best interest for companies to implement restoration-oriented SCSM mechanisms. Just as the human immune system needs the blood platelet to promote blood clotting and wound repair (Parham, 2005), companies need restoration ability to heal their "wounded" operations. For example, Republic Bank of Fort Lauderdale, a local bank in the state of Florida, was recently attacked by a hacker who stole the personal data of 3,600 online-banking customers. The bank has hired a team of IT professionals and spent significant financial resources to improve IT security before it can re-open its online services (BankersOnline.com, 2013). However, this damaged customer trust and shareholder confidence would be difficult to recover. Many more efforts have been undertaken by the bank in order to repair its eroded reputation. The story suggests that if companies do not invest in restoration before a SCS breach happens, they will be paying a lot on the aftermath of the SCS breach. Therefore, it is quite reasonable to expect that firms will consider performance pressure when adopting restoration-oriented SCSM mechanisms.

H4: Institutional pressures are positively related to the level of the deployment of restoration-oriented SCSM mechanisms.

3.2.2 Relative Power of Antecedents

Supply chain security and trade facilitation are not mutually exclusive, but it is not easy to support both equally. Institutional stakeholders (e.g., the government versus the buying firms) may have conflicting interests when it comes to SCS. While better SCS is generally a desirable outcome for all parties, each constituent is driven perhaps by different motives. For example, governments need better SCS at the firm level to ensure or enhance security at the national level. They want to protect the country and the people. Because of the significance of human life, SCS requirements originating from government directives cannot be compromised. From a government's perspective, the profitability of an organization is secondary. The obligation to provide reasonable protection overrides the need for firm profitability. To achieve necessary or expected levels of SCS, legislation is usually ratified without consideration for firm profitability. For instance, the 100% inspection of U.S.-bound containers policy mandates nonintrusive imaging and radiation detection for 100% of U.S.-bound containers at international ports. While enhancing national security, the resulting congestion hinders international trade significantly (Bakshi et al., 2011). As an executive from a global electronics manufacturer that operates in more 150 countries put it recently: "We can have the most incredible manufacturing, and the supply chain dies as soon as it hits the border" (Thomas, 2010).

Customers, predominantly comprising buying firms, also require superior SCS. But their intents are quite different from those of a government. Governments promote SCSM mechanisms primarily for sole security purposes. Buying firms, however,

advocate SCSM mechanisms not only to ensure the security of their products but also to protect their reputation and public image. The onerous government mandates that are likely to follow a SCS attack (e.g., the 100% inspection of U.S.-bound containers policy after the 9/11 terrorist attacks) will generally *slow down* the supply chain. Buying firms, on the other hand, want fast movement of products because they need the right products in the right place at the right time with low cost. Buying firms are profit driven. They may not be willing to compromise some aspects of their supply chain performance (e.g., fast/on-time delivery) for better SCS in all cases (Voss et al., 2009a). Consequently, firms must carefully consider whether or not the implementation of SCSM mechanisms will compromise other supply chain performance measures, especially when these implementations may result in unsatisfied customers. Hence, there is likely to be a balance between SCS and operational efficiency if customer pressure is the primary driver of SCSM mechanisms. The SCSM mechanisms are apt to be executed to a point such that the operational outcomes would not be significantly and negatively influenced by security related actions. As an IBM top security executive said, "both SCS and trade facilitation are necessary to keep the global economy running efficiently and effectively" (Fletcher, 2007).

Due to the different intents of these institutional stakeholders, their influences on each class of SCSM mechanisms may vary. For example, government pressure would be stronger on prevention-oriented SCSM mechanisms than on restoration-oriented ones because governments generally do not care as much about how firms recover from a SCS crisis as long as the national security goals are achieved. Therefore, it is

theoretically and practically relevant to explore the relative power of different institutional pressures on each class of SCSM mechanisms respectively.

Preventing SCS attributed tragedies in the first place is critical to the governments. This is the case not only because prevention is a cost-efficient way to achieve better SCS but also because the results of SCS breaches can be devastating. The 9/11 terrorist attacks left 2973 victims, with more than 6000 injured people. The U.S. stocks alone lost $1.4 trillion in value during that week (Bob, 2001). The negative effects of those attacks went further than economic losses to human life and beyond. The losses caused by the 9/11 terrorist attacks are not something a country can afford to repeat. If any party would promote prevention-oriented SCSM mechanisms, government would be one of the first advocators.

Customers prefer better prevention as well. However, as I elaborated earlier, their actions are largely profit-driven. As long as the suppliers can control the impacts of SCS breaches on their customers to a reasonable level, relatively low levels of prevention are somewhat acceptable to customers. Similarly, firms would mimic peers in the same industry or follow industry norms to improve prevention ability. They may also adopt it because of performance concerns. Yet these drivers would not appear to be as strong as government mandates. While all institutional stakeholders want high levels of prevention, no one comes as strongly and forcefully as government pressure.

H5: Government pressure is the strongest institutional predictor of prevention-oriented SCSM mechanisms.

Government pressure is likely to be the strongest predictor for detection-oriented SCSM mechanisms as well. Nations want to keep supply chain related security problems outside their borders and therefore launch very strict detection processes at their national boundaries and international ports. They want firms to provide necessary cooperation and implement detection processes to accommodate government legislation. U.S. mandates, such as the 100% inspection of containers at international ports and the 10+2 rules designed for international carriers and importers, attest to these interests. These government-mandated programs have placed considerable pressures on organizations that operate globally. Without solid detection ability in hand, firms are likely to face sanctions.

Customers would also benefit if their suppliers have better detection ability toward SCS. Detection-oriented SCSM mechanisms, such as the installation of RFID or other technology-based solutions, improve supply chain visibility that provides time sensitive information regarding delivery schedule. Utilizing such information, customers can coordinate their own manufacturing activities or manage their inventory levels more efficiently. Besides, better detection carries with it the opportunity to better respond to potential SCS breaches. For example, early detection gives firms the leeway to deploy effective action in order to reduce losses and maintain normal operations. Nevertheless, nothing comes without a price. Effective detection requires not only state-of-the-art equipment but also collaboration among different parties along the supply chain. The costs of building superior detection ability include but are not limited to administrative costs, the cost to deploy advanced tracking systems, and the cost to develop an effective

communication channel, both within and outside a firm's boundaries. While large firms may already invest in those areas, it may not be the case for small to medium size firms, which have limited resources to invest toward SCS. In other words, government pressure applies to all kinds of firms irrespective of their size whereas customer pressure may only effectively affect large firms that have the resources to implement detective mechanisms. As such, customer pressure would not to be as strong as government pressure.

In the same vein, normative pressure and peer pressure are unlikely to have a stronger impact than government pressure. Norms are generally "rule of thumbs" and lack effective legal binding. Peer pressure motivates the adoption of SCSM mechanisms that have been widely implemented by peers. However, firms still have the right to either respond or not respond to peer pressure. On the other hand, performance pressure may have a rather strong effect on the implementation of detection-oriented SCSM mechanisms. High detection ability may lead to a number of collateral benefits such as improved supply chain responsiveness and supply chain visibility (Closs and McGarrell, 2004; Peleg-Gillai and Bhat, 2006). Better detection ability enables quick and early reaction to SCS breaches. Owing to early detection, firms can save significantly as less effort is needed to resolve problems later. High supply chain visibility, obtained via detection processes, also prevents theft and therefore cuts inventory shrinkage related costs. However, due to idiosyncratic situations firms are facing, they may or may not fully redeem those collateral benefits. For instance, better customer satisfaction comes only when buyers desperately require timely product information. In other words, there

is some level of "uncertainty" regarding potential outcomes, which impedes firms from harvesting collateral benefits associated with superior detection ability. Firms may still hesitate to invest in detection-oriented SCSM mechanisms even when they know they *may* benefit from the investment. In this sense, performance needs would not affect organizational actions as strongly as government pressure does. Hence, I argue that:

> *H6: Government pressure is the strongest institutional predictor of detection-oriented SCSM mechanisms.*

So far my arguments have shown that government pressure is rather strong when it comes to SCS. However, government pressure cannot forcefully influence all aspects of organizational life. While governments may have a strong interest in preventing and detecting SCS breaches, they might not be very interested in the internal processes firms undertake to react to and/or recover from SCS breaches. The rationale lies in that governments do not care as much whether or not a firm can successfully survive a SCS breach. Consider the 2011 customer data loss at SONY. It was one of the largest data security breaches in history (see, http://news.sky.com/story/850949/hackers-steal-playstation-gamers-details). The costs associated with it could top $24 billion (Thorsen, 2011). But the U.S. government neither had the legitimacy nor the interests to push SONY to improve its IT security since it was more of a *business* crisis. Although some government officials voiced concern over the theft, no substantial action was taken (Thorsen, 2011). This SCS breach did not significantly jeopardize national security and therefore how SONY reacted on the aftermath of the disaster should not be a big concern

of the government. In this sense, the government would have diminishing interests in promoting reaction-oriented SCSM mechanisms compared to in promoting prevention and detection-oriented ones.

Customers, on the other hand, have significant concerns regarding a supplier's reaction ability. Supply chain continuity is very important to them. If a SCS breach disrupted the supply chain, the economic losses could be very high; buying firms may have to discount their products to comfort their unsatisfied customers due to delayed shipments; they may also suffer additional expenditures and administrative costs because of the need to tackle abnormal operations (e.g., shortage of supply). In some cases, there is little the buying firms can do to make up for the disruptions without impacting their own customers (Croxton, 2003). As such, customers have rather strong interest to assure supplier's reaction capability. They need their suppliers to solve SCS problems in a timely manner such that their own operations would not be significantly affected. Therefore, while somewhat negotiable, customer pressure is likely to be greater than the government pressure when it comes to reaction-oriented SCSM mechanisms (Williams et al., 2008).

Peer pressure is also potent as it relates to reaction. If firms cannot react to SCS breaches as well as their peers, they may gradually lose their ground against competitors. In extreme cases, their survival will come under question. As such, firms are prone to mimic their peers to implement reaction-oriented SCSM mechanisms in order to remain competitive. While both customer and peer pressure could be strong, I argue that customer pressure will generally be more salient than peer pressure for three reasons.

First, firms model after their peers to either match the services other peers have provided or reap benefits other firms have experienced. No matter which is the case, eventually firms may utilize what they gain from mimicking to win more customers. In this sense, competition among peers is customer-driven. Firms may naturally give customer requirements higher priority. When facing pressures from both the customers and the peers, they are likely to go with the customer pressure first. Second, customers are the sources of business. Outmaneuvering competitors is likely to help firms generate new customers. But the possibility of failing to capture new customers while defeating competitors still exists. Under such circumstances, satisfying (and thus keeping) existing customers is arguably a more pragmatic option for firms. Therefore, firms would give customer pressure more weight when compared to peer pressure. Finally, while negotiable, customer pressure is more coercive than peer pressure. Peer pressure is relatively less influential as rivals cannot force the focal firm to adopt a certain type of SCSM mechanisms.

The impact of normative pressure and performance pressure are unlikely to exceed customer pressure as well. Norms are naturally embedded in cultural traditions and developed as industry professionalism moves forward. For a new norm to gain popularity, pioneering firms would have to adopt the norms-to-be first and demonstrate that they indeed reap the benefits from the adoption of these norms. In addition, the benefits also need to be substantive so that the norms would be touted as "best strategies/practices" and thus be widely diffused and adopted by firms. In other words, norms-to-be need to be examined and scrutinized repeatedly before they can actually

become norms. Unlike norms, customer pressure is straight forward, immediate, and vigorous. Suppliers often do not have the option to assess whether the reaction-oriented SCSM mechanisms required by customers are beneficial or not before implementing them. These reaction-oriented SCSM mechanisms must be adopted no matter whether they are norms or not. As for performance pressure, reactive SCSM mechanisms generally serve as necessary responses to SCS disruptions. They are associated with the potential of fewer losses in case of a crisis. However, the realization of such potential depends on several factors such as the managerial efforts the firms invested. Maybe some firms can effectively grab the benefits of effective reaction to SCS breaches. But not all firms benefit fundamentally and equally. As the results of the case studies suggest, companies do not have reliable data to measure the performance gains from SCSM mechanisms. It would be difficult to persuade top managers to invest in reaction-oriented SCSM mechanisms solely based on expected financial outcomes. In this sense, customer pressure is likely to be more salient than performance pressure.

H7: Customer pressure is the strongest institutional predictor of reaction-oriented SCSM mechanisms.

Primarily building on similar reasons elaborated for the reaction-oriented SCSM mechanisms, I argue that customers are the strongest advocates for restorative SCSM mechanisms. As I indicated previously, governments have limited incentives to care about how firms recover from a SCS beach unless it is a catastrophic disaster like the 9/11 Terrorist Attacks. Peer pressure is pushing restoration ability to a high bar but such

effects are unlikely to exceed those from customers. In essence, outperforming peers is meant to win more customers. Customer pressure appears to have higher priority than peer pressure. Norms are important but they will not be as straight-forward and forceful as customer pressure because it takes time for norms to materialize. Finally, because of the low probability of catastrophic failures, it is hard to quantify the benefits of restoration-oriented SCSM mechanisms. Firms therefore may not have very strong momentum to improve restoration ability. Plus, they may believe that devastating breaches are every unlikely to happen to them and thereby lack interests in building up restoration ability. Nevertheless, customer pressure is rather salient. As the global supply chain manager from Electronics Savvy stated, "we have to work closely with our customers and fulfill their requirements." The company invests so aggressively in SCSM technologies which allow it to quickly assess recovered products (i.e., stolen products that are found) and determine whether or not these products can be shipped to customers on the aftermath of a SCS breach—it wants to recover from SCS breaches and satisfy customer demand as soon as possible. As such, customers are likely to have the strongest impact on restoration ability and push their suppliers to improve it.

H8: Customer pressure is the strongest institutional predictor of restoration-oriented SCSM mechanisms.

3.2.3 Moderation Effects—Boundary Conditions

Next, I articulate how two boundary conditions can shape the aforementioned relationships. *Shared supply chain security perception within an organization* (shared

SCS perception hereafter) refers to the extent to which employees perceive SCS breaches as potential threats to their firm. When the shared SCS perception is high, employees are likely to embrace the idea that there are considerable SCS threats that can impact the firm. The ability to successfully overcome SCS challenges is critical to firm survival. Therefore, emergency preparedness is likely to be widely endorsed by organizational members. There would be little resistance to changes for security purposes (i.e., the implementation of SCSM mechanisms). Employees are ready to perform necessary SCSM practices as their daily tasks (Autry and Bobbitt, 2008). Further, when employees believe that serious SCS breaches in their supply chain are imminent and even minor SCS breaches in the supply chain can be devastating to their firm, they will exert efforts to be more prepared to respond to those breaches because their jobs may be on the line. For example, IHS Global Insight's analysis (2009) shows that a disruption caused by SCS breaches of only one percent in total industry output in the United States would result in a loss of approximately 1,250 jobs directly tied to the air cargo shipping industry.

Therefore, when the shared SCS perception is high, putting SCS first becomes a sentiment widely shared within the organization. Employees may do more than required because they know SCS is critical to the firm and their own well-being. They would have the momentum to resolve SCS related problems. They are prone to be more active to identify SCS breaches as well. In some cases, they may even get proactively involved in SCSM mechanisms which allow them to keep a close eye not only on their own operations but also on the status of their supply chain partners. These ideas are consistent

with the findings from the Retail Guru case. The Retail Guru's procurement director of own brand products stated that "in our cases all of the world is adulterated. There is lots of food adulteration, economic adulteration…we (employees) must be prepared for it and we know a minor SCS issue can ruin all our hard work." To the Retail Guru employees, the company earns its current reputation through more than 100 year's hard work and the brand equity can be easily ruined by even minor SCS breaches. Therefore, the same director also stated that "we see the need to be able to know more about our supply chain, and much further down the supply chain than we have been before." The employees at Retail Guru are willing to go beyond normal requirements and proactively implement SCSM mechanisms owing to their shared SCS perception. Hence, I argue that shared SCS perception is likely to make firms more willing to conform to institutional drivers that call for better SCS.

H9: Shared SCS perception moderates the relationships between institutional pressures and SCSM mechanisms such that these relationships are strengthened at high levels of shared SCS perception.

Top management commitment for supply chain security management (top management commitment hereafter) refers to the extent to which top managers are active in managing supply chain security. High level of top management commitment suggests that top managers are actively engaged and demonstrate interest to become aware of the risks and consequences associated with SCS breaches. Top managers

usually assume a leadership role in SCSM when they sense that their supply chains are under threat. As Theo Fletcher, VP of import compliance & SCS for IBM, said:

> "We are all responsible for securing global supply chains…As a large, globally integrated enterprise doing business in more than 170 countries. IBM values a secure, compliant, and efficient supply chain. That's why at IBM supply chain security begins with executive commitment and extends throughout our global processes. It affects not only manufacturing, fulfillment, and logistics but also information management, procurement, and even employee education and human resources." (Theo Fletcher, VP of import compliance & SCS for IBM, 2007).

Several reasons are linking top management commitment to effective implementation of SCSM mechanism. First, the literature suggests that top management commitment is rather influential as top managers are in a unique position to have most impact on organizational behaviors (Finkelstein and Hambrick, 1996). Different organizational functions treat the tasks with clear top management commitment as more important and critical to the well-being of the firm when compared with others tasks (Raes et al., 2011). As a result, these functions (e.g., finance department which reviews the proposal of security investments) tend to be more responsive to those tasks. Multiple organizational functions would work collectively as a whole to fulfill the organizational goals, as opposed to act independently based on functional interests which are sometimes in conflict with organizational goals. In this sense, top management

commitment results in effective coordination in the implementation of SCSM mechanisms.

Second, strong top management commitment is expected to negate organizational resistance to change and thus lead to superior conversion effectiveness (Thong et al., 1996). A firm's existing internal structures often create inertia that impedes the implementation of new practices (Normann, 1977; Tushman and Romanelli, 1985). Such inertia results in disturbances in practice implementations, and can potentially nullify the intended positive effects of the implemented practices (Nord and Jermier, 1994). Nevertheless, top management commitment can lead employees away from denying changes and foster an acceptable attitude toward changes (Piderit, 2000). Because of the active involvement of top managers, the SCS efforts (the intent to implement SCSM mechanisms) are thus likely to better convert into productive outputs.

Third, because top managers are in charge of the use of organizational resources (Bouquet and Birkinshaw, 2008 a, b), supply chain managers may have more resources to accomplish jobs which have top management endorsement. As discussed in the Retail Guru case, the company devoted resources to hire a manager who exclusively deals with C-TPAT compliance. Finally, the unambiguous objectives established by the top managers put forward a clear guideline for supply chain managers and employees, which in turn make the implementation of SCSM mechanisms easier (Ahire and O'Shaughnessy, 1998). Target clarity allows supply chain managers to set appropriate goals and measure their achievements effectively. It also speeds up decision-making at lower operation levels and reduces the need of consulting superiors frequently. Clear

objectives designed at the top thus puts forward a shield against potential interventions which may slow down the implementation of SCSM mechanisms (Senge, 1990). Based on this reasoning, I propose that top management commitment will enhance the effects of institutional pressures on SCSM mechanisms:

> *H10: Top management commitment moderates the relationships between institutional pressures and SCSM mechanisms such that these relationships are strengthened at high levels of top management commitment.*

3.2.4 Differential Effects of SCSM Mechanisms

Relying on the principles of the human immune system, I further explore which classes of SCSM mechanisms are most conducive to a specific performance dimension. Human bodies do not rely on a *single simple* immune system that always works the same way every time the body is threatened by foreign invaders. In truth, the entire human immune system is made up of several different and highly complex sub-systems, each designed to protect the body in a different way. When an invasion takes place, all of the systems work together, but the particular sub-system that will predominate in any given case will depend on the nature of the invading viruses (or bacteria, etc.). In other words, one sub-system would play a prevailing role under some circumstances but just assume a supporting role under other circumstances.

The four classes of SCSM mechanisms operate similarly. They have their idiosyncratic "talent" in handling some specific aspects of a SCS threat. At the same time they have to be implemented together to solve the SCS issues because any single

class may not be capable to protect the supply chain. For example, detection-oriented mechanisms, as suggested by the name, are designed to detect SCS threats and gaps. Compared to other classes of mechanisms, their role is primarily monitoring the supply chain so that firms can be warned when SCS problems surface. However, detection alone cannot ensure the security of the supply chain. At least, effective reaction must follow. In this sense, the four classes of routines are naturally bounded and all are needed in combating SCS breaches.

In this effort, their impact on performance is diverse partly due to their different orientation as well as the multidimensional essence of supply chain performance. As I mentioned in the previous chapter, SCSM mechanisms may lead to not only better SCS performance (e.g., lower supply chain security risk, low levels of theft, less potential losses due to security problems) but also to a number of collateral benefits which are essentially different performance dimensions. These dimensions encompass supply chain cost performance, supply chain responsiveness, supply chain resilience, and supply chain visibility among others. *Supply chain cost performance* measures the extent to which the adoption of SCSM mechanisms results in reductions in overall cost, excess inventory, insurance premiums, or costs associated with SCS disruptions. *Supply chain responsiveness* measures the extent to which firms gain an improved ability for early intervention, faster response to problems, and efficient problem resolution. *Supply chain resilience* is operationalized as the extent to which firms are capable of withstanding serious SCS breaches and capable of restoring normal operations. Finally, *supply chain*

visibility denotes the extent to which firms obtain better access to supply chain data such as timely shipping information or tracking the location of cargo at any given time.

Like each sub-systems of the human immune system would dominate the battle against antigens given certain conditions, each class of SCSM mechanisms is likely to have differential effects on performance dimensions. They may have rather strong effects on some dimensions but weak impacts on others. Given the fact that few firms can implement all desirable SCSM mechanisms at a time, it is quite relevant to understand which class of mechanisms should be implemented to improve a specific performance dimension.

3.2.4.1 Prevention-oriented SCSM Mechanisms→Supply Chain Performance

As far as the preventative mechanisms are concerned, I argue that (1) they will positively affect supply chain performance dimensions and (2) they will have stronger effects on supply chain security performance than on other performance dimensions. Prevention-oriented mechanisms target breach avoidance. The human skin is a fair analogy to preventative practices. Skin is a formidable barrier that prevents infection. Not only does the skin function as an impressive physical obstacle like the walls of a castle, it is also an unfriendly environment for many microbes. The skin is slightly acidic and some areas are quite dry; neither conditions suit many microbes, which makes it a deterrent to bacteria. In addition, it secrets sebum which helps coat the skin and block out antigens, effectively handing out a "No Trespassing" sign for bacteria. Because of those "actions", the skin can block 95% of invading antigens (Parham, 2005). Without it,

the human immune system would have to deal with many more challenges and is likely to be fatigued easily. In this sense, the skin absorbs a significant burden and provides other human immune system components the opportunity to focus their effects on a small number of antigens.

Similarly, when firms have high prevention ability, they will endure lower levels of pain because many of the breaches are averted to begin with. Naturally, supply chain security risk is lowered and therefore better SCS performance can be achieved. The need for these firms to amass excessive reaction and restoration mechanisms would be relatively low. In other words, firms do not need to invest aggressively in the other classes, if breaches can be averted. Thus, firms can minimize the cost to address extensive SCS breaches. A typical example of such savings is the cost associated with expediting freight on the aftermath of a disaster. In addition, high prevention ability makes the supply chain more stable. In this sense, firms along the supply chain may effectively predict potential disruptions and thus respond to these abnormal conditions swiftly. Further, when a sizable number of potential SCS breaches are prevented, the variety of SCS breaches a firm will face would become narrower. This makes it possible for firms to amass pre-planned activities in order to survive SCS breaches. Finally, to effectively avert SCS breaches, firms need to first identify the potential sources of SCS breaches in their supply chains. As such, a number of prevention-oriented mechanisms can be attributed as detective purposes as well, which leads to improved supply chain visibility. Hence, I propose:

H11a: Prevention-oriented SCSM mechanisms are positively associated with supply chain security performance, supply chain cost performance, supply chain responsiveness, supply chain resilience, and supply chain visibility.

Following the logic applied in the TQM literature, it is reasonable to argue that prevention-oriented SCSM mechanisms have rather strong effects on supply chain security performance (Lee and Whang, 2005). For example, firms with pretention-oriented practices collect relevant data, analyze and identify potential SCS breaches, and then design processes and train employees to achieve zero SCS breaches. These actions reduce the probability that potential SCS threats are under-identified or ignored. For instance, employees are involved in detecting theft because they are trained to do so. SCS breaches such as smuggling and counterfeit products can be minimized as there is a clear chain of command to counteract these issues. Both internal and external SCS failures can be diminished and therefore better SCS would be achieved.

While prevention ability is conducive to SCS performance, its effects on other performance dimensions would be relatively marginal when compared to its effects on SCS performance. Prevention mechanisms, such as supplier education about SCS, are unlikely to reveal a strong direct effect on cost performance. Cost reduction is primarily achieved because SCS breaches are averted. Further, in order to effectively prevent SCS breaches, firms may attempt to reduce the complexity of its supply chain by nurturing sturdy relationship with only a small number of suppliers. However, such strategy renders a focal firm's ability to respond to and recover from SCS breaches more

ineffective because it will have fewer alternative suppliers to select from at times of crises. Moreover, although in order to prevent SCS breaches firms need to uncover them first, the effect of prevention-oriented SCSM mechanisms on supply chain visibility is unlikely to be stronger than their effect on SCS performance. While detection activities are an imperative part of the SCS breach prevention system, some preventive mechanisms, such as selection of qualified suppliers, would prevent security incidents but not increase supply chain visibility. Hence,

> *H11b: The effects of prevention-oriented SCSM mechanisms on supply chain security performance will be stronger than those on supply chain cost performance, supply chain responsiveness, supply chain resilience, and supply chain visibility.*

3.2.4.2 Detection-oriented SCSM Mechanisms→Supply Chain Performance

Firms use sophisticated technologies or other processes to detect whether or not their containers have been compromised during shipment. For instance, firms utilize live time tracking of cargo offered by RFID techniques. They also actively monitor the loading/unloading processes to identify potential SCS breaches. Such actions allow firms to synthesize information regarding supply chain operations in real time and achieve better SCS. Besides the installation of the state-of-the-art equipment, the detection-oriented SCSM mechanisms also involve practices such as conducting periodic SCS assessments of suppliers across tiers. Such mechanisms enable organizations to detect "near" SCS breaches and notify supply chain partners across tiers if the supply chain is

threatened. It helps to establish an effective and clear communication channel among supply chain partners, leading to high supply chain visibility which eventually results in better SCS performance.

On top of SCS performance and supply chain visibility, detection-oriented SCSM mechanisms contribute to other performance dimensions as well. Such mechanisms are conducive to superior cost performance. Many detection-oriented practices can be used not only to boost SCS performance but also to enhance operational efficiency. For example, the ability to track and trace cargo shipments in real time permits firms to adjust their manufacturing plans in a way such that the costs associated with excessive waiting time and redundant inventory can be minimized. In addition, early detection permits firms to undertake actions systematically and thus enhances effective reaction to emerging SCS breaches. High detection capability also makes quick resolution of security problems possible and thus increases the possibility that firms can withstand SCS crises. In other words, the implementation of detection-oriented SCSM mechanisms would promote supply chain responsiveness and supply chain resilience. Hence,

> *H12a: Detection-oriented SCSM mechanisms are positively associated with supply chain security performance, supply chain cost performance, supply chain responsiveness, supply chain resilience, and supply chain visibility.*

Arguably, successful detection is a prerequisite of many other SCS related practices. Only when SCS breaches are detected can other responses be carried out. The treatment of cancer is a good example to illustrate the instrumental role of detection-

oriented SCSM mechanisms. When normal cells turn into cancer cells, the detection mechanisms of the human immune system would cause some of the tumor antigens on their surface to change (Schindler, 1991). These new or altered antigens flag the immune system defenders, including lymphocyte-T cells, natural killer cells, and macrophages, to conduct the foremost responses to infectious cancer cells. Since quite a few types of cancer can only be cured or contained when they are diagnosed at early stages (Nourse, 1982), failure of early detection would imply that human life is compromised.

In the context of SCSM, detection-oriented SCSM mechanisms play a similar role as the cancer treatment example demonstrates. They provide synthesized information for other SCSM mechanisms to effectively function. The information detection-oriented mechanisms offer enables multiple functional departments within an organization to coordinate their efforts to react to SCS breaches and thus reduce operational costs. Even when the type of SCS breaches that is identified cannot be fully addressed immediately, effective detection still allows companies to develop a sophisticated treatment plan than may mitigate the impact of the SCS breaches and sustain operations. In this sense, detection ability is the foundation for other SCSM mechanisms. Nonetheless, except for supply chain visibility, it affects other performance dimensions only indirectly and instrumentally by delivering timely information. Therefore, I propose:

> *H12b: The effects of detection-oriented SCSM mechanisms on supply chain visibility will be stronger than those on supply chain cost performance, supply chain responsiveness, supply chain resilience, and supply chain visibility.*

3.2.4.3 Reaction-oriented SCSM Mechanisms→Supply Chain Performance

Reaction-oriented SCSM mechanisms involve activities that are designed as a response to SCS breaches. This class of SCSM mechanisms aims to correct and remove SCS perils. Typical reactive mechanisms include but are not limited to developing protocols for communication when a crisis arises, delegating authority so that teams/individuals can take necessary action in case of a crisis, and cross-training employees as a mechanism to deal with potential SCS breaches. These mechanisms ensure firms can launch an early intervention in case of a SCS breach and make efficient and fast problem resolution possible. In other words, reactive SCSM mechanisms lead to better SCS performance and supply chain responsiveness.

Rapid reaction results in better cost performance as well because a quick response may contain the magnitude of a SCS breach and reduce potential losses. It also gives the firm an immediate and probably important taste of what the problem is and how the firm can resolve it. Consequently, the damage due to a SCS breach can be minimized. Effective reaction also conjures successful restoration. Firms employ several strategies and practices at the product design and manufacturing stages in order to improve efficient problem resolution. For instance, many manufacturers use interchangeable or generic parts for their major product lines and negotiate flexible capacity contracts with suppliers. By doing so, they build flexibility in their supply chains and can quickly assume normal operations in case of a security crisis. Finally, some firms go beyond "common" reaction activities. They designate a quick reaction force as first respondents in case of a crisis and equip those employees with a specific

crisis management room. Such action keeps all relevant individuals/parties better informed about the status of the supply chain and makes the details of SCS breaches more visible to managers. Taken together, I propose:

> *H13a: Reaction-oriented SCSM mechanisms are positively associated with supply chain security performance, supply chain cost performance, supply chain responsiveness, supply chain resilience, and supply chain visibility.*

While reaction SCSM mechanisms are postulated to positively affect supply chain performance, their effects on these performance dimensions could be different in terms of magnitude of impact. Specifically, I argue that the effect of reaction mechanisms on supply chain responsiveness would be stronger than their effects on other four performance dimensions. This idea can be better explained by looking at the example of lymphocyte-T cell in the human immune system. Lymphocyte-T cells are a special group of small white cells that directly participate in the immune defense (Schindler, 1991). While they can detect viruses through the receptors on their surface, the principle role played by Lymphocyte-T cells is to eliminate pathogens (Schwartz, 1980). Indeed, they are evolved to be able to detect viruses without the help of other cells simply because they need to effectively destroy these viruses: if the lymphocyte-T cells cannot effectively engaged in pathogen elimination, the human life would likely come under question (Schwartz, 1980). Similarly, reaction-oriented SCSM mechanisms are, by their very nature, designed to facility fast responses to SCS breaches. The reactive mechanisms may advance other four performance measures primarily because

they enable firms to react to SCS breaches more effectively. In this sense, the effects of reaction mechanisms on other performance dimensions are essentially "by-products" of better supply chain responsiveness. As such, I propose:

> *H13b: The effects of reaction-oriented SCSM mechanisms on supply chain responsiveness will be stronger than those on supply chain security performance, supply chain cost performance, supply chain resilience, and supply chain visibility.*

3.2.4.4 Restoration-oriented SCSM Mechanisms→Supply Chain Performance

Even when firms have high reaction ability to respond to SCS disruptions, they cannot overlook the need for restoration-oriented SCSM mechanisms (Sheffi, 2005). They have to quickly resume normal operations because any breakdown caused by SCS breaches can be very costly. For example, as the managers I interviewed suggested, a SCS related crisis may compel their firm to adjust their pre-set manufacturing plans which can significantly affect material supplies and inventory, product lead time, and product quality. In an endeavor to deal with such a crisis, firms institute disaster recovery plans (Rice and Spayd, 2005). For instance, they maintain strategic inventories (both raw material and machinery) (Peleg-Gillai and Bhat, 2006). Their strategy also specifies the selective use of slack resources in anticipation of SCS disruptions (Peleg-Gillai and Bhat, 2006). All these strategies and practices enhance the ability of firms to withstand a SCS disruption and reinstate operations on the aftermath of a disruption, leading to better supply chain resilience.

Besides supply chain resilience, restoration-oriented SCSM mechanisms are related to other performance dimensions as well. As the results of the case studies reveal, restoration-oriented mechanisms overlap with reaction-oriented mechanisms. For instance, restorative practices, such as the development of alternative material sources in case of a supply chain disruption, are also helpful to build supply chain responsiveness and thus enhance SCS performance. Quick responses, in turn, cut operational costs and ease the need to tackle abnormal conditions caused by SCS disruptions because these abnormal conditions are unlikely to be lasting when quick responses are standing by. In addition, restorative mechanisms could help firms move to a new and better status after major SCS disruptions because these SCS disruptions provide opportunities for effective changes that otherwise would have faced strong resistance (Thong et al., 1996). In this sense, restoration-oriented mechanisms inform managers about the status of their supply chain and potentially make hidden supply chain problems more visible to the organization leaders.

H14a: Restoration-oriented SCSM mechanisms are positively associated with supply chain security performance, supply chain cost performance, supply chain responsiveness, supply chain resilience, and supply chain visibility.

As far as the differential effect is concerned, restorative mechanisms are likely to exhibit a stronger effect on supply chain resilience than on other performance dimensions. The reason is that restoration-oriented mechanisms are "post-hoc" practices that generally take place on the aftermath of a SCS breach. While they help a firm to

restore normal operations, their "post-hoc" nature determines that they will have little impact on SCS breaches *a priori*. Firms should not expect to utilize restorative mechanisms to significantly reduce the number of SCS breaches, effectively facilitate early intervention, or effectively improve supply chain visibility. Unsurprisingly, the effect of restoration-oriented mechanisms on cost performance is also unlikely to be superior. While many people believe that restorative mechanisms can reduce overall cost when considered as a whole (Peleg-Gillai and Bhat, 2006; Rice and Spayd, 2005), even more people would probably also agree that some restorative practices, such as maintaining strategic inventory, actually increase operational cost (Sheffi, 2005; Voss et al., 2009b). Taken together, I propose:

> *H14b: The effect of restoration-oriented SCSM mechanisms on supply chain resilience will be stronger than those on supply chain security performance, supply chain cost performance, supply chain responsiveness, and supply chain visibility.*

3.2.5 Impact of SCSM Mechanisms as A Portfolio

While it is clear that all four classes of SCSM mechanisms boost firm performance respectively, it remains unclear how the four classes may potentially interact to enhance performance. The presumption is that if the four classes function collaboratively as many sub systems in the human immune system do, then theoretically the firms with *uniform-high* SCSM ability (i.e., they score high in all four classes, uniform-high hereafter) would perform better than other firms. In reality, however, do

these firms actually outperform their peers with *mixed* (i.e., firms that score high in at least one of the classes but not all classes, mixed hereafter) or *uniform-low* (i.e., firms that, for whatever reasons, score low in all classes, uniform-low hereafter) SCSM ability?

The answer to this question is important as it allows us to look at the impact of SCSM mechanisms on firm performance from a different perspective. For instance, what is the value of implementing other classes of SCSM mechanisms if the most essential class is already implemented to improve the most critical performance dimension that a firm desires? Can the stimulus generated by adopting/implementing additional strategies and practices in other classes justify the investment? For example, two firms may have implemented detection-oriented SCSM mechanisms to the same level. According to my previous arguments, one can expect that the two firms may gain similarly in terms of supply chain visibility. Yet, the supply chain visibility of one firm could be higher than the other firm's simply because it implements more mechanisms in other classes and those mechanisms interact with detection practices in a way such that the compound effect on supply chain visibility becomes stronger.

The human immune system is again a fair analog to help us understand this phenomenon. Many different proteins and antibodies in the human immune system need to work together to achieve their maximal effects. These different forms of proteins and antibodies, while have specific functions to perform, become more effective when working as an integrated entity to destroy invading antigens. The example of complement proteins presents an exemplar case. Complement plays a remarkable role in

the human immune system. Complements are a group of special protein molecules. They have been given the odd name of *complement* because, when they were first discovered, it was mistakenly assumed their job was to help or assist antibodies rather than destroy invading antigens. Scientists later learned that it was exactly backward. It is the antibodies that help or assist the complement molecules to fit together and transform them into a powerful bacteria-killer.

There are at least nine different forms of molecules that have been found in this particular family of proteins. They are somewhat "harmless" to invading bacteria individually. Imagine that a powerful rifle is lying on the table as separate pieces. Any one, or two of the pieces, taken alone or together, are perfectly harmless. All nine pieces are literally harmless if they are lying separately on the table. It is only when all those pieces have been assembled in the right way, in the right order, that the rifle becomes a commanding weapon. The nine complement proteins work much like the pieces of the rifle. They are not as effective as the "assembled" complement complex when working separately.

The four classes of SCSM mechanisms work alike to those complement molecules and their assisting antibodies. Each class functions like an individual form of complement molecule. They positively affect SCS performance and have differential effects on other performance dimensions. However, the optimal security/supply chain performance may not be achieved if the implementation of these classes of SCSM mechanisms is not aligned. For example, lack of prevention-oriented SCSM mechanisms may impose too much pressure on the focal firm to effectively detect and react to SCS

breaches. Likewise, lack of reaction-oriented ability forces the focal firm to invest heavily in prevention and detection so that they can identify SCS breaches and resolve them at the early stage. None of the four classes of SCSM mechanisms alone can ensure the security of the supply chain. In addition, the four classes are likely to enhance each other. For instance, in order to prevent SCS breaches, firms need to have high detection ability so that potential security glitches will be identified beforehand. As such, the deployment of preventive SCSM mechanisms would positively affect the implementation of detective SCSM mechanisms. In a similar vein, the reaction class and the restoration class are interacting in a positive way. Effective reaction is arguably the first step of restoration. In order to recover from a SCS disruption, firms have to react to it first. In this sense, uniform-high firms would outperform uniform-low or mixed firms along different performance dimensions.

> *H15a: Uniform-high firms outperform uniform-low/mixed firms on supply chain security performance, supply chain cost performance, supply chain responsiveness, supply chain resilience, and supply chain visibility.*

Yet, the observations from the human immune system also warn us that applying an excessive effort to fight antigens is not necessarily a good thing for the human body. Consider the complements as an example. Once the complement complex "riffle" has been correctly assembled, it is not very safe to have around. For example, it may accidentally go off or be fired in the wrong direction instead of at its chosen target. Indeed, experiments show that the complement complex does not really care which *cell*

it attacks (Nourse, 1982). The human immune system must send the right "command" to the bacteria-killer so that self-cells won't be killed mistakenly (Nourse, 1982). A similar example relates to allergies. People are allergic not because their human immune system is not working but because their system is working too hard (Nourse, 1982; Schindler, 1991). The immune responses are triggered by false alarms. Normally harmless substances, such as grass pollen or house dust, are perceived as threats and are attacked by the human immune system. Consequently, the human beings have to suffer unnecessary pains.

The lessons of excessive human immune responses can be applied to the SCSM system as well. Additional inspections for detection purposes may slow down the movement of products and thus hurt supply chain responsiveness. These inspections also increase operational costs and administrative costs. In addition, when a firm decides to implement all four classes of practices at a high level, more coordination among different parties and organization functions is required. Effective management of the implementation of the four classes is not an easy task (Closs and McGarrell, 2004) and ineffective coordination may cause problems which can negate the rents generated by implementing these classes. For example, as discussed in the case studies, Retail Guru faces cargo delays every month due to its strict security screening policy. An alternative view would thus suggest that, while the SCS performance is improved, other performance dimensions could be compromised when firms invest aggressively in all four classes.

Therefore, I propose two competing hypotheses against H15a:

H15b: Uniform-high firms outperform uniform-low firms/mixed firms on supply chain security performance.

H15c: Uniform-high firms perform at least as well as uniform-low/mixed firms on supply chain cost performance, supply chain responsiveness, supply chain resilience, and supply chain visibility.

CHAPTER IV

RESEARCH METHODS AND RESULTS

The previous chapter laid out a set of hypotheses. To test these hypotheses, I collected data and performed respective analyses.

4.1 Research Design and Research Methods

A survey-based approach was employed for this dissertation. In addition, this work has benefited greatly from four case studies from diverse industries. Since the institutional theory and the tenets of the human immune system used in the present study are well developed, this study is essentially testing a variance theory model based on mature theories. Thus, the data collection methods can be primarily quantitative (Edmondson and McManus, 2007). Survey is an attractive method of data collection as it has the potential to afford the researcher a large amount of information that can be analyzed to test relationships between two or more variables (Miller, 1991). Survey is also attractive owing to its ability to generate generous amounts of information from a large sample of subjects under study (Kerlinger, 1986). This presents the opportunity to increase the generalizability of findings (Dobrzykowski et al., 2010).

Nevertheless, the survey-based method faces challenges. Currently, a major challenge faced by researchers when using the survey method is low response rate. This is a serious concern for researchers because response rate is critical to the generalizability of a study's findings (Malhotra and Grover, 1998). Observations show

that the response rate in academic studies has declined steadily in recent decades (Baruch, 1999). This challenge has been exacerbated in the context of SCS owing to the sensitivity of the topic: SCS information, measures, and strategies are considered confidential and the data are not publicly available (Williams et al., 2009b).

Recognizing this challenge, I subscribe to the recommendations of Erdos (1970) and Blankenship and Breen (1992) to improve the response rate to the survey. The survey had a simple appearance and was designed to be easily read with black letters that are highly visible. The study also implemented the use of incentives, which is recommended by Erdos (1970). Benchmark reports were prepared for participants free-of-charge. In addition, two Amazon Kindle Fire tablets were granted to two individual respondents randomly selected from the sample pool. To further improve response rate, I administrated a personalized notice before sending out the survey. Therefore, when possible, phone calls were placed to potential respondents, not only explaining the purpose of this study and assuring the anonymity, but also informing the importance of the study. It was anticipated that this action also helped to mitigate another threat to survey-based research: "that the questionnaire may be answered by someone other than the addressee (Erdos, 1970, p. 125)."

Paralleled with the survey administration, I conducted four field studies based on a qualitative approach. There are three reasons why the qualitative approach is important and necessary to this study. First, adopting multiple methods is an effective way to enhance the research validity. Ethnographic interviews help discover what is meant by specific concepts or whether there is a misunderstanding between practitioners and

academics (Flynn, Sakakibara, Schroeder, Bates, & Flynn, 1990). The interviews are thus critical to the present study as they helped to define concepts, such as supply chain security, more effectively. Second, these interviews afforded me the opportunity to refine the proposed hypotheses. The four companies reside in different industries (i.e., food and beverage, IT & electronics, and high technology manufacturing) and are all sensitive to SCS breaches, though their sensitivity varied. Their understanding of SCS is invaluable and allows me to fine-tune/refine the theoretical relationships proposed in chapter III. A multiple-case design was adopted in order to fully extract the information from the four field visits. Supply chain managers from these companies were interviewed. Besides the interviews, information was collected from archival data (e.g., documents, historical records, and organizational charts) and observations (e.g., plant tour, attendance at meetings). Third, the qualitative approach is utilized because of the need to verify the content domain of the four classes of SCSM mechanisms proposed in chapter II. The four case studies involve interviews with practitioners who were familiar with their firms' SCS affairs. These case studies were used to determine the content domain of the four classes of SCSM mechanisms respectively. Establishing the content domain of each construct is vital for content validity.

4.2 Survey Data Collection

4.2.1 Pre-testing

In an endeavor to further refine the measurement scales, a pre-testing was conducted. A total of 15 academics and practitioners were interviewed following the

rigorous instrument development approach proposed by Swink and Song (2007). The participating academics were considered experts in the field of supply chain management and had published papers in leading academic journals. Each participating practitioner had many years of experience in manufacturing firms, and especially in the purchasing area.

The overall theoretical model was first introduced during the interviews. The experts were then solicited for their opinions regarding the model and the construct definitions. The author also probed them to share any relevant experiences. The subjects' perceptions with respect to the relevance and completeness of the measurement scales were solicited as well. Each expert's feedback was analyzed to assure consistency between construct definition and operationalization. The pre-testing resulted in minor changes of the survey questionnaire.

4.2.2 Sample and Procedures

The final questionnaire included survey items which were based on a seven point Likert type scale to obtain necessary variance, where 1: Not at all and 7: A great deal. The target population is primarily composed of manufacturing firms operating in the United States and Italy. The questionnaire was translated and back-translated into Italian in line with the procedures proposed by Brislin (1980). A group of operation managers from three large Italian organizations were also involved to increase clarity and avoid misunderstanding of survey questions. High ranking supply chain executives of targeted firms were asked to respond to the questionnaire because they were the people who had

the knowledge of supply chain strategies, manufacturing practices, and respective performance.

Due to the sensitivity of the topic and subsequently the potential low response rate, we solicited endorsement from leading professional SCM organizations. The U.S. based Council of Supply Chain Management Professionals (CSCMP) agreed to support this research. The cover letter to U.S. respondents was signed by the CSCMP director of public relations to encourage participation. The potential U.S. respondents of the survey were selected from the member list provided by CSCMP. Members of the Institute for Supply Management (ISM) were also targeted. Two academics with extensive experience in O&SCM selected 1,855 potential respondents from an initial list of more than 6,000 supply chain/logistics/operations professionals. They sought the participation of high- and middle-level executives because (1) they would possess knowledge of the SCSM mechanisms and, (2) they would have sound knowledge of the institutional environment where their firms reside. As mentioned before, when possible, I provided advanced personalized notice by phone calls before sending the potential respondents the survey. Roughly, 400 phone calls were placed. The initial list of potential respondents from Italy was obtained from Associazione Italiana Acquisti e Supply Management (ADACI), the Italian association of Supply Chain Managers. My Italian colleague selected 1,125 potential respondents using the same criteria used for the U.S. sample. The Italian researcher also provided advanced personalized notice by phone calls whenever possible.

The target population was composed primarily of manufacturing firms for both countries. We selected firms from various industries with different firm sizes because this allowed us to generalize the research findings. The final survey was administrated in both countries via both mailings and emails (i.e., mixed-mode survey, Dillman, Smyth, and Christian, 2009), along with a cover letter explaining the study's purpose and assuring the anonymity of each participating firm. The mixed-mode survey allows potential respondents to choose the communication medium they like and may potentially improve their willingness to respond to the survey (Dillman et al., 2009).

The data-collection process yielded 261 responses from the U.S. with a response rate of 14.1% (261/1855). Responses from 32 companies were not utilized because they did not provide sufficient information for meaningful analysis. This led to 229 usable responses, with an effective response rate of 12.3% (229/1855). As for the Italian sample, complete responses from 233 companies were collected with an effective response rate of 20.7% (223/1125). Both effective response rates compared favorably with other survey studies in SCS research (e.g., Williams et al., 2009b). The overall effective response rate is 15.5% (462/2980).

In order to assess that the samples obtained from the two countries were comparable, I tested for measurement invariance following the procedures recommended by Koufteros and Marcoulides (2006). The equivalence of measures was assessed using confirmatory factor analysis via Mplus version 6.2.1. For each theoretical construct, a base model (model 1) was first specified without adding any constraints on it. Good model fit was necessary to establish that the number of factors is the same across

countries. Then a second model (model 2) was specified where the factor loadings between the U.S. group and the Italian group were constrained to be equal. A non-significant difference between the chi-square values of the two models (model 1 and model 2) suggests measurement invariance. The chi-square differences for all theoretical constructs were non-significant ($p>0.05$), suggesting that the measurement items are invariant across the two considered groups. Therefore, I combined the two samples to test hypotheses.

Note that when the interest is to assess the difference of path coefficients between groups, further assessment for equal measurement errors, equal correlations, and equal structural coefficients are required (Koufteros and Marcoulides, 2006). Nevertheless, a test of equal loading is sufficient for examining measurement invariance between two samples collected using the same instrument (Kirkman et al., 2009).

4.2.3 Sample Characteristics

Due to the sensitivity of the subject matter, 87 firms opted not to provide any information regarding their industry affiliation or other identifying information and thus I was unable to classify these firms into industry clusters. Nevertheless, I divided the remaining 384 firms into six industry sectors which were widely used for research purposes in the O&SCM literature (e.g., Villena et al., 2009): Food & Beverage, Chemical & Pharmaceutical, Automotive, IT & Electronics, Other Manufacturing, and others.

Table 12 displays the sample characteristics of participating firms in terms of number of employees, annual sales, respondent position, and industry membership.

Table 12. Sample characteristics

Firms by Size:			
Number of employees		Frequency	Percentage
Less than 100		65	17%
100 to 499		100	26%
500 to 999		35	9%
1,000 to 9,999		84	22%
Over 10,000		100	26%
	Total	384	100%
Annual sales		Frequency	Percentage
Less than 10 million		59	15%
10 to 99.9 million		84	22%
100 to 999.9 million		92	24%
1 to 10 billion		88	23%
More than 10 billion		61	16%
	Total	384	100%
Respondents by position:			
Position		Frequency	Percentage
President/Chairman		16	4%
CEO/COO		38	10%
Director		100	26%
Managers		211	55%
Others		19	5%
	Total	384	100%
Firms by industry membership:			
Industry		Frequency	Percentage
Food		38	10%
Chemical & Pharmaceutical		56	15%
Automotive		23	6%
IT & Electronics		30	8%
Other Manufacturing		160	42%
Others		77	20%
	Total	384	100%

Firm size was measured by two relevant indices: number of employees and annual sales (Pagell et al., 2004; Villena et al., 2009). As shown in table 12, about 57% of firms in the sample were medium to large firms and had more than 500 employees (Wu and Choi, 2005). In terms of sales, 63% of firms had $100 million or more in annual sales. As far as management position is concerned, 95% of respondents held at least a managerial level position in their company. Typical titles of respondents were vice president of supply chain, supply chain security manager, and procurement manager. About 80% of participating firms were from manufacturing, which was not surprising as the target population was primarily manufacturing firms.

4.3 Measurement Scales Operationalization

4.3.1 Institutional Pressures

The first group of variables captures different institutional antecedents of SCSM mechanisms. The institutional theory is a mature theory with well-development constructs (Heugens and Lander, 2009). Thus, this dissertation adapted existing manifest variables of institutional pressures from a recent literature review of the institutional theory research by Heugens and Lander (2009) and several classic studies (e.g., DiMaggio and Powell, 1983; Scott, 2001). Minor changes were made to ensure the manifest variables were well accommodated with the research context. Specifically, five institutional pressures were included: government, customer, peer, normative, and performance pressure. Measurement items for institutional pressures are listed in table 13 along with their factor loadings based on exploratory factor analysis, extracting

factors using *principal axis factoring* coupled with *direct oblimin* specification for rotation. Using the eigen-value-greater-than-one criterion, I found only one factor emerged from each group.

Table 13. Measurement items for institutional pressures

	Factor loading
Government pressure: eigen value = 2.437, percentage of variance explained = 60.93%	
There is definite pressure from our government to meet security standards	.83
We will receive significant benefits if we adopt security standards prescribed by our government	.70
Our government takes an active role on security matters	.80
We cannot take security lightly as our government will hold us accountable	.78
Customer pressure: eigen value = 2.70, percentage of variance explained = 75.45%	
Our customers pressure us to do better on security	.78
We have to meet standards for security as our customers are demanding us to do so	.88
Our customers hold us accountable for security	.80
Our customers are monitoring our security practices/performance	.83
Peer pressure: eigen value = 1.89, percentage of variance explained = 74.63%	
We feel that we have to adopt security practices because everybody else does it	.66
We feel the pressure to adopt security practices as most of our peers have done so	.82
We feel that we have to adopt security practices as most of our rivals have done so	.88
Normative pressure: eigen value = 1.84, percentage of variance explained = 72.99%	
We employ risk & security practices in order to conform to professional norms	.82
We implement supply chain security practices to conform to industry norms	.89
We employ supply chain security practices to conform to cultural norms	.61
Performance pressure: eigen value = 2.23, percentage of variance explained = 82.88%	
We implement security practices because they can improve performance	.86
We implement security practices because they can lead to competitive advantage	.86
We implement security practices because we see operational benefits	.87

4.3.2 Four Classes of SCSM Mechanisms

The second group of variables involves constructs that capture the four classes of SCSM mechanisms. The present study first operationalizes various SCSM measures based on prior SCS research (e.g., Lee and Whang, 2005; Mena et al., 2009; Sheffi 2001,

2005; Williams et al. 2009a, 2009b), industry-oriented reports (the IBM special report series for supply chain security), and a number of SCS initiatives/programs developed by either governments or international organizations (e.g., C-TPAT, AEO, etc.). A large number of SCSM measures (100 measures) were selected, representing a rather broad spectrum of strategies and practices firms implemented to improve SCS and mitigate risk. Then these measures were categorized into four groups to capture the four classes of SCSM mechanisms proposed in the taxonomy.

There are a few techniques that can be deployed to categorize SCSM mechanisms. For example, exploratory factor analysis can be used to find out how many SCSM mechanism clusters "naturally" emerge or underlie the data. Yet, exploratory factor analysis exhibited several trivial factors or generated several cross-loadings that were hard to interpret even when different extraction/rotation methods and robust estimators were used. This is understandable and can be explained by the immunology literature. When discussing how the human immune system operates, immunology authors state that a particular lymphocyte cell can serve as both a detection and reaction mechanism (Parham, 2005). Similarly, security personnel who detect a SCS breach could also be the first ones who react to that security breach. In this sense, a security-oriented mechanism may be ascribed to more than one class of mechanisms in the proposed taxonomy. In addition, the SCSM mechanisms may cross-fertilize each other as well. For example, high detection ability grants more time for effective reaction. As a result, purely data-driven clustering techniques, such as exploratory factor analysis, may not yield useful results. Thus, this study opted first to incorporate subjective clustering

methods to tackle this issue. The purpose of the subjective clustering method is to capture the extent of agreement among people in how they employ concepts, in our case how people treat a SCSM mechanism as preventive, detective, reactive, or restorative.

The classic Q-Sort method (Stephenson, 1953) which has been widely used in the social sciences research was employed in this dissertation. The use of ranking, rather than rating numerically in Q-Sort, is meant to acknowledge that people think about ideas in relation to other ideas, rather than in isolation. The key concern with this method is that the Q-sorter (the individual who actually does the sorting) may frequently experience doubt, indecision, and despair over the actions requested of him or her. Nevertheless, Frank (1956) shows that the behavior of the Q-sorter is highly repeatable: test-retest reliabilities range from .93 to .97 in his study. The skepticism over this type of reliability is unwarranted (Thomas and Baas, 1992).

Forced Q-sorting was used (i.e., the number of classes was constrained to be five, including one N/A class for items that the Q-sorters believe do not belong to any of the four classes) because (1) unforced Q-sorting provides lower discrimination and suffers from the Barnum effect (Meehl, 1956); (2) the unforced Q-sorting is not more reliable than the forced one (Block, 1961); and finally (3) the five-class setting is consistent with the taxonomy proposed in the second chapter.

Three O&SCM professors and three practitioners who had extensive experience in supply chain management and were cognizant of the SCS issues served as the Q-sorters. Since the interest of the Q-sort method is the extent to which viewpoints are converging or not, the number of sorters, fundamental to most social research, is

rendered relatively unimportant (Brown, 1980). A Q methodological process requires only a limited number of Q-sorters. The reason for this is that increasing the number of Q-sorters will introduce unnecessary variation and potentially taint the Q-sorting results. As Brown put it, "…all that is required are enough subjects to establish the existence of a factor for purposes of comparing one factor with another" (Brown 1980, p. 201). In addition, the sorters are not randomly drawn. This is because Q-sorters are drawn from a sample of judges who are knowledgeable about and theoretically relevant to the problem under investigation (Brown, 1980, 1993).

The objectivity of the Q-sorting process should not be a concern for this study. One of the most important characteristics of Q-sorting is that the results are highly replicable, i.e., the same condition of instruction should lead to factors that are schematically reliable. According to Brown (1980), only a limited number of distinct viewpoints exist on any topic and these viewpoints will be revealed when the Q sample is administrated to different sets of Q-sorters. Based on the findings of two pairs of tandem studies, Thomas and Baas (1992) endorsed this idea and concluded that skepticism over replicability/generalizibility is unwarranted.

A brief of the proposed taxonomy was provided to the six Q-sorters. The six Q-sorters then individually sorted the SCSM measures based on the proposed taxonomy. The Q-sorting results were then collected and analyzed. The results were quite consistent among Q-sorters. About 72% of the SCSM measures were sorted into the same class by at least four of the six Q-sorters. In addition, only 1.4% of the SCSM measures were marked under the N/A class. The Q-sorting results are reported in Appendix B.

While the Q-sorting exercise provided a valid categorization, a practical problem before moving to hypothesis testing still existed. Each class of SCSM mechanisms entailed a fairly large number of measures. In essence, sampling from the domain of each construct is necessary. Thus, this present study opted to utilize a qualitative approach to identify the most important SCSM measures that represent each of the four classes of SCSM mechanisms. Toward this end, the four case studies proved invaluable. The author conducted semi-constructed interviews with supply chain managers from these firms. The taxonomy of SCSM mechanisms was first introduced and then the interviewees were solicited to elaborate on what their firm (or even other manufacturing firms they know of) has implemented to prevent (detect, react to, and restore from) SCS breaches (see Tables 9 and 10). The interviewees were also requested to discuss SCSM mechanisms that are most critical to their firm and why.

Building upon the case studies, I was able to select a representative sample of SCSM measures from the Q-sorted measures to reflect each of the four classes proposed by the taxonomy. The final set of indicators is reported in Table 14. Exploratory factor analysis using *principal axis factoring* extraction and *direct oblimin* rotation was performed to each block of selected items. Using the eigen-value-greater-than-one criterion, I found only one factor emerged from each group.

Table 14. Measurement items for SCSM mechanisms

Prevention: eigen value = 3.95, percentage of variance explained = 56.40%	**Factor loading**
We secure containers at our facilities to assure they are not compromised	.68
Our supply chain strategy spells out security priorities	.82
Our supply chain risk management strategy can be characterized as proactive	.83
When it comes to supply chain security, our strategy focuses on prevention	.76
We hold all suppliers accountable for supply chain security	.72
We only approve suppliers (irrespective of tier) that have a risk management program in place	.68
We educate suppliers about supply chain security practices	.74
Detection: eigen value = 5.73, percentage of variance explained = 57.30%	
We have the ability to track and trace our cargo in real time	.63
We use active measures such as video and sensors to be able to detect security breaches	.61
We monitor the loading/unloading process of cargo to identify potential security breaches	.73
We use sophisticated technologies to detect if containers have been compromised	.79
We monitor and synthesize information regarding security breaches	.83
We do conduct periodic assessments of our supply chain security	.82
We have procedures to detect supply chain security failures or near failures	.69
We have procedures to detect near misses in supply chain security	.81
We monitor our supplier network to identify suppliers at risk	.81
We have a process that notifies supply chain partners across tiers if the supply chain is threatened	.80
Reaction: eigen value = 6.96, percentage of variance explained = 57.97%	
We pre-position resources to deal with crises effectively	.79
We know what to do when we encounter supply chain security breaches or crises	.88
We have designated a group of employees as first respondents in case of a crisis	.72
There is effective communication across our supply chain when a crisis hits	.86
There is a definite chain of command in case of an emergency	.75
We have protocols for communication when a crisis arises	.77
We have a well-defined contingency plan to react to serious supply chain security breaches	.84
We have a quick reaction force to deal with a crisis or a serious disruption in our supply chain	.76
We use interchangeable or generic parts as a strategy to deal with potential disruptions in the supply chain	.54
We cross-train our employees as a mechanism to deal with potential supply chain disruptions	.81
We have backup processes that can assist us at times of crises	.80
We have flexible capacity contracts with suppliers in order to improve our ability to react to a crisis	.53
Restoration: eigen value = 3.51, percentage of variance explained = 58.44%	
We do have a disaster recovery plan	.75
We have a specific process to reinstate operations in case of a major crisis/disruption	.72
We maintain strategic inventory stocks to deal with potential crises	.56
We have strategies for recovery action after supply chain disruptions	.88
We have strategies to use more standard parts to reduce the risk of supply chain disruptions	.71
We developed alternative material sources in case of supply chain disruptions	.61

4.3.3 Organizational Performance

The third group of variables measures different dimensions of organizational performance. Five performance constructs were included in this study in order to capture a broad performance spectrum. Such selection was consistent with the findings from the four case studies. Specifically, these dimensions encompass supply chain security performance, supply chain cost performance, supply chain responsiveness, supply chain resilience, and supply chain visibility. The last four performance measures were labeled as collateral benefits of SCSM mechanisms in the literature (Closs and McGarrell, 2004; Peleg-Gillai and Bhat, 2006; Rice and Spayd, 2005).

Supply chain security performance measures the extent to which there is (1) an improvement in SCS; (2) a reduction/less potential for theft/loss; (3) a reduction/less potential for smuggling of drugs; and (4) an improved capability to detect counterfeit parts/products over the last three years (Closs and McGarrell, 2004; Lee and Whang, 2005; Mena et al., 2009; Peleg-Gillai and Bhat, 2006; Rice and Spayd, 2005; Sheffi 2001, 2005; Williams et al., 2009a). *Supply chain cost performance* measures the extent to which the adoption of SCSM mechanisms results in reductions in overall cost, excess inventory, insurance premiums, or costs associated with SCS disruptions (Lee and Whang, 2005; Mena et al., 2009; Peleg-Gillai and Bhat, 2006; Rice and Spayd, 2005; Williams et al., 2009b). *Supply chain responsiveness* measures the extent to which firms gain an improved ability for early intervention, faster response to problems, and efficient problem resolution (C-TPAT, 2001; Closs and McGarrell, 2004; Peleg-Gillai and Bhat, 2006; Rice and Spayd, 2005). S*upply chain resilience* is operationalized as the extent to

which firms are capable of withstanding serious SCS breaches and capable of restoring operations to normal conditions (Mena et al., 2009; Peleg-Gillai and Bhat, 2006; Rice and Spayd, 2005; Sheffi 2001, 2005). Finally, *supply chain visibility* denotes the extent to which firms obtain better access to supply chain data such as timely shipping information or tracking the location of cargo at any given time (Closs and McGarrell, 2004; Peleg-Gillai and Bhat, 2006; Rice and Spayd, 2005). Measurement items for performance measures are listed in Table 15 along with their factor loadings based on exploratory factor analysis using *principal axis factoring* and *direct oblimin* rotation.

Table 15. Measurement items for performance measures

All items have "in the last three years, our company has experienced" in front of them	
Supply chain security performance: eigen value = 1.79, percentage of variance explained = 57.88%	**Factor loading**
An improvement in security	.52
A reduction/less potential for theft/loss	.64
A reduction/less potential for smuggling of drugs	.76
An improved capability to detect counterfeit parts/products	.76
Supply chain cost performance: eigen value = 2.26, percentage of variance explained = 56.45%	
A reduction in overall cost	.78
A reduction in excess inventory	.71
A reduction in insurance premiums	.67
Reduced costs associated with supply chain disruptions	.84
Supply chain responsiveness: eigen value = 2.00, percentage of variance explained = 77.51%	
Faster response to problems in the supply chain	.87
An improved ability for early intervention	.81
More efficient problem resolution	.76
Supply chain resilience: eigen value = 2.55, percentage of variance explained = 72.37%	
An increase in our ability to deal with serious crises	.83
An increase in our ability to restore operations	.88
An improved ability to recover from serious security breaches	.67
An increase in our ability to cope with disruptions	.79
Supply chain visibility: eigen value = 3.12, percentage of variance explained = 62.33%	
Gains in tracking where our goods are at any given time	.81

Table 15. continued

Gains in our knowledge of the state of our goods	.78
Higher supply chain visibility	.74
Better access to supply chain data	.82
More timely shipping information	.79

4.3.4 Boundary Conditions

The boundary condition variables were adapted from the strategic management and the O&SCM literature. The construct items of top management commitment are adapted from the top management team literature (a.k.a., the upper echelon theory literature, Floyd and Lane, 2000; Hambrick and Mason, 1984; Hambrick, 2007; Mangan and Christopher, 2005; Wooldridge et al., 2008) and early work about top management commitment in the O&SCM literature (Ahire & O'Shaughnessy, 1997; Senge, 1990). The measurement scales of shared supply chain security perception were adapted from the organizational culture and SCS literature, including Barret et al. (2005), Gutierrez and Hintsa (2006), Khripunov (1999), Lv (2004), Sonsbeek (2004). The two constructs reflect on factors that may potentially moderate the relationships between institutional pressures and SCSM mechanisms. Measurement items for top management commitment and shared SCS perception are listed in Table 16 along with their factor loadings based on exploratory factor analysis using *principal axis factoring* extraction and *direct oblimin* rotation.

Table 16. Measurement items for moderating factors

Top management commitment: eigen value = 3.33, percentage of variance explained = 73.14%	**Factor loading**
Our top management has assumed a leadership role in risk management	.84
Our top mgmt allocates proper levels of resources to enhance the security of our supply chain	.80
Our top management provides clear objectives for securing the supply chain	.84
Top management has an active oversight over supply chain risk management	.87
Top mgmt is aware of the risks and consequences associated with supply chain disruptions	.73
Shared SCS perception: eigen value = 3.20, percentage of variance explained = 53.34%	
Putting supply chain security first is a sentiment widely shared within the organization	.76
Emergency preparedness is widely endorsed by organizational members	.67
We believe that supply chain security is the responsibility of everyone in the organization	.85
We believe that supply chain security concerns should be viewed with respect	.80
We believe that there are considerable security threats that can impact us	.58
We believe that even minor security breaches in our supply chain will be devastating to our company	.70

4.4 Analysis and Results

4.4.1 Pre-test Assessments

An array of tests was conducted to ensure the integrity of the data.

4.4.1.1 Normality

Normality was examined through the Kolmogorov-Smirnov test (Smirnov, 1948). The null-hypothesis of the Kolmogorov-Smirnov test states that the data is normally distributed. Failure to reject the null-hypothesis suggests normality. The results showed that the majority of variables used in this study passed the test with a p-value greater than 0.05. Because the Kolmogorov-Smirnov test is regarded as sensitive to violations of normality (Smirnov, 1948), especially for a large sample, I further examined the respective histograms and normality plots to assess potential distribution problems. A visual assessment of the P-P and Q-Q plots (Gibbons and Chakraborti, 2003) of the 83 variables suggested that all variables in this sample were normally distributed. I also examined potential outliers via P-P and Q-Q plots. No outlier was

found. Finally, I examined the skewness and kurtosis of the variables (Cramer, 1997). A value of skewness (or kurtosis) between -2σ and +2σ suggests that the assumption of normality is not violated (Kendall and Stuart, 1969). All manifest variables met this criterion. These results suggested that the data met the normality assumption.

4.4.1.2 Non-response Bias

Non-response bias was assessed by comparing firm characteristics of the first quartile of the respondents and the last quartile of the respondents via an ANOVA procedure (Krause, 1999). This method is based on the assumption that the opinions of late respondents are somewhat representative of the opinions of non-respondents (Armstrong and Overton, 1977). A number of t-tests were performed to examine the difference of firm characteristics of early respondents and late respondents. Specifically, the results showed that there was no statistical difference between early respondents and late respondents in terms of number of employees ($p=0.15$), annual sales ($p=0.38$), and net profit ($p=0.18$). These results provided confidence that the sample represented the larger population from which it was drawn.

4.4.1.3 Common-method Bias

Common-method bias was assessed through two methods. The first one relies on Harman's single-factor test (Podsakoff and Organ, 1986; Podsakoff et al., 2003). A study that has significant common method bias is one in which a majority of the variance can be explained by a single factor. An exploratory factor analysis using principal axis

factoring extraction and direct oblimin rotation was performed with all 83 manifest variables. Using the eigen-value-greater-than-one criterion, I examined the number of distinct factors that emerged and the variance those factors explained. The results showed that 11 substantive factors emerged from the analysis and the first factor only captured a small portion of the total variance (25%), suggesting that common-method bias was not an issue. An alternative way to perform the Harman's single-factor test is to constrain the number of factors extracted in the exploratory factor analysis to be just one (Podsakoff et al., 2003). If common-method bias is an issue, a single factor will account for the majority of the variance in the model. This test was also performed using principal axis factoring and direct oblimin rotation and the single factor only accounted for 26% of the variance in the model.

Another method to assess common-method bias is the Common Latent Factor approach which compares the model fit of two models (Podsakoff et al., 2003). In the first model, all manifest variables are loaded to a single common-method factor. In the second model, all manifest variables are assigned to their theoretical factors. The respective model fit of the two models is then compared with each other. If the model fit of the second model is better than the first model, then it is safe to conclude that the existence of common-method bias would not be a concern (Podsakoff et al., 2003). The common latent factor test was performed respectively to institutional pressure constructs, SCSM mechanism constructs, performance constructs, and moderating constructs. The results (Table 17) showed that the model fit of the second model was indeed better than

the first model. Therefore, common method bias should not be a concern in the present study.

Table 17. Tests for common method bias

	Common Latent Factor Model Fit	Theoretical Factor Model Fit
Institutional pressure constructs	$\chi^2(114)=1259.86$, RMSEA=0.15, CFI=0.78, TLI=0.73, SRMR=0.08.	$\chi^2(104)=341.08$, RMSEA=0.07, CFI=0.95, TLI=0.94, SRMR=0.04.
SCSM mechanism constructs	$\chi^2(555)=1714.19$, RMSEA=0.09, CFI=0.87, TLI=0.85, SRMR=0.07.	$\chi^2(549)=1432.18$, RMSEA=0.06, CFI=0.91, TLI=0.90, SRMR=0.05.
Performance constructs	$\chi^2(169)=727.33$, RMSEA=0.09, CFI=0.88, TLI=0.87, SRMR=0.07.	$\chi^2(159)=597.47$, RMSEA=0.07, CFI=0.92, TLI=0.90, SRMR=0.05.
Moderating constructs	$\chi^2(42)=119.53$, RMSEA=0.09, CFI=0.83, TLI=0.84, SRMR=0.06.	$\chi^2(41)=119.53$, RMSEA=0.06, CFI=0.97, TLI=0.96, SRMR=0.04.

4.4.2 Assessment of Measurement Model

4.4.2.1 Unidimensionality

The unidimensionality of the 16 constructs was tested by examining the fit indices values from confirmatory factor analysis via Mplus 6.2.1. Measurement models were constructed for each of the 16 constructs. The fit of the measurement model was assessed using the following fit indices: chi-square (χ^2) and its ratio to the model degrees of freedom (χ^2/df), comparative fit index (CFI), Tucker-Lewis index (TLI), Root Mean Square Error Approximation (RMSEA), and Standardized Root Mean Square Residual (SRMR). In summary, it is generally recognized that to support model fit, a consensus among the following criteria is needed: a $\chi^2/df < 3$, a CFI > 0.90, a TLI > 0.90, a RMSEA < 0.08, and a SRMR < 0.08. A good model fit is an indication of scale unidimensionality (Bollen, 1989). Almost all model fit indices for each construct

exceeded the expected values and therefore provided strong support for scale unidimensionality (Table 18).

Table 18. Summary of individual measurement models

Construct	χ^2	χ^2/df	CFI	TLI	RMSEA	SRMR
Government pressure	0.02	0.01	1.00	1.00	0.00	0.00
Customer pressure	2.60	1.30	0.99	0.99	0.03	0.01
Peer pressure	0.00	N/A[1]	1.00	1.00	0.00	0.00
Normative pressure	0.00	N/A	1.00	1.00	0.00	0.00
Performance pressure	0.00	N/A	1.00	1.00	0.00	0.00
Prevention	55.35	3.95	0.97	0.96	0.07	0.03
Detection	166.24	4.75	0.94	0.92	0.08	0.04
Reaction	158.56	2.94	0.96	0.95	0.06	0.04
Restoration	29.35	3.26	0.97	0.95	0.07	0.04
Supply chain security performance	1.61	0.81	1.00	0.99	0.04	0.01
Supply chain cost performance	3.21	1.61	0.99	0.97	0.07	0.02
Supply chain responsiveness	0.00	N/A	1.00	1.00	0.00	0.00
Supply chain resilience	0.64	0.32	1.00	1.01	0.00	0.00
Supply chain visibility	0.07	0.01	0.99	0.98	0.06	0.01
Top management commitment	16.65	3.33	0.99	0.97	0.08	0.01
Shared SCS perception	18.08	2.01	0.99	0.98	0.06	0.03

[1]: A measurement model with three indicators is just identified. In other words, $df = 0$.

4.4.2.2 Convergent Validity

Convergent validity refers to the degree to which two measures of a construct that should be theoretically related, are in fact related. One way to assess convergent validity is to look at the corrected item-total correlations (CITC) of items that are assigned to the same theoretical construct. High CITC values suggest good convergent validity. The CITC values were requested by using SPSS for each of the 16 constructs. All of the CITC values were above 0.6. Convergent validity can also be assessed by factor loadings. I constructed confirmatory factor analytic measurement models for each group of factors respectively using Mplus 6.2.1. The model fit indices for all four models suggest good model fit (Tables 19-22). All items in my data illustrated high factor

loadings except for three (0.53, 0.50, and 0.52) respectively. See also Tables 19-22 which illustrate that all factor loadings were greater than 0.6 and were statistically significant.

Table 19. Factor loadings, Cronbach's α values, AVEs, and CRs for institutional pressure constructs

Factor and scale items	**Measurement items**		
	Std. loading	**S.E.**	**t-value**
Government pressure: CR=0.86, AVE=0.61, α=0.86			
There is definite pressure from our government to meet security standards	0.80	0.02	38.17
We will receive significant benefits if we adopt security standards prescribed by our government	0.73	0.03	28.06
Our government takes an active role on security matters	0.79	0.02	36.14
We cannot take security lightly as our government will hold us accountable	0.80	0.02	38.32
Customer pressure: CR=0.89, AVE=0.68, α=0.89			
Our customers pressure us to do better on security	0.78	0.02	37.29
We have to meet standards for security as our customers are demanding us to do so	0.87	0.02	57.88
Our customers hold us accountable for security	0.81	0.02	41.98
Our customers are monitoring our security practices/performance	0.83	0.02	46.74
Peer pressure: CR=0.83, AVE=0.64, α=0.83			
We feel that we have to adopt security practices because everybody else does it	0.67	0.03	22.68
We feel the pressure to adopt security practices as most of our peers have done so	0.84	0.02	42.67
We feel that we have to adopt security practices as most of our rivals have done so	0.87	0.02	47.49
Normative pressure: CR=0.80, AVE=0.58, α=0.82			
We employ risk & security practices in order to conform to professional norms	0.76	0.03	28.05
We implement supply chain security practices to conform to industry norms	0.76	0.03	27.88
We employ supply chain security practices to conform to cultural norms	0.72	0.03	24.98
Performance pressure: CR=90, AVE=0.75, α=0.90			
We implement security practices because they can improve performance	0.86	0.01	52.16
We implement security practices because they can lead to competitive advantage	0.86	0.02	50.56
We implement security practices because we see operational benefits	0.87	0.02	54.98

Model fit: $\chi^2(104)=341.08$, RMSEA=0.07, CFI=0.95, TLI=0.94, SRMR=0.04

Table 20. Factor loadings, Cronbach's α values, AVEs, and CRs for SCSM mechanism constructs

Factor and scale items	**Measurement items**		
	Std. loading	**S.E.**	**t-value**
Prevention: CR=0.90, AVE=0.58, α=0.90			
We secure containers at our facilities to assure they are not compromised	0.68	0.03	21.91
Our supply chain strategy spells out security priorities	0.85	0.02	52.71
Our supply chain risk management strategy can be characterized as proactive	0.85	0.01	59.26
When it comes to supply chain security, our strategy focuses on prevention	0.79	0.02	41.69
We hold all suppliers accountable for supply chain security	0.70	0.03	27.60
We only approve suppliers (irrespective of tier) that have a risk management program in place	0.70	0.03	27.96
We educate suppliers about supply chain security practices	0.72	0.02	29.58
Detection: CR=0.93, AVE=0.57, α=0.93			
We have the ability to track and trace our cargo in real time	0.63	0.04	17.50
We use active measures such as video and sensors to be able to detect security breaches	0.62	0.04	17.04
We monitor the loading/unloading process of cargo to identify potential security breaches	0.79	0.02	34.66
We use sophisticated technologies to detect if containers have been compromised	0.71	0.03	23.71
We monitor and synthesize information regarding security breaches	0.85	0.02	53.10
We do conduct periodic assessments of our supply chain security	0.82	0.02	42.25
We have procedures to detect supply chain security failures or near failures	0.81	0.02	45.67
We have procedures to detect near misses in supply chain security	0.79	0.02	39.79
We monitor our supplier network to identify suppliers at risk	0.79	0.02	41.02
We have a process that notifies supply chain partners across tiers if the supply chain is threatened	0.71	0.03	28.91
Reaction: CR=0.94, AVE=0.56, α=0.94			
We pre-position resources to deal with crises effectively	0.78	0.02	33.87
We know what to do when we encounter supply chain security breaches or crises	0.85	0.02	50.11
We have designated a group of employees as first respondents in case of a crisis	0.73	0.03	26.63
There is effective communication across our supply chain when a crisis hits	0.83	0.02	44.24
There is a definite chain of command in case of an emergency	0.76	0.03	29.94
We have protocols for communication when a crisis arises	0.77	0.02	33.43
We have a well-defined contingency plan to react to serious supply chain security breaches	0.86	0.01	55.34
We have a quick reaction force to deal with a crisis or a serious disruption in our supply chain	0.75	0.03	29.57
We use interchangeable or generic parts as a strategy to deal with disruptions in the supply chain	0.50	0.04	12.47
We cross-train our employees as a mechanism to deal with potential supply chain disruptions	0.76	0.02	33.69
We have backup processes that can assist us at times of crises	0.80	0.02	41.10
We have flexible capacity contracts with suppliers in order to improve our ability to react to a crisis	0.53	0.04	14.53
Restoration: CR=0.86, AVE=0.52, α=0.85			
We do have a disaster recovery plan	0.80	0.02	37.18
We have a specific process to reinstate operations in case of a major crisis/disruption	0.82	0.02	43.60
We maintain strategic inventory stocks to deal with potential crises	0.69	0.05	13.84
We have strategies for recovery action after supply chain disruptions	0.81	0.02	42.84
We have strategies to use more standard parts to reduce the risk of supply chain disruptions	0.65	0.03	22.23
We developed alternative material sources in case of supply chain disruptions	0.52	0.04	13.70

Model fit: $\chi^2(549)=1432.18$, RMSEA=0.06, CFI=0.91, TLI=0.90, SRMR=0.05

Table 21. Factor loadings, Cronbach's α values, AVEs, and CRs for performance constructs

Factor and scale items (All items have "in the last three years, our company has experienced" in front of them)	**Measurement items**		
	Std. loading	**S.E.**	**t-value**
Supply chain security performance: CR=0.77, AVE=0.51, α=0.79			
An improvement in security	0.73	0.03	26.72
A reduction/less potential for theft/loss	0.69	0.03	23.19
A reduction/less potential for smuggling of drugs	0.63	0.04	15.28
An improved capability to detect counterfeit parts/products	0.64	0.04	16.04
Supply chain cost performance: CR=0.77, AVE=0.52, α=0.74			
A reduction in overall cost	0.66	0.03	19.98
A reduction in excess inventory	0.62	0.04	16.67
A reduction in insurance premiums	0.63	0.04	16.25
Reduced costs associated with supply chain disruptions	0.79	0.03	28.43
Supply chain responsiveness: CR=0.80, AVE=0.57, α=0.63			
Faster response to problems in the supply chain	0.83	0.02	39.78
An improved ability for early intervention	0.62	0.04	16.03
More efficient problem resolution	0.80	0.02	37.65
Supply chain resilience: CR=0.87, AVE=0.64, α=0.87			
An increase in our ability to deal with serious crises	0.82	0.02	46.53
An increase in our ability to restore operations	0.86	0.02	54.50
An improved ability to recover from serious security breaches	0.69	0.03	25.14
An increase in our ability to cope with disruptions	0.81	0.02	43.99
Supply chain visibility: CR=0.89, AVE=0.62, α=0.89			
Gains in tracking where our goods are at any given time	0.79	0.02	37.58
Gains in our knowledge of the state of our goods	0.79	0.02	37.73
Higher supply chain visibility	0.75	0.03	30.79
Better access to supply chain data	0.83	0.02	46.15
More timely shipping information	0.78	0.02	37.65

Model fit: $\chi^2(159)=597.47$, RMSEA=0.07, CFI=0.92, TLI=0.90, SRMR=0.05.

Table 22. Factor loadings, Cronbach's α values, AVEs, and CRs for moderating constructs

Factor and scale items	Measurement items		
	Std. loading	S.E.	t-value
Top management commitment: CR=90, AVE=66, α=0.91			
Our top management has assumed a leadership role in risk management	0.80	0.02	41.05
Our top mgmt allocates proper levels of resources to enhance the security of our supply chain	0.82	0.02	44.98
Our top management provides clear objectives for securing the supply chain	0.85	0.02	54.68
Top management has an active oversight over supply chain risk management	0.87	0.01	59.13
Top mgmt is aware of the risks and consequences associated with supply chain disruptions	0.70	0.03	26.10
Shared SCS perception: CR=0.87, AVE=0.53, α=0.87			
Putting supply chain security first is a sentiment widely shared within the organization	0.78	0.02	32.05
Emergency preparedness is widely endorsed by organizational members	0.65	0.04	18.45
We believe that supply chain security is the responsibility of everyone in the organization	0.83	0.02	40.56
We believe that supply chain security concerns should be viewed with respect	0.79	0.02	34.12
We believe that there are considerable security threats that can impact us	0.64	0.04	17.96
We believe that even minor security breaches in our supply chain will be devastating to our company	0.66	0.03	19.35

Model fit: $\chi^2(41)=119.53$, RMSEA=0.06, CFI=0.97, TLI=0.96, SRMR=0.04.

4.4.2.3 Discriminant Validity

A confirmatory factor analysis based χ^2 difference test via Mplus 6.2.1 was used to assess discriminant validity (Bagozzi et al., 1991). Measurement models were constructed for all possible pairs of the 16 theoretical constructs. A total of 120 models were thus constructed. These models were tested by first allowing for the correlation between the two constructs to be freely estimated and then fixing the correlation between the constructs at 1.0. A significant difference in Chi-square values for the freely estimated model and the constrained (i.e. fixed) model indicates the distinctiveness of the two constructs (Bagozzi et al., 1991). A χ^2 difference values greater than 3.84 (df=1) suggests good discriminant validity. Table 23 reports these χ^2 difference values. All differences between the fixed and free solutions were greater than 3.84 (i.e.,

$\Delta\chi^2(1)>3.84$), thus providing strong evidence of discriminant validity among the 16 constructs.

Table 23. Summary of discriminant validity testing (χ^2 difference values)

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1. Government pressure															
2. Customer pressure	228														
3. Peer pressure	122	238													
4. Normative pressure	224	258	95												
5. Performance pressure	200	212	391	185											
6. Prevention	276	227	389	159	206										
7. Detection	277	206	386	178	265	4.20									
8. Reaction	174	121	441	253	291	62	134								
9. Restoration	145	130	422	195	159	34	81	9.97							
10. SCS performance	70	49	339	207	188	85	111	141	183						
11. Cost performance	51	48	322	262	230	234	230	206	198	81					
12. Responsiveness	48	60	313	224	197	164	180	139	112	33	34				
13. Resilience	92	82	502	359	467	284	338	252	186	13	78	44			
14. Visibility	80	61	520	365	475	421	478	427	285	41	88	78	72		
15. Top Mgmt commitment	207	523	426	212	277	12	37	63	33	100	262	114	111	457	
16. Shared SCS perception	177	173	134	86	83	8.40	35	61	34	164	225	92	84	294	6.38

4.4.2.4 Reliability

Reliability was assessed through Cronbach's α, average variance extracted (AVE), and composite reliability (CR) (see Table 19-22). Cronbach's α is a coefficient of internal consistency (Cronbach, 1951; Raykov, 1997). It is commonly used as an estimate of the reliability of a psychometric test for a sample of examinees. Cronbach's α is most appropriately used when the items measure different nuances within a single construct (Cortina, 1993; Schmitt, 1996). A Cronbach's α value of 0.6 or above is

considered acceptable (DeVellis, 1991). The Cronbach's α values of the 16 constructs were calculated and all of them were greater than 0.6.

While Cronbach's α was widely used in the literature as a measure of reliability, some researchers argued that Cronbach's α is not an effective estimate of the reliability of a scale. For example, Bollen opposed using Cronbach's α because "[Cronbach's α] makes no allowances for correlated error of measurements" (Bollen, 1989, p.221). As such, the present study also assessed scale reliability through AVE and CR. AVE measures the amount of variance that is captured by the construct in relation to the amount of variance due to measurement error (Fornell and Larcker, 1981). If the AVE is less than 0.50, then the variance due to measurement error is greater than the variance due to the construct. In this case, the reliability of a construct is questionable. On the other hand, an AVE value of 0.5 or above suggests good reliability (Fornell and Larcker, 1981). AVEs were calculated for all 16 constructs and all of them were greater than 0.5, suggesting reliability. CR estimates the extent to which a set of manifest indicators share in their measurement of a construct (Hair et al., 1998). A CR value of 0.7 or above suggests acceptable scale reliability (Hair et al., 1998). The CR values of the 16 constructs were calculated and all of them were greater than 0.75, suggesting good reliability.

Collectively, the Cronbach's α values, the AVE values, and the CR values provide sufficient evidence of reliability for each of the constructs.

4.4.3 Assessment of Structural Models

Hypotheses were tested using Covariance-based Structural Equation Models (CBSEM) via Mplus 6.2.1. CBSEM has proven to be a very useful statistical method for structural models. CBSEM allows for the structural model to relate the constructs to each other and test their effects on each other simultaneously (Jarvis et al., 2003). The foundation of CBSEM lies in two multivariate techniques: factor analysis and multiple regression (Hair et al., 2006). Specifically, "it examines the structure of interrelationships expressed in a series of equations, similar to a series of multiple regression equations" (Hair et al., 2006: p. 711). Owing to these traits, CBSEM was selected as the data analysis technique for the assessment of the structural models under study.

The fit of the structural model is evaluated first, followed by close examination of individual structural coefficients (i.e., Gamma - γ and Beta - β) and their respective t- and p-values. The overall structural model-to-data fit was assessed via fit indices: chi-square (χ^2) and its ratio to the model degrees of freedom (χ^2/df), comparative fit index (CFI), Tucker-Lewis index (TLI), Root Mean Square Error Approximation (RMSEA), and Standardized Root Mean Square Residual (SRMR). If there appears to be consistency between the posited structural model and the data, structural coefficients and their respective p-values can then be used to test hypotheses.

4.4.3.1 Institutional Pressure→SCSM Mechanism Model

The institutional pressure→SCSM mechanism model (H1-H4) was first tested (Figure 4). The data analysis for the structural model used raw data as input for Mplus. All variables were centered to avert potential multicollinearity problems. The highest VIF score was less than 5.0. Firm size, firm past performance, market share, and industry membership were used as control variables. The following fit criteria were determined: $\chi^2(50)=157.03$, $\chi^2/df=3.14$, RMSEA=0.07, CFI=0.96, TLI=0.95, SRMR=0.04. There appears to be consistency between the posited structural model and the data. The results are shown in Table 24 (std. coefficients & p-values).

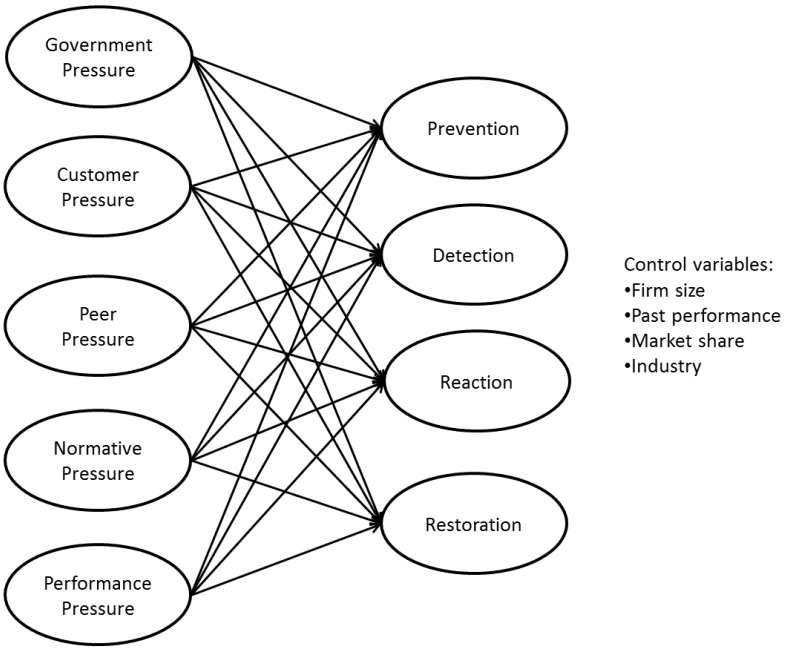

Figure 4. The institutional pressure→SCSM mechanism model

Table 24. Institutional pressure → SCSM mechanism model results

Paths	Std. Coeff.	p-value	Results
Hypothesis 1: Institutional pressures → Prevention			Partly supported
Government pressure → Prevention	.083	.211	
Customer pressure → Prevention	.112	.135	
Peer pressure → Prevention	**-.236**	**.050**	
Normative pressure → Prevention	**.432**	**.005**	
Performance pressure → Prevention	**.292**	**.007**	
Hypothesis 2: Institutional pressures → Detection			Partly supported
Government pressure → Detection	.109	.128	
Customer pressure → Detection	.071	.485	
Peer pressure → Detection	**-.154**	**.050**	
Normative pressure → Detection	**.242**	**.015**	
Performance pressure → Detection	**.191**	**.002**	
Hypothesis 3: Institutional pressures → Reaction			Partly supported
Government pressure → Reaction	-.051	.330	
Customer pressure → Reaction	-.108	.102	
Peer pressure → Reaction	**-.175**	**.048**	
Normative pressure → Reaction	**.447**	**.000**	
Performance pressure → Reaction	**.262**	**.001**	
Hypothesis 4: Institutional pressures → Restoration			Partly supported
Government pressure → Restoration	-.018	.461	
Customer pressure → Restoration	**.159**	**.043**	
Peer pressure → Restoration	**-.164**	**.025**	
Normative pressure → Restoration	**.506**	**.002**	
Performance pressure → Restoration	**.217**	**.021**	

Model fit: $\chi^2(50)=157.03$, RMSEA=0.07, CFI=0.96, TLI=0.95, SRMR=0.04.

The institutional pressures are purported to positively impact the prevention mechanisms. The results showed, however, that not all of the institutional pressures were conducive to prevention. Specifically, the effects of government pressure ($\gamma = 0.08$, $p > 0.05$) and customer pressure ($\gamma = 0.12$, $p > 0.05$) were trivial. Also, while the effects of normative pressure ($\gamma = 0.43$, $p < 0.01$) and performance pressure ($\gamma = 0.29$, $p < 0.01$) were positive and statistically significant, the effect of peer pressure was negative and

statistically significant ($\gamma = -0.24$, $p < 0.05$). The results suggest that norms and performance needs are the major sources that motivate firms to implement prevention mechanisms. H1 was only partly supported.

The effects of institutional pressures on detection mechanisms were also assessed. Specifically, government pressure ($\gamma = 0.11$, $p > 0.5$) and customer pressure ($\gamma = 0.07$, $p > 0.5$) did not manifest a significant impact on detection mechanisms. The statistically significant effects from normative pressure ($\gamma = 0.24$, $p < 0.05$), and performance pressure ($\gamma = 0.19$, $p < 0.01$) attested to the positive linkage between institutional pressures and detection mechanisms. However, the effect of peer pressure was negative and statistically significant ($\gamma = -0.15$, $p < 0.05$). This finding contradicts my hypothesis and suggests that peer pressure has adverse effect on detection mechanisms. Overall, H2 was partly supported as well.

The institutional pressures were also specified to positively affect the reaction mechanisms. Again, not all institutional pressures exhibited sizable effects on reaction. The impact from government ($\gamma = -0.05$, $p > 0.5$) and customer ($\gamma = -0.11$, $p > 0.5$) appeared to be negligible. The effect of peer pressure ($\gamma = -0.18$, $p < 0.05$) was negative and statistically significant. The effects of normative pressure ($\gamma = 0.45$, $p < 0.001$) and performance pressure ($\gamma = 0.26$, $p < 0.01$) were positive and statistically significant. In short, H3 was not fully supported. The results suggest that firms implement reaction mechanisms mainly because they need to conform to norms and improve performance.

Finally, the effects of institutional pressure on restoration mechanisms were examined. The results showed that government pressure ($\gamma = -0.02$, $p > 0.5$) again

revealed no significant association with restoration. However, the impact of peer pressure was rather strong and negative ($\gamma = -0.16$, $p < 0.05$) while customer pressure ($\gamma = 0.16$, $p < 0.5$), normative pressure ($\gamma = 0.51$, $p < 0.01$), and performance pressure ($\gamma = 0.22$, $p < 0.05$) exhibited significant and positive association with restoration. H4 was again partly supported. The findings are in line with the results of previous hypotheses and suggest that government pressure is somewhat negligible whereas peer pressure has rather consistent negative impact on SCSM mechanisms.

4.4.3.2 Differential Effect of Institutional Pressures on SCSM Mechanisms

H5 through H8 posit that the coefficients relating the institutional pressures and a given class of SCSM mechanism are different. A specific institutional pressure is hypothesized to exhibit a stronger effect on a given class of SCSM mechanisms than other institutional pressures. Specifically, I hypothesize that government pressure is the strongest predictor of prevention- (H5) and detection-oriented (H6) SCSM mechanisms; customer pressure is the strongest predictor of reaction- (H7) and restoration-oriented (H8) SCSM mechanisms. In these hypotheses, there are five different *independent variables* (i.e., five institutional pressures) but only one *dependent variable* (i.e., one SCSM mechanism).

In order to compare the differences in coefficients between the institutional pressures and a given class of SCSM mechanism, a set of regressions were performed. For example, in order to test whether government pressure is the strongest predictor of prevention-oriented SCSM mechanisms, one has to show that the effect of government

pressure is greater than the effect of the other four institutional pressures. One way to make this determination is to examine the significance levels and the corresponding p-values of the coefficients in an equation in which the dependent variable is the prevention-oriented SCSM mechanism while the independent variables (i.e., regressors) are the five institutional pressures. Under two scenarios the conclusion can be easily drawn: (1) government pressure is the only positive and statistically significant regressor; (2) government pressure reveals insignificant association with the dependent variable and at least one of the other four institutional pressures is statistically associated with the dependent variable. Given scenario one, it is safe to conclude that government pressure is the strongest predictor among the institutional pressures. In scenario two, there exists at least one institutional pressure whose effect is stronger than government pressure. However, more frequently researchers may find that there is more than one *estimated Beta coefficient* (Beta hereafter) that is positive and statistically significant. Under such circumstances, additional rigorous analyses are required, because simply comparing the p-values of the Betas is not a reliable test (Cramer, 1997).

Assuming the Betas of all five institutional pressures are positive and statistically significant, the comparisons of the coefficients can then be made by assessing four pairs of relationships (i.e., government v.s. customer, government v.s. peer, government v.s. normative, and government v.s. performance). If the effect of government pressure is stronger in all four comparisons, then government pressure is indeed the strongest institutional predictor of prevention-oriented SCSM mechanisms.

The comparison between government pressure and customer pressure can be performed as follows (Cramer, 1997). First, the prevention-oriented SCSM mechanism (*DV*) was regressed on government pressure (IV_1) and customer pressure (IV_2). The standard error of the two Betas (i.e., SE_1 and SE_2) and the covariance of the two Betas (i.e., COV_{12}) were attained from the SPSS output using the syntax command "STATISTICS=BCOV". Second, the joined standard error of β_1 and β_2, SE_{12}, was calculated. Because both regressors were from the same sample, the joined standard error was calculated using the formula: $SE_{12} = \sqrt{SE_1^2 + SE_2^2 - 2COV_{12}}$. Third, since $\frac{\beta_1 - \beta_2}{SE_{12}}$ follows a *t* distribution with (*n-k-1*) degrees of freedom, the value of the t-statistic, $\frac{\beta_1 - \beta_2}{SE_{12}}$, was calculated and assessed against the values listed in the *t* distribution table (Kutner, Nachtsheim, Neter, and Li, 2004). Because the degrees of freedom is greater than 120 in my case, a t-statistic value of 1.96 or above would suggest a significant difference between β_1 and β_2 (at α=0.05 level), that is, the effect of government pressure is greater than the effect of customer pressure. The same analysis was repeated for the comparison of other three pairs of pressures.

Table 25. Test of differential effect-1

Hypothesis	**Results**				
H5: *Government pressure is the strongest predictor of prevention-oriented SCSM mechanisms*					
Step 1 Regression results (DV: prevention)	Government	Customer	Peer	Normative	Performance
	.083	.112	-.236*	.432**	.292**
Step 2 Pair-wise comparisons	Not performed as government pressure is not significantly associated with prevention mechanisms. H5 is rejected				
H6: *Government pressure is the strongest predictor of detection-oriented SCSM mechanisms*					
Step 1 Regression results (DV: detection)	Government	Customer	Peer	Normative	Performance
	.109	.071	-.154†	.242*	.191**
Step 2 Pair-wise comparisons	Not performed as government pressure is not significantly associated with detection mechanisms. H6 is rejected				
H7: Customer pressure is the strongest predictor of reaction-oriented SCSM mechanisms					
Step 1 Regression results (DV: reaction)	Government	Customer	Peer	Normative	Performance
	-.051	-.108	-.175*	.447***	.262**
Step 2 Pair-wise comparisons	Not performed as customer pressure is not significantly associated with reaction mechanisms. H7 is rejected				
H8: Customer pressure is the strongest predictor of restoration-oriented SCSM mechanisms					
Step 1 Regression results (DV: restoration)	Government	Customer	Peer	Normative	Performance
	-.018	.159*	-.164*	.506**	.217*
Step 2 Pair-wise comparisons (t-values are reported)	customer v.s. government	customer v.s. peer		customer v.s. normative	customer v.s. performance
	2.04	4.51		**1.15**	**-3.72**

$^{\dagger}p < 0.1$, *p < 0.05, **$p < 0.01$, ***$p < 0.001$. Coefficients reported are standardized.

As shown in the Table 25 above, H5-H7 were rejected as the variable of interest was not statistically significant when all institutional pressures were tested as a group. H8 was rejected because (1) the effect of customer pressure was not significantly

different from the effect of normative pressure (t-value < 1.96) and (2) the effect of performance pressure on restoration is stronger than the effect of customer pressure (a negative and significant t-value).

4.4.3.3 Moderation Effect Hypotheses

Shared SCS perception (H9) and top management commitment (H10) were postulated to strengthen the relationships between institutional pressures and SCSM mechanisms. Before testing the moderation hypotheses, I centered all independent variables in order to minimize the potential multicollinearity that can be present when computing the square terms (Aiken and West, 1991). I did not use Mplus to directly test the hypotheses because it employs a rather complicated algorithm ("xwith" command) to calculate the interaction terms of any two latent factors. Such an algorithm imposes tremendous computational burdens when multiple latent interaction terms are included in a model. Plus, when the "xwith" command is used, Mplus does not produce model fit indices because there is a debate as to which baseline model should be used to compute fit indices (Mplus User's Guide, 2011). Thus, I used SPSS to perform data analysis. Table 26 and Table 27 display the results.

Table 26. Moderation effects of shared SCS perception

	Prevention	Detection	Reaction	Restoration
Variables				
Control variables				
Firm size	.057	.099	.174†	.176*
Past performance (profit margin)	-.038	-.023	-.001	.017
Market share	.116†	.030	.130	.177*
Food & Beverage	.119	.102	-.192†	-.177†
Chemical	.107	.089	-.096	-.043
Auto	.071	.140†	.035	-.052
IT	.062	-.030	-.002	-.014
Other Manufacturing	.059	.012	-.129	-.039
Main effects				
Government pressure	.164	.291†	.514**	.443**
Customer pressure	.379*	.081	-.397†	-.104
Peer pressure	.116	.098	-.329†	-.380*
Normative pressure	.069	.067	.143	-.003
Performance pressure	.035	.173	.196	-.082
Shared SCS perception	.211†	.185	.501*	.629**
Interaction effects				
Government x SSP	.028	-.016	-.170	-.232
Customer x SSP	-.109	-.064	.021	-.150
Peer x SSP	-.098	.093	**.587***	**.617***
Normative x SSP	**.347**†	.276	-.264	-.344
Performance x SSP	-.123	-.238	-.103	.164
R^2 *(adjusted)*	83.7%	79.1%	80.8%	85.7%

†$p < 0.1$, *p < 0.05, **$p < 0.01$, ***$p < 0.001$. Coefficients reported are standardized.

With respect to H9, the results showed that shared SCS perception interacted with peer pressure to positively affect reaction (β=0.587, p<0.05) and restoration (β=0.617, p<0.05). The results suggest that the effects of peer pressure on reaction- and restoration-oriented SCSM mechanisms will be stronger when shared SCS perception is high compared to when shared SCs perception is low. Shared SCS perception also interacted with normative pressure to positively affect prevention (β=0.347, p<0.1) However, shared SCS perception did not reveal any statistically significant interaction effect on other pressure-mechanism relations.

Table 27. Moderation effects of top management commitment

	Prevention	Detection	Reaction	Restoration
Variables				
Control variables				
Firm size	.043	.060	.095	.069
Past performance (profit margin)	-.012	.023	.060	.090
Market share	.142†	.046	.114	.186*
Food & Beverage	.110	.051	-.208*	-.177*
Chemical	.099	.021	-.136	-.079
Auto	.047	.036	.144	.044
IT	.034	-.077	-.001	.002
Other Manufacturing	.093	.037	-.142	.038
Main effects				
Government pressure	.222	.318*	.195	.030
Customer pressure	.369*	.051	-.241	.132
Peer pressure	.067	.054	-.262†	-.312*
Normative pressure	.075	.038	.274	-.140
Performance pressure	.038	.180	.209	.130
Top management commitment	.199	.371*	.489*	.598***
Interaction effects				
Government x TMC	-.043	.018	**-.414**†	**-.495***
Customer x TMC	-.056	.023	.147	.044
Peer x TMC	.063	.018	**.606***	**.603****
Normative x TMC	.112	-.004	-.059	-.166
Performance x TMC	-.0.39	-.010	-.231	-.065
R^2 *(adjusted)*	82.5%	79.3%	84.2%	89.3%

$^{\dagger}p < 0.1$, *p < 0.05, **$p < 0.01$, ***$p < 0.001$. Coefficients reported are standardized.

Regarding H10, the results showed that top management commitment only interacted with government pressure and peer pressure. Specifically, top management commitment interacted with government pressure to negatively affect reaction (β=-0.414, p<0.1) and restoration (β=-0.495, p<0.05). Top management commitment also exhibited positive joint effects with peer pressure on reaction (β=0.606, p<0.05) and restoration (β=0.603, p<0.01). The findings suggest that top management commitment may enhance or hamper the effects of institutional pressures on SCSM mechanisms. I plot these statistically significant interaction effects in Figure 5.

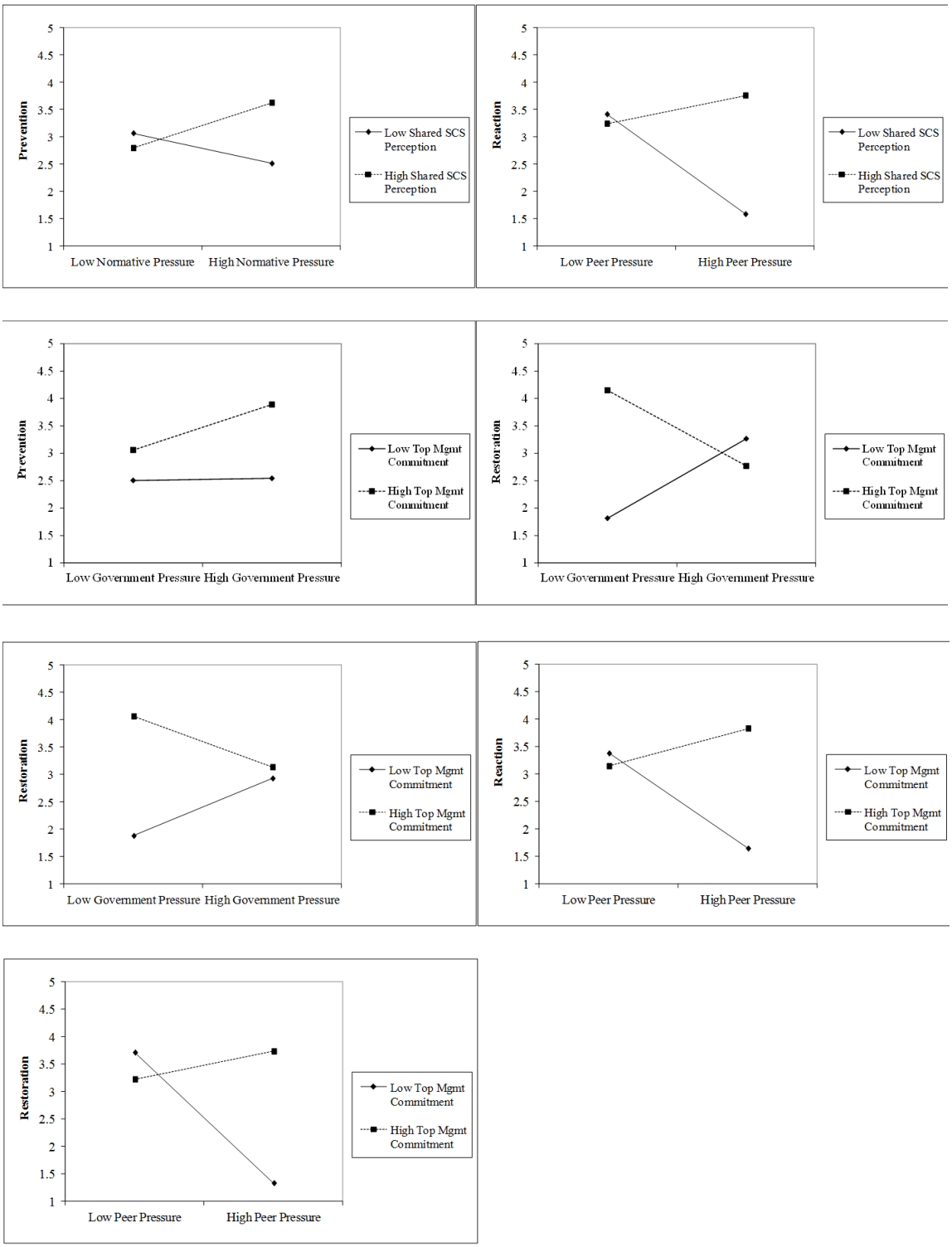

Figure 5. Interaction effect plots

4.4.3.4 SCSM Mechanism→Performance Model

The SCSM mechanism→performance model was then tested for hypotheses 11a, 12a, 13a, and 14a (Figure 6). The data analysis was performed via Mplus using raw data as input. All variables were once again centered to avert potential multicollinearity problem. Firm size, firm past performance, market share, and industry membership were used as control variables.

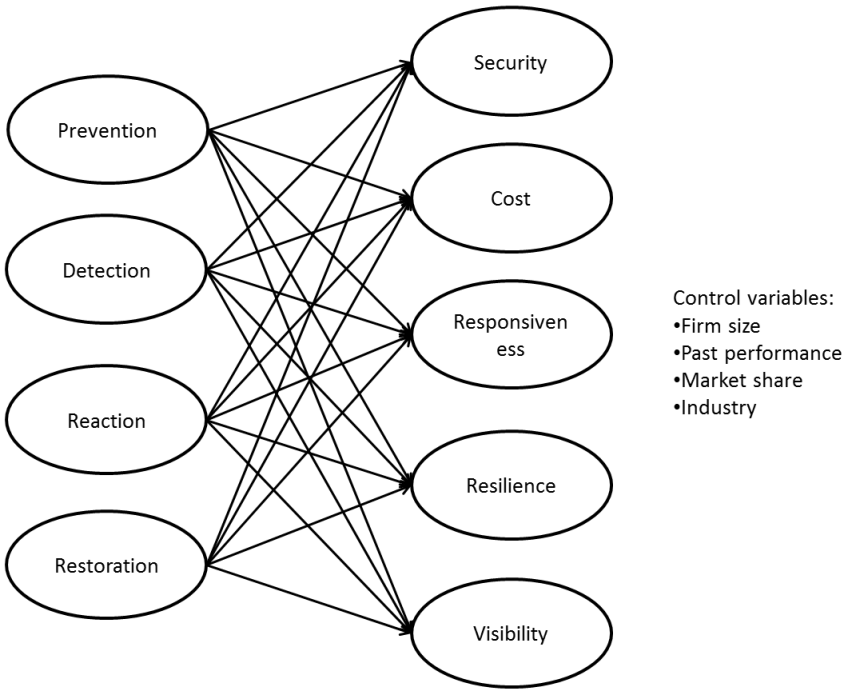

Figure 6. The SCSM mechanism → performance model

While the literature suggests that the four classes of SCSM mechanisms positively affect supply chain performance, it is surprising that none of the relationships exhibited statistical significance when tested at the first-order level of abstraction. This can be a signal of multicollinearity in the model. I therefore assessed multicollinearity through VIF. The results showed that all VIF scores of the SCSM mechanisms were greater than ten, suggesting that multicollinearity did exist. There is no doubt that prevention, detection, reaction, and restoration are important nuances of SCSM. Most people would agree that each of the four latent variables is "different" and displays idiosyncratic attributes. From a measurement perspective, I already demonstrated that the constructs discriminated from each other. However, most people would also agree that a responsible firm who is good at prevention is also likely to be good at detection and can effectively respond to SCS breaches. The four latent factors would be expected to be highly correlated, which may inflate standard errors and result in insignificant results (Chatterjee, Hadi, and Price, 2000). Being aware of this issue, I examined the effect of each SCSM mechanism on performance on an individual basis. All classes of SCSM mechanisms exhibited significant impact on performance (Table 28). But when tested as a group, such effects were not manifested (Table 29).

Table 28. The SCSM mechanism → performance model when tested individually

	Security	Cost	Responsiveness	Resilience	Visibility
Control variables					
Firm size	-.089	-.031	.012	.024	.080
Past performance (profit margin)	-.031	-.055	-.025	-.012	-.039
Market share	-.028	.103	-.002	.014	-.026
Main effect					
Prevention	.894***	.587***	.726***	.783***	.737***
Model fit: $\chi^2(365)=640.42$, RMSEA=0.07, CFI=0.91, TLI=0.90, SRMR=0.08.					

	Security	Cost	Responsiveness	Resilience	Visibility
Control variables					
Firm size	-.023	-.011	.064	.083	.141*
Past performance (profit margin)	.083	.045	.068	.083	.054
Market share	.013	.104	.007	.037	-.016
Main effect					
Detection	.867***	.599***	.689***	.779***	.706***
Model fit: $\chi^2(456)=870.98$, RMSEA=0.07, CFI=0.90, TLI=0.90, SRMR=0.08.					

	Security	Cost	Responsiveness	Resilience	Visibility
Control variables					
Firm size	.108	.136	.053	.073	.031
Past performance (profit margin)	.063	.028	.047	.059	.035
Market share	-.178*	-.138†	-.080	-.080	-.009
Main effect					
Reaction	.806***	.695***	.787***	.858***	.806***
Model fit: $\chi^2(516)=951.29$, RMSEA=0.07, CFI=0.91, TLI=0.90, SRMR=0.08.					

	Security	Cost	Responsiveness	Resilience	Visibility
Control variables					
Firm size	.071	.115	.021	.029	-.003
Past performance (profit margin)	.060	.029	.048	.062	.036
Market share	-.126	-.101	-.030	-.029	.041
Main effect					
Restoration	.692***	.589***	.690***	.813***	.711***
Model fit: $\chi^2(343)=654.74$, RMSEA=0.07, CFI=0.90, TLI=0.90, SRMR=0.07.					

†$p < 0.1$, *p < 0.05, **$p < 0.01$, ***$p < 0.001$. Coefficients reported are standardized.

Table 29. The SCSM mechanism → performance model when tested as a group

	Security		Cost		Responsive-ness		Resilience		Visibility	
	Coeff.	**VIF**	**Coeff.**	**VIF**	**Coeff.**	**VIF**	**Coeff.**	**VIF**	**Coeff.**	**VIF**
Control variables										
Firm size	.027	1.52	.126	1.52	.023	1.52	.032	1.52	-.001	1.52
Past performance (profit margin)	.005	1.03	.009	1.03	.007	1.03	.020	1.03	-.004	1.03
Market share	-.085	1.56	-.083	1.56	-.027	1.56	-.015	1.56	.050	1.56
Main effects										
Prevention	-1.861	10.30	3.987	10.30	0.198	10.30	2.074	10.30	.921	10.30
Detection	2.495	10.29	-3.377	10.29	-.023	10.29	-1.728	10.29	-.622	10.29
Reaction	-.437	11.83	-1.179	11.83	.244	11.83	-.305	11.83	-.428	11.83
Restoration	.696	10.21	1.128	10.21	.809	10.21	.759	10.21	.872	10.21

$\chi^2(1542)=5250.20$, RMSEA=0.10, CFI=0.76, TLI=0.75, SRMR=0.11.

$^{\dagger}p < 0.1$, *p < 0.05, **$p < 0.01$, ***$p < 0.001$. Coefficients reported are standardized.

While multicollinearity does not reduce the predictive power or reliability of the model as a whole, it affects calculations regarding individual predictors (Chatterjee et al., 2000; Farrar and Glauber, 1967). Researchers have proposed several remedial procedures for multicollinearity (Wang, 1996). Johnston (1972) introduced three methods which were widely used to tackle multicollinearity: (1) transformation of variable(s); (2) incorporation of prior information; and (3) dropping a variable or variables from the model. However, these remedial procedures do not come without a price. Transformation of variable(s) makes the results hard to interpret. Prior information regarding the value of coefficients may not be feasible, which is true in this case as the categorization of SCSM mechanisms is new to the literature. Dropping a variable or variables may heal the statistical problem but lacks theoretical support. Hence, I opted to use the more complicated higher-order latent variable approach to deal with multicollinearity (Li, 1992; Wen and Cook, 2007). Essentially, the higher-order method suggests that there is "synergy" among the first-order factors. By constructing a second-order factor, the new model can not only alleviate numerous methodological problems

but also capture such synergy effects (Malhotra and Mackelprang, 2012). A higher-order model is also consistent with the case study results and the tenets of human immunology. As mentioned in section 2.4, the case study results suggested that only when all four classes of SCSM mechanisms were implemented, could firms effectively mitigate SCS breaches. Similarly, the human immunology literature suggests that various sub-systems of the human body need to work together to eliminate invading pathogens (Kaufmann et al., 2004; Parham, 2005; Playfair and Bancroft, 2004). The use of higher-order modeling seems to be theoretically justified for this study.

In order to assess the soundness of using second-order factor specification analytically, I followed the paradigm for examining second-order factor models proposed by Koufteros et al. (2009). This paradigm suggests a careful examination and comparison of four measurement models. In the first model, all SCSM mechanism indicators were assigned to a single first-order factor (Figure 7). In the second model, the SCSM mechanism indicators were assigned to their theoretical factors respectively (i.e., prevention, detection, reaction, and restoration) but the correlations among the four first-order factors were constrained to be zero (Figure 8). In the third model, SCSM mechanism indicators were also assigned to their theoretical factors respectively. However, the correlations among the four first-order factors were freely estimated (Figure 9). In the fourth model, a higher-order factor was constructed. It included four first-order factors: prevention, detection, reaction, and restoration (Figure 10).

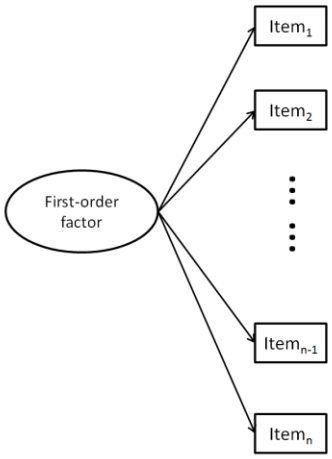

Figure 7. One first-order factor model

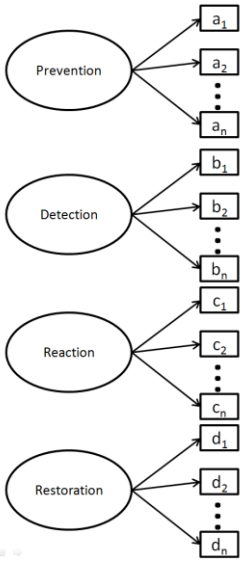

Figure 8. Four uncorrelated first-order factors model

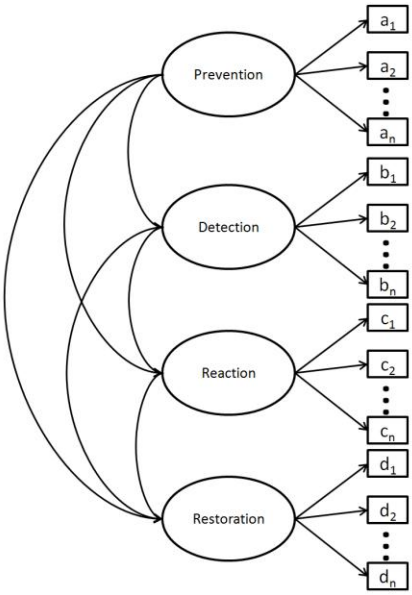

Figure 9. Four correlated first-order factors model

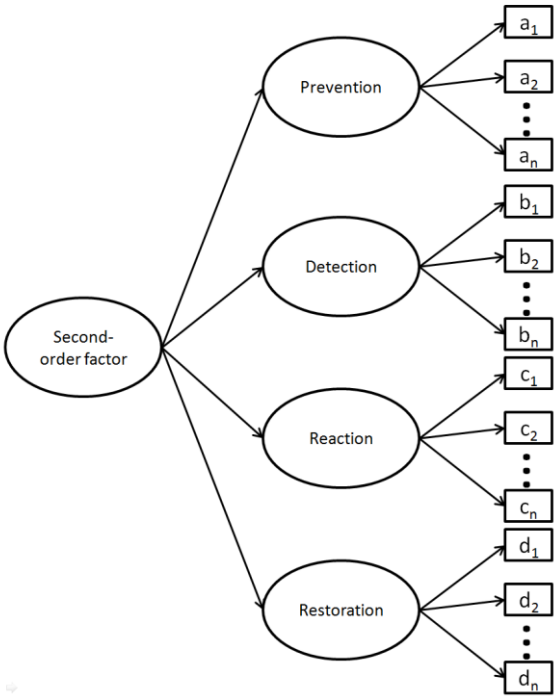

Figure 10. One second-order factor model

To compare the four proposed models and examine whether or not a second-order factor is plausible, various model fit indices can be compared. These indices serve as the "first-cut". Only models that exhibit good model fit ought to advance to the next stage of scrutiny. Therefore, model 1 and model 2 were eliminated for further consideration (see Table 30). Notice that a measurement model that generates the best model fit does not automatically secure itself as the best model. A first-order factor structure which includes correlated first-order factors always produces a better model fit than a second-order factor structure (Marsh and Hocevar, 1985; Arnau and Thompson, 2000). This advantage does not necessarily rule out the second-order factor model as an attractive candidate. In my case, the second-order model (model 4) is well-fitting and its model fit varies insignificantly from the fit generated by the first-order correlated model (model 3). The final selection should rest on theoretical soundness and methodological feasibility (Koufteros et al., 2009; Malhotra and Mackelprang, 2012). The second-order model captures the synergy effect suggested by the managers from the case studies. In addition, because only one independent variable (i.e., the second-order factor) exists in the second-order model, multicollinearity becomes a trivial issue in higher-order model specification. Owing to these merits, the second-order model was selected as the best measurement model. Table 31 reports the factor loadings of the higher-order model.

Table 30. Alternative measurement model structures

	Model 1 One first-order factor	**Model 2** Four uncorrelated first-order factors	**Model 3** Four correlated first-order factors	**Model 4** Four first-order factors and one second-order factor
χ^2(df)	1714.19(555)	3558.78(555)	1432.18(549)	1436.84(551)
χ^2/df	3.09	6.41	2.61	2.61
CFI	0.87	0.68	0.91	0.91
TFI	0.86	0.66	0.90	0.90
RMSEA	0.07	0.11	0.05	0.06
SRMR	0.06	0.46	0.05	0.05

Table 31. Factor loadings of the second-order factor model

Factor and scale items	**Measurement items**		
	Std. loading	**S.E.**	**t-value**
Prevention:			
We secure containers at our facilities to assure they are not compromised	.68	.03	21.78
Our supply chain strategy spells out security priorities	.85	.02	53.53
Our supply chain risk management strategy can be characterized as proactive	.85	.01	58.90
When it comes to supply chain security, our strategy focuses on prevention	.79	.02	41.63
We hold all suppliers accountable for supply chain security	.70	.03	27.49
We only approve suppliers (irrespective of tier) that have a risk management program in place	.70	.03	27.91
We educate suppliers about supply chain security practices	.72	.02	29.73
Detection:			
We have the ability to track and trace our cargo in real time	.63	.04	17.43
We use active measures such as video and sensors to be able to detect security breaches	.62	.04	17.01
We monitor the loading/unloading process of cargo to identify potential security breaches	.71	.03	23.76
We use sophisticated technologies to detect if containers have been compromised	.78	.02	34.37
We monitor and synthesize information regarding security breaches	.85	.02	53.05
We do conduct periodic assessments of our supply chain security	.82	.02	41.87
We have procedures to detect supply chain security failures or near failures	.71	.03	29.00
We have procedures to detect near misses in supply chain security	.81	.02	46.12
We monitor our supplier network to identify suppliers at risk	.79	.02	39.75
We have a process that notifies supply chain partners across tiers if the supply chain is threatened	.79	.02	40.83
Reaction:			
We pre-position resources to deal with crises effectively	.78	.02	33.87
We know what to do when we encounter supply chain security breaches or crises	.85	.02	5.19
We have designated a group of employees as first respondents in case of a crisis	.73	.03	26.87
There is effective communication across our supply chain when a crisis hits	.83	.02	44.37
There is a definite chain of command in case of an emergency	.76	.03	30.08
We have protocols for communication when a crisis arises	.77	.02	33.28

Table 31. continued

We have a well-defined contingency plan to react to serious supply chain security breaches	.86	.02	55.32
We have a quick reaction force to deal with a crisis or a serious disruption in our supply chain	.75	.03	29.50
We use interchangeable or generic parts as a strategy to deal with disruptions in the supply chain	.59	.04	12.41
We cross-train our employees as a mechanism to deal with potential supply chain disruptions	.76	.02	33.77
We have backup processes that can assist us at times of crises	.80	.02	41.06
We have flexible capacity contracts with suppliers in order to improve our ability to react to a crisis	.53	.04	14.52
Restoration:			
We do have a disaster recovery plan	.80	.02	37.34
We have a specific process to reinstate operations in case of a major crisis/disruption	.83	.02	44.65
We maintain strategic inventory stocks to deal with potential crises	.59	.05	10.87
We have strategies for recovery action after supply chain disruptions	.80	.02	42.08
We have strategies to use more standard parts to reduce the risk of supply chain disruptions	.65	.03	22.16
We developed alternative material sources in case of supply chain disruptions	.51	.04	13.62
Second-order factor:			
Prevention	0.93	0.01	81.54
Detection	0.91	0.01	73.55
Reaction	1.02	0.01	164.89
Restoration	1.00	0.01	120.12

Model fit: $\chi^2(551)=1436.84$, RMSEA=0.06, CFI=0.91, TLI=0.90, SRMR=0.05

After selecting a measurement model, I then specified a structural model using the same control variables to test substantive hypotheses (Figure 11). The model fit of the structural model, $\chi^2(1373)=2841.52$, RMSEA=0.05, CFI=0.91, TLI=0.90, SRMR=0.05, suggested that the model fit the data appropriately. Thus, the structural coefficients could be used to test the research hypotheses. Table 32 reports the structural coefficients. The results showed that the second-order factor revealed significant effects on all performance measures. Although I did not test the original hypotheses proposed in chapter III, the results highly suggest that SCSM mechanisms are conducive to better performance.

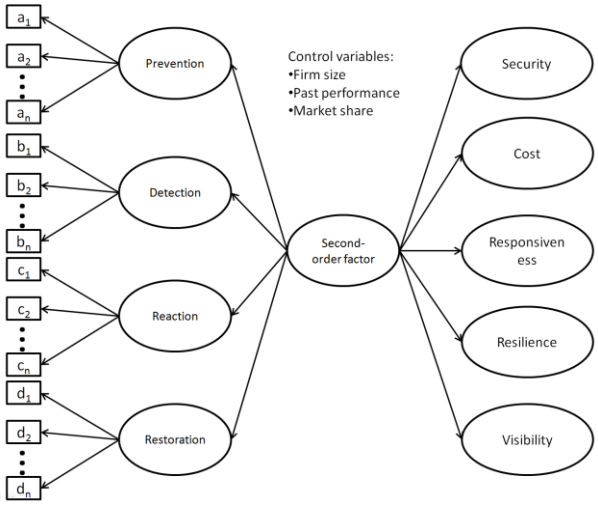

Figure 11. The second-order factor structural model

Table 32. SCSM mechanism → supply chain performance model results

Paths	Std. Coeff.	p-value	Results
SCSM mechanisms → Performance			Fully supported
Second-order factor → Supply chain security performance	0.82	0.000	
Second-order factor → Supply chain cost performance	0.57	0.000	
Second-order factor → Supply chain responsiveness	0.70	0.000	
Second-order factor → Supply chain resilience	0.79	0.000	
Second-order factor → Supply chain visibility	0.73	0.000	

Model fit: $\chi^2(1373)=2841.52$, RMSEA=0.05, CFI=0.91, TLI=0.90, SRMR=0.05.

4.4.3.5 Differential Effect of SCSM Mechanisms on Performance

H11b, H12b, H13b, and H14b posit that the coefficients relating a given class of SCSM mechanism and performance measures are different. Unlike the first group of differential hypotheses, in the second group, there is only one independent variable (i.e., one SCSM mechanism) but five different dependent variables (i.e., five performance dimensions).

In order to assess whether the relationships between a given factor of interest (e.g. prevention-oriented SCSM mechanisms) and the five performance dimensions are comparable, I ran several regression analyses. First, five regression models (one for each performance dimension) were conducted so that the effect of the variable of interest on performance can be assessed. The comparisons can be made by looking at the significance levels of Betas across equations, with the five performance dimensions as dependent variables.

While a difference in p-value for that factor's Betas across the equations is relevant to the hypotheses, more rigorous analysis can be undertaken. The conclusion that one effect is greater than the other may only be drawn when one Beta is statistically significant while the others are statistically insignificant. This study opted to adopt the rigorous procedures proposed by Madjar et al. (2009). To test whether the magnitude of the relationship between a given class of SCSM mechanism and each performance dimension is indeed statistically different requires a test of the difference of Betas for different dependent variables from the same sample (Cramer, 1997). Specifically, in order to compare the effect of prevention-oriented SCSM mechanism on supply chain security performance (prevention→ supply chain security performance) with the effect of prevention-oriented SCSM mechanism on supply chain visibility (prevention→visibility), the *standardized predicted value* of one of the two performance variables must first be derived by using prevention-oriented SCSM mechanism as an independent variable. Assuming that the standardized predicted value of supply chain security performance is acquired, the difference between the *observed* value of supply

chain visibility and the standardized predicted value of supply chain security performance is then calculated (e.g., diff = supply chain visibility – standardized predicted value of supply chain security performance). Finally, another regression is performed with prevention-oriented SCSM mechanism as the independent variable and the calculated difference (i.e., diff) as the dependent variable. Whether the difference in magnitude is statistically significant or not can be ascertained by examining the significance of the Beta coefficient in the last equation. In this example, if the Beta of prevention-oriented SCSM mechanism is negative and statistically significant in the final equation, then it is concluded that the effect of prevention-oriented SCSM mechanism on supply chain security performance is greater than its effect on supply chain visibility.

Following the procedures above, several sets of equations were analyzed. Owing to the aforementioned multicollinearity issue, only the second-order factor was examined as the synergy of the four classes of SCSM mechanisms. Since all SCSM mechanisms are essentially deployed to mitigate SCS breaches, I test a new hypothesis that the effect of the second-order factor on supply chain security performance will be stronger than its effect on other performance measures. As shown in table 33 below, the effect of the higher-order factor on supply chain security performance is indeed greater than its effect on any other performance measures.

Table 33. Test of differential effect-2

Variable of interest: the second-order factor	Std. Beta	t-value	p-value
SC cost v.s. SC security (i.e., cost-security)	-.414	-6.841	.000
SC responsiveness v.s. SC security (i.e., responsiveness-security)	-.297	-4.684	.000
SC resilience v.s. SC security (i.e., resilience-security)	-.272	-4.268	.000
SC visibility v.s. SC security (i.e., visibility-security)	-.255	-3.980	.000

4.4.3.6 Portfolio Hypothesis

The last hypothesis posits that firms with uniform-high SCSM levels outperform their peers with mixed or uniform-low SCSM levels. As mentioned in the previous chapter, this hypothesis is exploratory in nature. In order to test this hypothesis, the present study first conducted latent class analysis (LCA) to examine whether or not the firms in my sample can be appropriately categorized as uniform-high, uniform-low, and mixed (Lazarsfeld and Henry, 1968; Dillon and Mulani, 1984).

Several methods can be applied to categorize companies in my sample. One method is cluster analysis. However, cluster analysis is not based on a statistical model (Cramer, 1997). It assigns companies into groups, but it does not provide information such as the probability that a given company is a uniform-high (or uniform-low) company. Plus, cluster analysis does not provide information such as: given that a company reports high prevention ability, what is the probability that the company will be classified as a uniform-high company.

Another method is factor analysis. Factor analysis is a technique widely used with latent variables. However, one critical assumption of factor analysis is that the latent variable is continuous and normally distributed. In our case, the latent variable,

class membership, is categorical. It includes only three possible values: uniform-high, uniform-low, and mixed. Compared to the two methods, LCA is more appropriate for this study. LCA uncovers unobserved heterogeneity in a sample and aims to identify meaningful groups of subjects that are similar in their responses to measured variables (Hagenaars and McCutcheon, 2002). It allows for a latent categorical factor and provides additional information that may generate meaningful insights.

The first step of LCA is to identify the number of classes that is present in the data. I used the Vuong-Lo-Mendell-Rubin likelihood ratio test and Lo-Mendell-Rubin adjusted LRT test (Lo, Mendell, and Rubin, 2001) via Mplus 6.2.1 to identify the appropriate number of classes. The two tests are based on previous work by Vuong (1989). They compare the improvement in model fit between neighboring class models and produces a p-value to determine if statistically significant improvement exists for the inclusion of one more class (Lo, Mendell, and Rubin, 2001). Specifically, the process to determine the best number of classes is iterative. It begins by fitting a set number of classes and then iteratively adding more classes. It compares an estimated model with a model with one less class (K-1). The null hypothesis states that a model with the smaller number of classes is adequate to describe the data. Thus, if there is sufficient evidence to reject the null hypothesis (i.e., $p<.05$), a model with the higher number of classes (e.g., K) may be more adequately describing the data. Table 34 displays the results. Both tests suggested that two classes were not enough to capture the variability of the companies whereas three classes are deemed sufficient to represent the companies in my sample.

Table 34. V-L-M-R likelihood ratio test and L-M-R adjusted LRT test results

	2 (H_0) Versus 3 Classes	3 (H_0) Versus 4 Classes
V-L-M-R Likelihood Ratio Test	p-value=0.000	p-value=0.158
L-M-R Adjusted LRT Test	p-value=0.000	p-value=0.168

I then performed LCA while setting the number of classes equal to three. The first 15 cases of the LCA are demonstrated in table 35. Columns 2 to 5 display each firm's scores on prevention, detection, reaction, and restoration respectively. The next three columns report the probability of being in class 1, class 2, or class 3 respectively. The last column reports the final class a firm is assigned to. For example, based on its score on the four classes of SCSM mechanisms, firm 1 has a 0.0% chance of being in class 1 (99.4% in class 2, 0.6% in class3). For this company, class 2 is the most likely class, and Mplus indicates this information in the last column.

Table 35. LCA outputs of first 15 observations

	Prevention	Detection	Reaction	Restoration	%(C1)	%(C2)	%(C3)	Class
Firm 1	5.00	4.50	4.75	4.50	0.0%	99.4%	0.6%	2
Firm 2	3.00	2.75	4.00	4.50	43.7%	56.3%	0.0%	2
Firm 3	4.40	4.50	3.75	3.75	0.0%	100.0%	0.0%	2
Firm 4	2.20	1.50	2.25	2.75	100.0%	0.0%	0.0%	1
Firm 5	6.00	6.00	5.75	5.25	0.0%	0.0%	100.0%	3
Firm 6	5.00	5.25	5.00	5.25	0.0%	15.6%	84.4%	3
Firm 7	5.20	4.75	5.00	4.75	0.0%	60%	40%	2
Firm 8	5.00	4.75	4.75	6.00	0.0%	28.4%	71.6%	3
Firm 9	4.60	4.50	3.75	4.50	0.0%	99.9%	0.1%	2
Firm 10	4.20	3.75	4.25	5.00	0.0%	100.0%	0.0%	2
Firm 11	2.60	2.75	3.25	4.50	96.5%	3.5%	0.0%	1
Firm 12	6.60	4.75	4.00	4.50	0.0%	25.7%	74.3%	3
Firm 13	2.80	3.25	3.00	4.50	82.7%	17.3	0.0%	1
Firm 14	3.00	2.50	3.25	3.00	99.8%	0.2%	0.0%	1
Firm 15	5.20	4.00	5.25	4.50	0.0%	94.6%	5.4%	2

I further re-arranged the results based on class membership (Table 36) and plotted the mean scores on SCSM mechanisms of each class (Figure 12). The scores suggest that class 1 maps to the uniform-low class, class 2 maps to the mixed class, while class 3 maps to the uniform-high class. The results justified my prediction that firms can be characterized as uniform-high, uniform-low, or mixed.

Table 36. LCA outputs of first 15 observations—organized by class membership

	Prevention	Detection	Reaction	Restoration	%(C1)	%(C2)	%(C3)	Class
Firm 4	2.20	1.50	2.25	2.75	100.0%	0.0%	0.0%	1
Firm 11	2.60	2.75	3.25	4.50	96.5%	3.5%	0.0%	1
Firm 13	2.80	3.25	3.00	4.50	82.7%	17.3	0.0%	1
Firm 14	3.00	2.50	3.25	3.00	99.8%	0.2%	0.0%	1
Firm 1	5.00	4.50	4.75	4.50	0.0%	99.4%	0.6%	2
Firm 2	3.00	2.75	4.00	4.50	43.7%	56.3%	0.0%	2
Firm 3	4.40	4.50	3.75	3.75	0.0%	100.0%	0.0%	2
Firm 7	5.20	4.75	5.00	4.75	0.0%	60%	40%	2
Firm 9	4.60	4.50	3.75	4.50	0.0%	99.9%	0.1%	2
Firm 10	4.20	3.75	4.25	5.00	0.0%	100.0%	0.0%	2
Firm 15	5.20	4.00	5.25	4.50	0.0%	94.6%	5.4%	2
Firm 5	6.00	6.00	5.75	5.25	0.0%	0.0%	100.0%	3
Firm 6	5.00	5.25	5.00	5.25	0.0%	15.6%	84.4%	3
Firm 8	5.00	4.75	4.75	6.00	0.0%	28.4%	71.6%	3
Firm 12	6.60	4.75	4.00	4.50	0.0%	25.7%	74.3%	3

Figure 12. Mean scores of each class

H15 was then tested via ANOVA across all five performance dimensions. Table 37 displays the results. Consistent with my prediction, uniform-high companies achieved better performance in all performance measures when compared against mixed companies. So did mixed companies when compared against uniform-low companies. The results, thus, favor H15a against H15b and H15c.

Table 37. Tests of between group differences

	SC Security	SC visibility	Cost performance	SC responsiveness	SC resilience
Class 1: Uniform-low	3.23[1]	3.71	3.68	3.91	3.38
Class 2: Mixed	4.07 (0.84***)[2]	4.69(0.98***)	4.40(0.72***)	4.79(0.88***)	4.45(1.07***)
Class 3: Uniform-high	4.99 (1.76***) (0.92***)[3]	5.69(1.98***) (1.00***)	5.11(1.43***) (0.71***)	5.76(1.85***) (0.97***)	5.52(2.14***) (1.07***)

[1]: the mean score.
[2]: the mean difference when uniform-low class is used as the base class.
[3]: the mean difference when mixed class is used as the base class.
Sample size of class 1 is 90 (class 2, 187; class 3, 124).

4.5 Discussion of Results

Drawing on the institutional theory and the tenets of the human immune system, I proposed that five institutional pressures affect the four classes of SCSM mechanisms, and these SCSM mechanisms, in turn, impact supply chain performance. Two moderators, top management commitment and shared SCS perception, were hypothesized to moderate the institutional pressure-SCSM mechanism relations. I also postulated a differential effect between institutional pressures and a given class of SCSM mechanisms. The potential differential effect between a given class of SCSM mechanisms and performance measures was also explored. The results suggest that not all hypotheses are fully supported. Some of the findings are rather intriguing and counter-intuitive and, therefore, merit further investigation. I discuss these findings in detail below.

The results first show that not all institutional pressures are conducive to SCSM mechanisms (H1-H4). While many supply chain security studies reference government pressure as one of the strongest drivers that lead to the implementation of SCSM mechanisms, the results show that government pressure surprisingly reveals trivial effects on all classes of SCSM mechanisms. This is rather counter-intuitive because it is extremely difficult for companies to operate without compliance to government regulations. Thus, I believe this finding needs to be interpreted with caution. One possible and reasonable explanation for this result is that government pressure does have a sizable impact but such impact is not statistically manifested. To verify my speculation, I carefully examined the data again. I find that government pressure has the highest

mean and the second lowest standard deviation when compared with other institutional pressures. The paired sample t-tests further indicate that the mean of government pressure is statistically different from the means of other pressures. Therefore, the findings may simply suggest that the majority of firms have conformed to government pressure. The effect of government pressure does exist. But because the standard deviation is very small, such effect is not statistically manifested.

Second, the results illustrate that peer pressure has a consistent inverse effect on all classes of SCSM mechanisms. While the strategic management literature suggests that mimicking peers is one of the most predominant drivers of many organizational behaviors, my findings perhaps disclose the dark side of the mimicking process. Companies may not always benefit from the modeled processes as many peers' operational details are not clear or even imitable. This situation seems to echo the case of total quality management (TQM). Since the CEOs of IBM, P&G, Ford, Motorola, AEC, and Xerox announced that "we are absolutely convinced that TQM is a fundamentally better way to conduct business" (in an open letter sent to Harvard Business Review in 1991), firms just stopped thinking and blindly mimicked the so-called TQM philosophy. However, after waves of implementations of TQM across industries, many firms found themselves lost in the quality quandaries with little performance gains (Zbaracki, 1998). As a result, companies may intentionally avoid the bandwagon effect. My findings thus suggest that companies seem to be very cautious and prudent as it relates to the implementation of SCSM mechanisms. They do not simply surrender to peer pressure but rather treat it as a warning sign due to the potential downsides associated with it.

Regarding the differential effect of coefficients relating institutional pressures and a given class of SCSM mechanisms (H5-H8), the results suggest that government pressure does not exhibit a stronger impact on prevention- and detection-oriented SCSM mechanisms than other pressures. Indeed, as I discussed above, the effect of government pressure did not even manifest a statistically significant effect. Customer pressure, on the other hand, exhibits significant association with restoration-oriented SCSM mechanisms. However, further assessments show that the impact of customer pressure is weaker than the impact of performance pressure. The results suggest that companies do care about performance more when making decisions with respect to restoration mechanisms.

As far as the moderation effects are concerned (H9-H10), I find that shared SCS perception (SSP) only interacts with normative pressure and peer pressure to affect SCSM mechanisms. Specifically, the joint effect of SSP and normative pressure is found to enhance the implementation of prevention-oriented SCSM mechanisms whereas the joint effect of SSP and peer pressure is found to enhance the implementation of reaction- and restoration-oriented SCSM mechanisms. In other words, the results suggest that the effects of peer/normative pressure on SCSM mechanisms will be stronger when shared SCS perception is high compared to when shared SCS perception is low. Top management commitment (TMC), on the other hand, reveals significant interaction effects with government pressure and peer pressure. Contrary to my prediction, the joint effect of TMC and government pressure is found to negatively affect reaction- and restoration-oriented SCSM mechanisms. The result is understandable though. Whether or not a company can survive SCS breaches is not a major concern for a government. As

the Master Baker manager disclosed during our interview, "[government] only focuses on prevention and detection practices, at least from the seminars I've attended." In this sense, when government pressure is high, top managers would direct available resources toward prevention and detection, and, therefore, have less support to improve reaction and restoration.

In terms of the impact of SCSM mechanisms on performance (H11a, H12a, H13a, and H14a), the results provide strong empirical evidence that high levels of SCSM result in better supply chain performance. The higher-order construct reveals rather strong positive associations with all five performance measures included in this study. While the individual effect of each class of SCSM mechanisms cannot be demonstrated in an integrated structural model due to multicollinearity concerns, these effects may be manifested through post-hoc analyses. Specifically, I ran a set of regression models for each mechanism-performance pair. After controlling for firm size, firm past performance (net profit margin in the past year), market share and industry membership, all four classes of SCSM mechanisms reveal statistically significant association with performance measures.

Owing to the same multicollinearity issue, the differential effect of coefficients relating a given class of SCSM mechanisms and performance measures (H11b, H12b, H13b, and H14b) was assessed though the second-order factor as well. The results show that the effect of SCSM on supply chain security performance is stronger than its effect on other performance measures. This is somewhat intuitive because SCSM mechanisms are designed to secure the supply chain and mitigate SCS breaches.

Finally, the portfolio hypothesis (H15) was assessed via LCA and ANOVA procedures. The results show that uniform-high companies outperform their uniform-low or mixed peers across all five performance dimensions investigated. It is not surprising that uniform-high companies achieve better performance than uniform-low companies. But it is intriguing that uniform-high companies also dominate mixed companies across all performance measures. It suggests that excellence in only one or two classes of SCSM mechanisms does not help a company to achieve the best performance possible. It also appears that the "more is not necessarily good" rule (over reaction to SCS breaches may actually hurt performance) does not apply to the participating firms in my sample. The findings perhaps suggest that better SCS does drive business value. Gains in supply chain security do not compromise other performance measures. Alternatively, it is possible that companies who invest more in SCSM are also those who are the leaders in their respective market segment. They already built up competitive advantage against their competitors and thus demonstrate better performance.

CHAPTER V

CONCLUSIONS

This chapter first discusses the key contributions of this dissertation. It then highlights the implications for both academics and practitioners. This chapter ends by presenting some of the study's limitations along with future research opportunities.

5.1 Contributions

By integrating the institutional theory and the tenets of the human immune system, this study attempts to explore the antecedents as well as the consequences of four classes of SCSM mechanisms. I first define *supply chain security* based on a thorough literature review of various relevant research streams. Having SCS defined, I next propose a taxonomy of SCSM mechanisms. This taxonomy is then applied to develop a set of testable hypotheses which link institutional pressures to SCSM mechanisms and then relate SCSM mechanisms to supply chain performance. This present dissertation is the first large-scale empirical study that aims to test both the antecedents and the consequences of SCSM mechanisms. A more detailed discussion of this study's contributions follows.

The first contribution of this study is the formal conceptualization of *supply chain security*. To the best of my knowledge, this study is the first attempt to define this critical term in the supply chain security research stream. While a few related concepts, such as *supply chain security management*, were defined in the past, there was no widely

recognized definition of supply chain security. The lack of a clear and formal definition of SCS results in several difficulties for the development of SCS research. As Autry and Bobbitt (2008) summarized, the literature contains ambiguous definitions and terminology, and reveals inconsistency in theoretical development. After contrasting the meaning of "security" from the criminology, risk management, psychology, and strategic management literatures, I adopt the "end" perspective (relative to the "mean" perspective) and define supply chain security as *the absence of breaches in the supply chain*. I further list seven potential sources of supply chain security breaches: theft, product adulteration, smuggling, counterfeit products, sabotage, terrorist attacks, as well as the illicit acquisition and use of data. This definition was then validated through four case studies. It appears that practitioners also believe this is a valid definition of supply chain security. The proposed definition is neat and specific in terms of what the potential sources of SCS breaches are, and, therefore, eliminates unnecessary ambiguity and makes the concept easy to understand and measure.

The second contribution refers to the taxonomy of SCSM mechanisms. The broad scope of SCS involves necessarily numerous SCSM mechanisms which are advocated by various interest groups. Those mechanisms are discrete and scattered with various foci. A comparison of the most publicized SCS programs suggests that even governments and leading professional organizations have different perceptions of what constitutes best supply chain security management practices (Gutierrez and Hintsa, 2006). The literature has not produced a theoretical framework that can organize the SCSM mechanisms into different taxons and has failed to advocate propositions based

on theoretical argumentation. In its current status, the SCS literature is like a literature of security programs; there are many lists of what to do, but no formal guide of how to do. Leveraging the human immune system as a metaphor of a SCSM system, I posit that we can theoretically categorize SCSM mechanisms into four classes based on their intent: prevention, detection, reaction, and restoration. Such a taxonomy not only allows researchers to explore some under-studied areas (e.g., comparison of effects relating different classes of SCSM mechanisms and performance measures) but also helps managers to review their company's SCSM system and identify areas (e.g., restoration ability) that need improvement the most. This taxonomy may also apply to other research streams to help researchers generate interesting hypotheses.

The third contribution of this study is the development and validation of four SCSM mechanism constructs based on the taxonomy. This study has made a considerable effort to identify a rather broad list of SCSM mechanisms. I first employed the Q-sort method to sort various SCSM mechanisms into four classes: prevention, detection, reaction, and restoration. I next utilized four case studies to further select the most relevant mechanisms to represent each class. The four theoretical constructs were then empirically validated through a large sample collected in the U.S. and Italy. In doing so, this study conceptualizes and provides empirical evidence in support of four SCSM dimensions drawing on the human immunology literature (Kaufmann et al., 2004; Parham, 2005; Playfair and Bancroft, 2004; Segel and Cohen, 2001). As such, researchers have a new set of constructs to study SCS issues that have been shown to influence supply chain performance.

The fourth contribution rests at the empirical examination of the antecedents as well as the consequences of SCSM mechanisms. Empirical research on SCS is scant (Martens et al., 2011). Observations have shown that some firms are very proactive in implementing SCSM mechanisms while others are lagging (Kleindorfer and Saad, 2005; Martha and Subbakrishna, 2002), suggesting that the drivers of SCSM mechanisms are complex. Drawing on the institutional theory (DiMaggio and Powell, 1983; Meyer and Rowan, 1977; Powell, 1991; Scott and Meyer, 1983; Scott, 1987; Zucker 1987), this study theoretically proposes and empirically assesses five underlying antecedents of SCSM mechanisms. The results show that some institutional pressures act as predominantly powerful explanatory variables of SCSM mechanisms while other pressures appear to have negligible or even adverse effects. These findings advance our understanding in terms of what really motivates firms to support SCSM endeavors. This study also empirically examines the effects of SCSM mechanisms on supply chain performance using a large scale empirical dataset. Given the difficulty of obtaining SCS related data, few large scale empirical studies exist. I respond to this issue and provide strong evidence to support the positive effects of SCSM mechanisms as suggested by the literature (Giunipero and Eltantawy, 2004; Jüttner et al. 2003; Kleindorfer and Saad, 2005; Knemeyer et al., 2009; Speier et al., 2011;Sheffi, 2005).

The fifth contribution is to identify top management commitment and shared SCS perception as two important factors that shape the effect of institutional pressure on SCSM mechanism. My findings point out that the interactions between top management commitment and institutional pressures have mixed effects on SCSM mechanisms. For

example, while enhancing the effect of government pressure on prevention-oriented SCSM mechanisms, top management commitment also weakens the effect of government pressure on restoration-oriented SCSM mechanisms. Shared SCS perception, on the other hand, only interacts with peer pressure to enhance reaction- and restoration-oriented SCSM mechanisms. These intriguing findings have meaningful managerial implications, because they identify means through which supply chain managers are more likely to succeed in their efforts to secure the supply chains.

The sixth contribution relates to the assessment of differential effects. Two groups of differential effects were examined in this study. The findings show that coercive isomorphism (i.e., government pressure and customer pressure) does not necessarily exhibit stronger effects as the literature suggests (Williams et al., 2008) than other types of isomorphism pressures. Companies may adopt SCSM related practices because they face rather strong pressure to conform to industry norms or to improve performance. The findings also show that SCSM mechanisms reveal a stronger effect on supply chain security performance than on other performance measures. It appears that some companies attain improved cost performance (or responsiveness, etc.) because they achieve better security performance. Researchers can thus build on these results to further explore the potential mediating role of supply chain security performance.

The seventh contribution relates to methodological variety. Following the suggestion of Singhal and Singhal (2012), I employed multiple empirical methods to enhance the validity of this research. I present an innovative use of psychometric techniques. In order to operationalize the four classes of SCSM mechanisms, I applied

Q-sort procedures to categorize SCSM mechanisms which may not be appropriately categorized via exploratory factor analysis effectively. Four in-depth case studies were then employed in order to select the most representative Q-sorted items and build up confidence in using the four constructed factors. After operationalizing the four classes of SCSM mechanisms, I empirically validated them through a large sample collected in the U.S. and Italy and tested related hypotheses. This study provides a prototypical example for empiricists who intend to make use of complementary methodologies.

5.2 Implications

5.2.1 Implications for Researchers

This study presents several findings with scholarly implications. First, the institutional theory literature has a recent debate about the co-existence of institutional isomorphism and competitive isomorphism (Heugens and Lander, 2009). The old and dominant view in the literature avers that institutional isomorphism is the primary driver of organizational behaviors. The institutional environment determines what resources firms can attract by conforming to specific types of pressures, and, therefore, renders the effect of competitive isomorphism (Scott, 2001). However, recent studies suggest that competitive isomorphism is also impactful (Heugens and Lander, 2009). The new view is more acceptable to economists and organizational sociologists alike as it emphasizes that market competition weeds out less efficient practices in favor of more efficient ones. By integrating both types of isomorphism in the theoretical model, this study shows that the two types of isomorphism affect SCSM mechanisms simultaneously. In other words,

the findings suggest that institutional isomorphism and competitive isomorphism are commensal rather than mutually exclusive. They co-exist and affect firms collectively. The dissertation thus provides evidence for scholars to seriously consider including competitive isomorphism (i.e., performance pressure in this study) in future institutional theory related studies.

Second, the present study is the first attempt to relate immunology theories to SCS research. By utilizing the human immune system as an analog to the SCSM system, I propose a taxonomy of SCSM mechanisms. I also rely on the principles regarding how the human immune system battles against invading pathogens in order to provide theoretical support for the differential effect hypotheses. As such, this study serves as a prototypical example of applying a natural science theory to solve a social science problem. It suggests that supply chain management scholars may find more useful theories by extending their search of good theories to a broader set of disciplines, including those that are generally considered as natural science disciplines.

Third, the proposed taxonomy applies not only to SCSM mechanisms but also to other organizational strategies and practices. For example, the same taxonomy may also be useful to group quality management practices. Inspection of raw materials and finished products can be labeled as detection-oriented. Product recall, on the other hand, can be prescribed as reaction-oriented. These activities may have different financial implications to firms. Putting them into different categories is advantageous to reveal their differential effect on firm performance. In this sense, the taxonomy provides

researchers a new perspective to look at organizational practices and potentially generate new and interesting research questions.

Finally, this study also carries a methodological implication. It presents an example of the innovative use of multiple empirical methods to enhance research validity. The Q-sorting method, which is widely used in the psychological literature, was employed to select appropriate SCSM mechanisms to underline each latent factor suggested by the taxonomy. A case-based qualitative approach was then deployed to justify that taxonomy and further select most representative items for each construct. Finally, a large sample was used to validate the four constructs and test substantive hypotheses. The combination of both qualitative and quantitative methods makes the findings of this study reliable as some drawbacks of using a single method are overcome.

5.2.2 Implications for Practitioners

This study provides several valuable insights to assist practitioners. First, while the literature suggests that conformity to government pressure may lead to performance gains (e.g., Closs and McGarrell, 2004; Peleg-Gillai et al., 2006; Rice and Spayd, 2005), firms must realize that these potential benefits are unlikely to transform into competitive advantage. As I discussed before, my results perhaps suggest that government pressure is omnipresent such that almost all firms have conformed to it. Subsequently, the implementation of government specified mechanisms will not lead firms to standout against competition. Alternatively, the results can be interpreted as a caveat. While Oliver (1991) argues that under some circumstances firms may employ strategies such as

avoidance and manipulation to indirectly disregard or change government requirements, my results suggest that in the context of supply chain security, these strategies will make firms less competitive as many other firms have acquiesced to the government demands. In other words, firms need to carefully adhere to government issued SCS regulations not only to stay legal but also to avoid falling behind competition.

Second, the findings suggest that different stakeholders (e.g., government, customer, etc.) have different perceptions with respect to SCSM mechanisms. Customers (buying firms) seem to care more about restoration than the other three classes. On one hand, customers may agree that a supply chain disruption is by its very nature inevitable. On the other hand, they want the right products in the right place at the right time with low cost (Fisher, 1997). In some extreme conditions, customers are not willing to compromise their on-time delivery performance for better SCS performance (Voss et al., 2009a). Smooth and stable material supply is rather critical to their own operations. As a result, the way suppliers respond to disruptions and restore normal operations on the aftermath of SCS breaches becomes rather important to their customers. Operations managers should utilize this finding in order to design specific strategies to satisfy customers well.

Third, the interactions between top management commitment and institutional pressures raise several recommendations for supply chain managers to achieve better security performance. Top managers have more significant influence than supply chain managers in that these executives can decide which functional managers to reward, promote, or fire, as well as design the firm's overarching strategies. However, supply

chain managers can also influence the top managers primarily by means of issue selling and initiative taking (Bouquet and Birkinshaw, 2008 a, b). Our results show that top management commitment can interact with peer pressure and performance pressure to positively affect the adoption of SCSM mechanisms. As such, supply chain managers should advocate the importance of modeling after peers and promote the collateral benefits of SCSM mechanisms through their contacts with top managers to advance the implementation of SCSM mechanisms. Our results also show that shared SCS perception interacts with peer pressure to positively affect reaction and restoration SCSM mechanisms. It reveals that cultivating a security oriented organizational culture is conducive to high levels of SCS. Therefore, supply chain managers should again influence top managers through issue selling to promote shared SCS perception within their organization.

Fourth, the taxonomy provides supply chain managers a new tool to evaluate the status of their SCSM system. The four classes of SCSM mechanism can be essentially used as four measures. Supply chain managers may use them to identify areas that their company needs to improve. For example, an evaluation may suggest that a firm has high levels of prevention but very low levels of reaction. Reaction-oriented SCSM mechanisms would thus become a focus for that firm to improve SCS performance next. The four mechanisms can also be used to compare companies operating in the same industry. Such comparison keeps supply chain managers informed about their company's status relative to rivals. Note that while the taxonomy was proposed for SCSM mechanisms, it can also be used outside the SCSM arena.

Finally, this study somewhat demonstrates differential effects of SCSM mechanisms on supply chain performance. In practice, firms always face a situation where resources are scarce. They may not implement all practices they need simply because they cannot afford all of them. The results regarding differential effects can thus be used to support decision-making. Managers can intentionally and wisely focus on only one class of SCSM mechanisms at a time according to their firm's specific resource constraints and that particular class's effect on desirable performance outcomes.

5.3 Limitations

This study is not immune to limitations, which are discussed below in some detail. First, data were collected from one respondent from each participating firm. A single respondent approach may not be able to provide reliable information regarding complex organizational behaviors (Venkatraman and Grant, 1986). This approach also precludes me from examining inter-rater reliability. While I performed tests for common method bias and conducted case studies to enhance research validity, it would be useful if multiple responses can be collected from each company (McFadden et al., 2009).

Second, because this research is cross-sectional, it only provides a "snapshot" of the operations of the participating firms. This inherent flaw renders my ability to evaluate how SCSM mechanisms actually get implemented, readjusted, or annulled over time. Certainly these themes are important topics for future longitudinal studies.

Third, while the four SCSM mechanism constructs were empirically validated, the manifest variables of these constructs were selected based on subjective methods. A

Q-sort approach and qualitative interviews were employed to select these manifest variables. Although the objectivity of the Q-sort (Brown, 1980; Thomas and Baas, 1992) and case study (Wu and Choi, 2005) results should not be a concern for this study, I acknowledge that it is possible that some important manifest variables are missing. After all, the final manifest items were selected based on interviews with four companies and these companies may not have implemented an exhaustive array of SCSM mechanisms.

Fourth, as discussed in chapters III and IV, different SCSM mechanisms could "fertilize" each other. This is somewhat "illustrated" by the multicollinearity issue of the four mechanism classes. The differential effect of SCSM mechanism on supply chain performance was, thus, assessed through a higher-order construct instead. The higher-order construct did reveal a statistically significant association with performance measures. Nevertheless, it would be more informative if the four SCSM constructs can be individually examined as the results may generate meaningful insights regarding the mechanism-performance linkage.

Finally, a survey-based method offers the advantage of collecting a large amount of data to identify relationships of interest. However, such information does not go deeply beyond the surface (Kerlinger, 1986). The data may be useful in demonstrating associations among variables, but it may not always answer "why" these associations exist. While the institutional theory and the tenets of human immunology are theoretically well-grounded, follow-up ethnographic studies would be worthwhile to explore the same phenomena in a real-life context (Yin, 1981).

5.4 Future Research

This study provides several potential opportunities for future research. First, with regard to the limitations mentioned in section 5.3, there is a clear need to repeat this study in order to create longitudinal comparisons. The SCSM mechanisms are evolving, so is the institutional environment. It would be valuable to collect longitudinal data to assess how the relationships proposed in this study change over time.

Second, a better understanding of how institutional pressures interact with contextual factors to affect SCSM mechanisms is necessary to advance the SCS literature. Although this study focuses on the moderating role of top management commitment and shared SCS perception, future studies might examine other important factors. For example, the effect of institutional pressure on SCSM mechanisms may vary under different ownership configuration. Depending on whom the dominant owner is (family, venture capitalist, pension plan, the public, etc.), the degree of security a specific firm needs may vary, and, thus, firms may respond to institutional pressures differently.

Third, the statistical results suggest that the effect of SCSM mechanisms on supply chain security performance is stronger than its effects on other performance measures. The results perhaps suggest that SCS performance partly mediates the relationship between SCSM mechanisms and other supply chain performance dimensions. For example, the reduction of overall operational costs may be achieved in part because SCSM mechanisms help improve operational efficiency and in part because supply chain security performance is enhanced (e.g., fewer thefts). Future studies may

examine whether or not this mediation effect does exist and enhance our understanding of the SCSM mechanism-performance link.

Fourth, future studies should explore the potential comprehensive role of SCSM mechanisms. While the results suggest that it is the synergy of the four classes of SCSM mechanisms that really matters, it does not completely rule out the possibility that SCSM mechanisms could substitute for each other. Theoretically, an extremely high level of a given class of SCSM mechanisms reduces the need of other classes. For example, if a company can effectively prevent potential SCS breaches from happening, it probably would not need to invest significantly to get ready to respond to SCS breaches. In this sense, SCSM mechanisms are comprehensive. Understanding with this regard would help practitioners to better manage their limited resources.

Finally, the data were collected from companies within both the U.S. and Italy. Given the security policy differences among geographic regions, it would be meaningful to engage in comparative studies. For example, the Italian companies have to conform not only to supply chain security regulations issued by their government, but also to related legislations launched by the European Union. This fact may enable a comparative study that sheds light on the organizational responses to government pressure. In a similar vein, firms across diverse industries may be sensitized to SCS breaches differentially and therefore reveal various patterns when it comes to the implementation of SCSM mechanisms. This offers another opportunity to conduct a study providing useful insights into the effect of industry membership.

REFERENCES

ABC News, 2010. Clues Sought in $75 Million Record-Breaking Drug Heist. Reported by Denies, Y., FERRAN, L., available at: http://abcnews.go.com/GMA/TheLaw/75-million-drugs-stolen-dramatic-connecticut-heist/story?id=10133205#.T3x29tXy83E.

Ahire, S.L., O'Shaughnessy, K.C., 1998. The role of top management commitment in quality management: an empirical analysis of the auto parts industry. International Journal of Quality Science 3(1), 5-37.

Aiken, L.S., West, S.G., 1991. Multiple Regression: Testing and Interpreting Interactions. Newbury.

Armstrong, J.S., Overton, T.S., 1977. Estimating nonresponse bias in mail surveys. Journal of Marketing Research 14, 396-402, 1977.

Arnau, R.C., Thompson, B., 2000. Second-order confirmatory factor analysis of the WAIS-III. Assessment 7 (3), 237–246.

A.T. Kearney Analysis, 2010. Consumer product fraud: deterrence and detection. Available at: http://www.gmaonline.org/downloads/research-and-reports/consumerproductfraud.pdf. [last accessed, August 03, 2012].

Atwater, C., Gopalan, R., Lancioni, R., Hunt, J., 2010. To change or not to change: How motor carriers responded following 9/11. Journal of Business Logistics 31(2), 129-155.

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

Bagozzi, R.P., Yi, Y., Phillips, L.W., 1991. Assessing construct validity in organizational research. Administrative Science Quarterly 36, 421–458.

BankersOnline.com, 2013. How do you recover from a security breach? Know how to respond even before it happens. Available at: http://www.bankersonline.com/vendor_guru/redsiren/redsiren_securitybreach.html. [last accessed: May 13, 2013].

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

Bakshi, N., Flynn, S.E., Gans, N., 2011. Estimating the operational impact of container inspections at international ports. Management Science 57(1), 1–20.

Baruch, Y., 1999. Response rate in academic studies. Human Relations 52(4), 421-438

Baum, J.A.C., Oliver, C., 1991. Institutional linkages and organizational mortality. Administrative Science Quarterly 36, 187–218.

Berger, P. L., Luckmann, T., 1966. The social construction of reality. New York: Doubleday.

BIS report, 2010. Detection and avoidance of counterfeit electronic parts. Available at: www.pscouncil.org%2FPolicyIssues%2FLegislation%2FNDAA%2FARWG_FY12_NDAA_Comments___Appendix_B.aspx&ei=cYOZUajTLo_i9gTrwYHICw

&usg=AFQjCNGMmB8xOYMm6fubIJ8Yaof8_Ra19g&sig2=B3gy2ekE-jFSR-HGehWoxg&bvm=bv.46751780,d.aWM. [Last assessed: August 03, 2012].

Blankenship, A.B., Breen, G.E., 1992. State of the Art Marketing Research. Ch. 7, Choosing the method of collecting data, 121-165.

Block, J., 1961. The Q-sort method in personality assessment and psychiatric research. Springfield, IL: Charles C. Thomas.

Bob, Fernandez, 2001. U.S. markets decline again. KRTBN Knight Ridder Tribune Business News (The Philadelphia Inquirer, September 22, 2001).

Bollen, K.A., 1989. Structural Equations with Latent Variables. New York: John Wiley & Sons, Inc.

Bouquet, C., Birkinshaw, J., 2008a. Weight versus voice: how foreign subsidiaries gain attention from corporate headquarters. Academy of Management Journal 51, 577–601.

Bouquet, C., Birkinshaw, J., 2008b. Managing power in the multinational corporation: how low-power actors gain influence. Journal of Management 34, 477–508.

Bowden, A., 2010. The economic cost of maritime piracy. One Earth Future Working Paper, available at: http://oceansbeyondpiracy.org/sites/default/files/documents_old/The_Economic_Cost_of_Piracy_Full_Report.pdf

Braunscheidel, M.J., Suresh, N.C., 2009. The organizational antecedents of a firm's supply chain agility for risk mitigation and response. Journal of Operations Management 27(2), 119-140.

Brislin, R. W. 1980. Translation and content analysis of oral and written materials. In H. C. Triandis & J. W. Berry (Eds.), Handbook of cross-cultural psychology: Methodology, vol. 2: 389–444. Boston: Allyn & Bacon.

Broder, J.F., 1984. Risk Analysis and the Security Survey. Butterworth Publishers.

Brooks, D.J., 2010. What is security: definition through knowledge categorization. Security Journal 23, 225–239.

Brown, S.R., 1980. Political subjectivity: Applications of Q methodology in political science. Yale University Press.

Brown, S.R., 1993. A primer on Q methodology. Operant Subjectivity 16, 91-138.

Carroll, G. R., Hannan, M. T., 1989. Density dependence in the evolution of populations of newspaper organizations. American Sociological Review 54, 524-541.

Chao, S., Lin, P., 2009. Critical factors affecting the adoption of container security service: The shippers' perspective. International Journal of Production Economics122, 67-77.

Chatterjee, S., Hadi, A.S., Price, B., 2000. Regression Analysis by Example, 3rd Edition, A Wiley-Interscience Publication, John Wiley and Sons.

Chopra, S., Sodhi, M.S., 2004. Managing risk to avoid supply-chain breakdown. MIT Sloan Management Review 46 (1), 53–61.

Christopher, M., Peck, H., 2004. Building the resilient supply chain. The International Journal of Logistics Management 15(2), 1-13.

Closs, D.J., McGarrell E.F., 2004. Enhancing security throughout the supply chain. Special Report Series, IBM Center for the Business of Government, available at: https://www-304.ibm.com.

Closs, D.J., Speier, C., Whipple, J. Voss, M.D., 2008. A framework for protecting your supply chain. Supply Chain Management Review 12(2), 38-45.

CNN, 2009. Drug smugglers becoming more creative, U.S. agents say. Available at: http://articles.cnn.com/2009-04-16/justice/creative.drug.smugglers_1_drug-traffickers-smuggling-mexican-border?_s=PM:CRIME. [Last accessed: August 03, 2012].

CNN, 2011. Drug theft goes big. Available at: http://features.blogs.fortune.cnn.com/2011/03/31 /drug-theft-goes-big/. [Last accessed: August 03, 2012].

Cortina, J.M., 1993. What is coefficient alpha? An examination of theory and applications. Journal of Applied Psychology 78, 98–104.

Craighead, G., 2003. High-Rise Security and Fire Life Safety. Woburn, MA: Butterworth-Heinemann.

Craighead, C.W., Blackhurst, J., Rungtusanatham, M.J., Handfield, R.B., 2007. The Severity of Supply Chain Disruptions: Design Characteristics and Mitigation Capabilities. Decision Sciences 38(1), 131-157.

Cramer, D., 1997. Basic Statistics for Social Research. Routledge.

Cronbach, L.J., 1951. Coefficient alpha and the internal structure of tests. Psychometrika 16 (3), 297–334.

Croxton, K.L., 2003. The order fulfillment process. International Journal of Logistics Management 14(1), 19–32.

Cyert, R.N., March, J.G., 1963. A Behavioral Theory of the Firm. Prentice-Hall, Englewood Cliffs, NJ.

Davidson, M.A., 2005. A matter of degrees. Security Management 49(12), 72-99.

Deephouse, D. L., 1999. To be different, or to be the same? It's a question (and theory) of strategic balance. Strategic Management Journal 20, 147–166.

Deephouse, D. L., Suchman, M.C., 2008. Legitimacy in organizational institutionalism. In Greenwood, R., Oliver, C. Sahlin, K., & Suddaby, R. (eds.), The Handbook of Organizational Institutionalism, 49–77. Thousand Oaks, CA: Sage.

Department of Homeland Safety (DHS) Report, 2007. Strategy to enhance international supply chain security. Available at: https://www.dhs.gov.

DeVellis, R.F., 1991. Scale Development: Theory and Applications. Newbury Park, CA: Sage Publications.

Dillman, D.A., Smyth, J.D., Christian, L.M., 2009. Internet, Mail and Mixed-mode Surveys: The Tailored Design Method. (3rd ed.). New York: Wiley.

Dillon, M., 1996. The Politics of Security. London: Routledge.

Dillon, W.R., Mulani, N., 1984. A probabilistic latent class model for assessing inter-judge reliability. Multivariate Behavioral Research 19, 438-458.

DiMaggio, P.J., Powell, W.W., 1983. The iron cage revisited: institutional isomorphism and collective rationality in organizational fields. American Sociological Review 48 (2), 147–160.

Djavanshir, G.R., Khorramshahgol, R., 2006. Applications of chaos theory for mitigating risks in telecommunications systems planning in global competitive markets. Journal of Global Competitiveness 14 (1), 15–24.

Dobrzykowski, D., Tran, O. Tarafdar, M., 2010. Value co-creation and resource based perspectives for strategic sourcing. Strategic Outsourcing: An International Journal 3(2), 106-127.

Dubin, R., 1978. Theory Building. Revised edition. The Free Press, New York.

Edmondson, A.C., McManus, S.E., 2007. Methodological fit in management field research. Academy of Management Review 32, , 1155-1179.

Eisenhardt, K.M., 1989. Building theories from case study research. Academy of Management Review 14, 532-550.

Ekwall, D., 2009. The displacement effect in cargo theft. International Journal of Physical Distribution & Logistics Management 39(1), 47-62.

Elkins, D., Handfield, R.B., Blackhurst, J., Craighead, C.W., 2005. 18 Ways to Guard Against Disruption. Supply Chain Management Review 9 (1), 46–53.

Erdos, P.L., 1970. Professional Mail Surveys. McGraw-Hill, New York, NY.

Faisal, M.N., Banwet, D.K., Shankar, R., 2006. Supply chain risk mitigation: modeling the enablers. Business Process Management Journal 12 (4), 535–552.

Farrar, D.E., Glauber, R.R., 1967. Multicollinearity in regression analysis: the problem revisited, The Review of Economics and Statistics 49(1), 92-107.

Finkelstein, S., Hambrick, D.C., Cannella, A., 2008. Strategic Leadership: Theory and Research on Executives, Top Management Teams, and Boards. Oxford University Press, Oxford, UK.

Fischer, R.J., Green, G., 2004. Introduction to Security. 7th ed., Butterworth-Heinemann, Boston, MA.

Fisher, M.L., 1997. What is the right supply chain for your product? Harvard Business Review 75(2), 105–116.

Fletcher, T., 2007. It's your supply chain — secure it! CSCMP's Supply Chain Quarterly, quarter 4 2007, available at: http://www.supplychainquarterly.com/print/scq200704security/. [Last accessed: August 03, 2012].

Floyd, S.W., Lane, P.J., 2000. Strategizing throughout the organization: managing role conflict in strategic renewal. Academy of Management Review 25, 154–177.

Flynn, S.E., 2008. Overcoming the flaws in the U.S. government efforts to improve container, cargo, and supply chain security. Testimony before the Homeland Security Appropriations Subcommittee. U.S. House of Representatives, April 2, 2008.

Flynn, B.B., Sakakibara, S., Schroeder, R.G., Bates, K.A., Flynn, E.J., 1990. Empirical research methods in operations management. Journal of Operations Management 9 (2), 250–284.

Fornell, C., Larcker, D.F., 1981. Evaluating structural equation models with unobservable variables and measurement errors. Journal of Marketing Research 18(1), 39-50.

Foxnews, 2012. Government to warn motorists tens of thousands may have counterfeit air bags. Available at: http://www.foxnews.com/leisure/2012/10/10/government-to-warn-motorists-tens-thousands-may-have-counterfeit-air-bags/. [Last accessed: April 03, 2012].

Frank, G.H., 1956. Note on the reliability of Q-sort data. Psychological Reports 2(3), 182.

Read more: http://www.foxnews.com/leisure/2012/10/10/government-to-warn-motorists-tens-thousands-may-have-counterfeit-air-bags/#ixzz2Tm4Pt3fm

Gibbons, J.D., Chakraborti, S., 2003. Nonparametric Statistical Inference. 4th Edition, CRC Press.

Glaser, B.G., Strauss, A.L., 1967. The Discovery of Grounded Theory: Strategies for Qualitative Research. Aldine, Chicago, Illinois.

Gneezy, U., List, J.A., Wu, G., 2006. The uncertainty effect: when a risky prospect is valued less than its worst possible outcome. Quarterly Journal of Economics 121, 1283–1309.

Goldberg, R., Herman, K., 2006. Nestle's milk district model: economic development for a value-added food chain and improved nutrition. Harvard Business Case Study, No. 9-906-406.

Goh, M., Lim, J.Y.S., Meng, F., 2007. A stochastic model for risk management in global supply chain networks. European Journal of Operational Research 182 (1), 164–173.

Gutierrez, X., Hintsa, J., 2006. Voluntary supply chain security programs: a systematic comparison. The International Conference on Information System, Logistics and Supply Chain, Lyon France.

Hagenaars, J.A., McCutcheon, A.L., 2002. Applied Latent Class Analysis Models. Cambridge University Press.

Haimes, Y., 1998. Risk Modeling, Assessment and Management. John Wiley, New York, NY.

Hair, J.F. Jr., Anderson, R.E., Tatham, R.L., Black, W.C., 1998. Multivariate Data Analysis (5th ed.). Upper Saddle River, New Jersey: Prentice Hall.

Hair, J.F. Jr., Black, W., Babin, B., Anderson, R., and Tatham, R. (2006). Multivariate Data Analysis, Sixth edition. Pearson Prentice Hall: Upper Saddle River, NJ.

Hambrick, D.C., 2007. Upper echelons theory: an update. Academy of Management Review 32 (2), 334–343.

Hambrick, D.C., Mason, P.A., 1984. Upper echelons: the organization as a reflection of its top managers. Academy of Management Review 9 (2), 193–206.

Helferich, O.K., Cook, R.L., 2002. Securing the Supply Chain. Council of Supply Chain Management Professionals, Oak Brook, IL.

Helferich, O.K., Cook, R.L., 2007. Chapter 29: Global supply chain security. In Mentzer, J., Myers, M., Stank, T., (ed.) Handbook of global logistics and supply chain management. Sage Publications, Thousand Oaks, CA.

Hempel, C.G., 1970. Methods of concept formation in science. In Neurath, O., Carnap, R., Morris, C. (Eds), Formations of unity of science. University of Chicago Press, Chicago.

Hendricks, K.B., Singhal, V.R., 2003. The effect of supply chain glitches on shareholder value. Journal of Operations Management 21 (5), 501–523.

Hendricks, K.B., Singhal, V.R., 2005. An empirical analysis of the effect of supply chain disruptions on long-run stock price performance and equity risk of the firm. Production and Operations Management 14 (1), 35–52.

Heugens P., Lander, M.W., 2009. Structure! Agency! (And other quarrels): a meta-analysis of institutional theories of organization. Academy of Management Journal 52(1), 61-85.

Homeland Security Report, 2006. Targets for terrorism: food and agriculture. Available at: http://www.cfr.org/homeland-security/targets-terrorism-food-agriculture/p10197. [Last accessed: August 03, 2012].

Hoffman, A.J., 1999. Institutional evolution and change: environmentalism and the U.S. chemical industry. Academy of Management Journal 42, 351-371

Hunt, S.D., 1991. Modern Marketing Theory: Critical issues in the philosophy of marketing science. Southwestern Publishing Co., Cincinnati, OH.

IHS Global Insight, 2009. Commerce & Transport Industry Analysis. Available at: http://www.ihs.com/products/global-insight/industry-analysis. [Last accessed: August 03, 2012].

Janeway, C.A., Jr., 1989. Approaching the asymptote? Evolution and revolution in immunology. Cold Spring Harbor Symposia on Quantitative Biology 54, 11-13.

Janeway, C.A., Jr., 1992. The immune system evolved to discriminate infectious nonself from noninfectious self. Immunology Today 13, 11-16.

Johnston, J., 1972. Econometric Methods. McGraw-Hill, New York, NY.

Jones, T., Newburn, T., 1998. Private Security and Public Policing. Oxford: Clarendon Press.

Joossens, L., Merriman, D., Ross, H., Raw, M., 2011. How eliminating the global illicit cigarette trade would increase tax revenue and save lives. International Union Against Tuberculosis and Lung Disease Report. Available at: http://www.worldlungfoundation.org/ht/a/GetDocumentAction/i/6535. [Last accessed: August 03, 2012].

Kahneman, D., Tversky, A., 1979. Prospect Theory: An Analysis of Decision under Risk. Econometrica 47(2), 263-292.

Kaplan, A., 1964. The conduct of inquiry: Methodology for behavioral sciences. Chandler Publishing Company, San Francisco, CA.

Kaufmann, S.H.E., Medzhitov, R., Gordon, S., (eds.), 2004. The innate immune response to infection. ASM press, Washington, D.C.

Kendall, M.G., Stuart, A., 1969. The Advanced Theory of Statistics, Volume 1: Distribution Theory, 3rd Edition, Griffin.

Kennedy, M.T., Fiss, P.C., 2009. Institutionalization, framing, and the logic of TQM adoption and implementation decisions among U.S. hospitals. Academy of Management Journal 52, 897–918.

Kerlinger, F.N., Lee, H.B., 1986. Foundations of Behavioral Research. McGraw Hill: New York, NY.

Ketokivi, M.A., Schroeder, R.G., 2004. Strategic, structural contingency and institutional explanations in the adoption of innovative manufacturing practices. Journal of Operations Management 22(1), 63-89.

Khalifa, M., Davison, M., 2006. SME adoption of IT: the case of electronic trading systems. IEEE Transactions on Engineering Management 53(2), 275-284.

King, A., Lennox, M., 2001. Who adopts management standard early? An examination of ISO 14001 certifications. In Nagao, D. (eds.), Best Paper Proceedings: Fifty-Ninth Meeting of the Academy of Management, A1-A6, Washington, DC.

Kirkman, B.L., Chen, G., Farh, J., Chen, Z.X., Lowe, K.B., 2009. Individual power distance orientation and follower reactions to transformational leaders: a cross-level, cross-cultural examination. Academy of Management Journal 52(4), 744-764.

Kleindorfer, P.R., Saad, G.H., 2005. Managing disruption risks in supply chains. Production and Operations Management 14 (1), 53–68.

Knemeyer, A.M., Zinn, W., Eroglu, C., 2009. Proactive planning for catastrophic events in supply chains. Journal of Operations Management 27, 141-153.

Koufteros, X.A., Marcoulides, G.A., 2006. Product development practices and performance: A structural equation modeling-based multi-group analysis. International Journal of Production Economics 103, 286-307.

Koufteros X.A., Babbar, S., Kaighobadi, M., 2009. A paradigm for examining second-order factor models employing structural equation modeling. International Journal of Production Economics 120 (2), 633–652.

Krause, D.R., 1999. The antecedents of buying firms' efforts to improve suppliers. Journal of Operations Management 17(2), 205–224.

Kutner, M.H., Nachtsheim, C.J., Neter, J., Li, W., 2004. Applied Linear Statistical Models. Fifth edition, Richard D. Irwin, Inc.

Kyero, 2011. €15m of cocaine found in fake bananas. Available at: http://live.kyero.com/2011/01/13/e15m-cocaine-found-in-fake-bananas/. [Last accessed: August 03, 2012].

Ladendorf, K., 2011. Thailand floods leave mark on key semiconductor players Intel, Dell, AMD. STATESMAN, Dec. 12, 2011. Available at: http://www.statesman.com/business/technology/thailand-floods-leave-mark-on-key-semiconductor-players-2028379.html.

Lazarsfeld, P.F., Henry, N.W., 1968. Latent Structure Analysis, Boston: Houghton Mifflin.

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

Lee, H.L., Wolfe, M., 2003. Supply chain security without tears. Supply Chain Management Review (Jan/Feb), 12-20.

Li, K.C., 1992. On principal Hessian directions for data visualization and dimension reduction: another application of Stein's lemma. Journal of the American Statistical Association 86, 316-342.

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

Lo, Y., Mendell, N.R., Rubin, D.B., 2001. Testing the number of components in a normal mixture. Biometrika 88, 767-778.

Lounsbury, M. (2007). A tale of two cities: competing logics and practice variation in the professionalizing of mutual funds. Academy of Management Journal 50, 280 –307.

Madjar, N., Greenberg, E., Chen, Z., 2011. Factors for radical creativity, incremental creativity, and routine, noncreative performance. Journal of Applied Psychology 96, 730-743.

Malhotra, M.K., Grover, V., 1998. An assessment of survey research in POM: from constructs to theory. Journal of Operations Management 16, 407-425.

Malhotra, M.K., Mackelprang, A.W., 2012. Are internal manufacturing and external supply chain flexibilities complementary capabilities? Journal of Operations Management 16, 407-425.

Mangan, J., Christopher, M., 2005. Management development and the supply chain manager of the future. International Journal of Logistics Management 16 (2), 178–191.

Manuj, I., Mentzer, J.T., 2008. Global supply chain risk management. Journal of Business Logistics 29(1), 133-156.

Manunta, G., 1999. What is security? Security Journal 12(3), 57-66.

Manunta, G., 2002. Risk and security: are they compatible concepts? Security Journal 15(2), 43-55.

Manunta, G., Manunta, R., 2006. Theorizing about security. In Gill, M., (eds.) The Handbook of Security. New York: Palgrave Macmillan, 629-657.

March, J.G., Olsen, J.P., 1976. Ambiguity and choice in Organization. Universitetsforlaget, Bergen,

Marsh, H.W., Hocevar, D., 1985. Application of confirmatory factor analysis of the study of selfconcept: first and higher order factor models and their invariance across groups. Psychological Bulletin 97(3), 562–582.

Martha, J., Subbakrishna, S., 2002. Targeting a just-in-case supply chain for the inevitable next disaster. Supply Chain Management Review, Sept. Available at: http://www.highbeam.com/doc/1G1-91562584.html. [last accessed: August 3, 2012]

Martens, B.J., Crum, M.R., Poist, R.F., 2011. Examining antecedents to supply chain security effectiveness: an exploratory study. Journal of Business Logistics 32, 153–166.

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

Matzinger P., 1994. Tolerance, danger and the extended family. Annual Review of Immunology 12, 991-1045.

Matzinger, P., 1998. An innate sense of danger. Seminars in Immunology 10, 399-415.

McCutcheon, D., Meridith, J., 1993. Conducting case study research in operations management. Journal of Operations Management 11 (3), 239–256.

McFadden, K.L., Henagan, S.C., Gowen, C.R., 2009. The patient safety chain: transformational leadership's effect on patient safety culture, initiatives, and outcomes. Journal of Operations Management 27, 390-404.

Meehl, P.E., 1956. Wanted – a good cookbook. American Psychologist, 11(6), 263-272.

Mena, C., Humphries, A., Wilding, R., 2009. A comparison of inter- and intra-organizational relationships: two case studies from UK food and drink industry. International Journal of Physical Distribution & Logistics Management 39(9), 762-784.

Meyer, J.W., Rowan, B., 1977. Institutionalized organizations: formal structure as myth and ceremony. American Journal of Sociology 83 (2), 340–363.

Meyer, J. W., Rowan, B., 1991. Institutionalized organizations: formal structure as myth and ceremony. In Powell, W. W. & DiMaggio, P. J. (eds.), The New Institutionalism in Organizational Analysis, 41-62. University of Chicago Press, Chicago.

Miles, M.B., Huberman, A.M., 1994. Qualitative Data Analysis: Grounded Theory Procedures and Techniques. Sage Publications, London.

Miller, D.C., 1991. Handbook of Research Design and Social Measurement, 5th edition. Sage Publications: Newbury Park, CA.

Moon, B., 2008. August 14, 2003: Remembering the Great Blackout. Wired, Aug. 14, 2008. Available at: http://www.wired.com/geekdad/2008/08/august-14-2003/. [Last accessed: August 03, 2012].

Mplus User's Guide, 2011. Available online at: http://www.statmodel.com/download/usersguide/Mplus%20Users%20Guide%20v6.pdf. [Last accessed: August 03, 2012].

Narasimhan, R., Talluri, S., 2009. Editorial: perspectives on risk management in supply chains. Journal of Operations Management 27, 114-118.

Nourse, A.E., 1982. Your Immune System. Franklin Watts: New York.

Nord, W.R., Jermier, J.M., 1994. Overcoming resistance to resistance: insights from a study of the shadows. Public Administration Quarterly 17(4), 396-409.

Normann, R. 1977. Management For Growth. New York: Wiley.

Norrman, A., Jansson, U., 2004. Ericsson's proactive supply chain risk management approach after a serious sub-supplier accident. International Journal of Physical Distribution & Logistics Management 34(5), 434-456.

Nourse, A.E., 1982. Your Immune System. Franklin Watts: New York.

Oliver, C., 1991. Strategic responses to institutional processes. Academy of Management Review 16(1), 145-179.

Osmond, D.G., 1993. The turn-over of B-cell populations. Immunology Today 14(1), 34-37.

Pagell, M., Yang, C., Krumwiede, D.K., Sheu, C., 2004. Does the competitive environment influence the efficacy of investments in environmental management? Journal of Supply Chain Management 40 (3), 30–39.

Parham, P., 2005. The immune system. 2nd edition, Garland Science Publishing, New York..

Peleg-Gillai, B. Bhat, G., Sept, L., 2006. Innovators in supply chain security: better security drives business value. The Manufacturing Innovation Series, available at: www.nam.org.

Perron, M., 2012. Fake avastin: FDA finds second counterfeit version of cancer drug. Available at: http://www.huffingtonpost.com/2012/04/04/fake-avastin_n_1402697.html. [last accessed: August 03, 2012].

Pfeffer, J., Salancik, G., 1978. The External Control of Organizations: A Resource Dependence Perspective. Harper and Row, New York.

Piderit, S.K., 2000. Rethinking resistance and recognizing ambivalence: a multidimensional view of attitudes toward an organizational change. Academy of Management Review 25(4), 783-794.

Playfair, J., Bancroft, G., 2004. Infection and immunity. 2nd edition, Oxford University Press, New York.

Podsakoff, P.M., Organ, D.W., 1986. Self-reports in organizational research: problems and prospects. Journal of Management 12, 531–544.

Podsakoff, P.M., MacKenzie, S.B., Lee, Y., Podsakoff, N.P., 2003. Common method biases in behavioral research: a critical review of the literature and recommended remedies. Journal of Applied Psychology 88, 879–903.

Post, R.S., Kingsbury, A.A., 1991. Security Administration: An Introduction to the Protection Services. Boston, MA: Butterworth-Heinemann.

Powell, W.W., 1991. Expanding the scope of institutional analysis. In Powell, W.W. & DiMaggio, P.J. (eds.). The New Institutionalism in Organizational Analysis, 183-203. University of Chicago Press, Chicago.

Prokop, D., 2004. Smart and safe borders: the logistics of inbound cargo security. International Journal of Logistics Management 15(2), 65-76.

Quinn, F.J., 2003. Security matters. Supply Chain Management Review 7(4), 38-45.

Raes, A.M.L., Heijltjes, M.G., Glunk, U., Roe, R.A., 2011. The interface of the top management team and middle managers: a process model. Academy of Management Review 36 (1), 102–126.

Raykov, T., 1997. Scale reliability, Cronbach's coefficient alpha, and violation of essential tau-equivalence with fixed congeneric components. Multivariate Behavioral Research 32(4), 329-353.

Reade, C., 2009. Human resource management implications of terrorist threats to firms in the supply chain. International Journal of Physical Distribution & Logistics Management 39(6), 469 – 485.

Rice, J.B. Jr, Caniato, F., 2003. Building a secure and resilient supply network. Supply Chain Management Review 7(5), 22-30.

Rice, J.B. Jr, Spayd, P.W., 2005. Investing in supply chain security: collateral benefits. Special Report Series, IBM Center for The Business of Government, available at: www.ibm.com.

Retail Info Systems News, 2008. Global theft costs retailers and consumers $104 billion annually. Available at: http://risnews.edgl.com/retail-trends/Global-Theft-Costs-Retailers-and-Consumers-$104-Billion-Annually38633. [Last assessed: August 03, 2012].

Ritchie, B., Brindley, C., 2004. Risk characteristics of the supply chain—a contingency framework. In: Brindley, C. (Ed.), Supply Chain Risk. Ashgate, Aldershot, pp. 28–42.

Ritchie, B., Brindley, C., 2007. Supply chain risk management and performance: a guiding framework for future development. International Journal of Operations and Production Management 27 (1), 303–322.

Russell, D.M., Saldanha, J.P., 2003. Five tenets of security-aware logistics and supply chain operation. Transportation Journal 42(4), 44-54.

Sarkis, J., Gonzalez-Torre, P., Adenso-Diaz, B., 2010. Stakeholder pressure and the adoption of environmental practices: the mediating effect of training. Journal of Operations Management 28 (2), 163–176.

Sarathy, R., 2006. Security and the global supply chain. Transportation Journal 45(4), 28–51.

Schindler, L.W., 1991. Understanding the Immune System. U.S. Department of Health and Human Services.

Schmitt, N., 1996. Uses and abuses of coefficient alpha. Psychological Assessment 8, 350–353.

Schwartz, L.M., 1980. Compendium of Immunology. Litton Educational Publishing, Inc. New York.

Scott, W.R., Meyer, J.W., 1983. Organizational environments: ritual and rationality. Beverly Hills, CA: Sage.

Scott, W.R., 1987. The adolescence of institutional theory. Administrative Science Quarterly 32 (4), 493–511.

Scott, W.R., 2004. Institutional theory: contributing to a theoretical research program. In Smith, K.G. & Hitt, M.A. (eds.), Great minds in management: The process of theory development. Oxford University Press, Oxford, UK.

Scott, W.R., 2001. Institutions and Organizations. Second edition. Thousand Oaks, CA: Sage

Segel, L.A., Cohen, I.R., (eds.), 2001. Design principles for the immune system and other distributed autonomous systems. Oxford University Press, New York.

Selznick, P., 1957. Leadership in Administration. Harper & Row, New York.

Senge, P.M., 1990. The Fifth Discipline: The Art and Practice of the Learning Organization. New York: Doubleday Currency.

Shavell, S., 1984. A model of the optimal use of liability and safety regulation. Rand Journal of Economics 15(2), 271–280.

Sheffi,Y., 2001. Supply chain management under the threat of international terrorism. The International Journal of Logistics Management 12(2), 1-11.

Sheffi, Y., 2002. Supply chains and terrorism. in Kausel, E. (Ed.), The Towers Lost and Beyond, A Collection of Essays on the WTC, Massachusetts Institute of Technology, available at: http://web.mit.edu/civenv/wtc/.

Sheffi, Y., 2005. The resilient enterprise: Overcoming vulnerability for competitive advantage. Cambridge, MA: The MIT Press.

Sheffi, Y., 2007, Building a resilient organization. The Bridge, 30-36.

Sheu, C., Lee, L., Niehoff, B., 2006. A voluntary logistics security program and international supply chain partnership. Supply Chain Management: An International Journal 11(4), 363-374.

Singhal, K., Singhal, J., 2012. Opportunities for developing the science of operations and supply chain management. Journal of Operations Management 30 (3), 245-252.

Smirnov, N.V., 1948. Tables for estimating the goodness of fit of empirical distributions. Annals of Mathematical Statistics 19(2), 279-281.

Speier, C. Whipple, J.M., Closs, D.J., Voss, M.D., 2011. Global supply chain design considerations: Mitigating product safety and security risks. Journal of Operations Management 29, 721-736.

Spitzer, S. 1996. Security and control in capitalist societies: the fetishism of security and the secrete thereof. In Lowman, J., Menzies, R.J., Palys, T.S., (eds.), Trancarceration: Essays in the Sociology of Social Control. 43-58.

Stephenson, W., 1953. The study of behavior: Q-technique and its methodology. University of Chicago Press: Chicago.

Strauss, A., Corbin, J., 1990. Basics of Qualitative Research: Grounded Theory Procedures and Techniques. Sage Publications, London.

Sutton, R.I., Galunic, D.C., 1996. Consequences of public scrutiny for leaders and their organizations. In Staw, B.M., Cummings, L.L., (eds.), Research in Organizational Behavior, 18, Greenwich, CT: JAI Press, 201–250.

Suchman, M.C., 1995. Managing legitimacy: strategic and institutional approaches. Academy of Management Review 20 (3), 571–610.

Swink, M., Song, M., 2007. Effects of marketing-manufacturing integration on new product development time and competitive advantage. Journal of Operations Management 25, 203-217.

Tang, C.S., 2006a. Perspectives in supply chain risk management. International Journal of Production Economics 103 (2), 451–488.

Tang, C.S., 2006b. Robust strategies for mitigating supply chain disruptions. International Journal of Logistics: Research and Applications 9(1), 33-45.

Tang, C.S., Tomlin, B., 2008. The Power of Flexibility for Mitigating Supply Chain Risks. International Journal of Production Economics 116(1), 12-27.

The New York Times, 1999. Disney recalls video over objectionable image. Available at: http://www.nytimes.com/1999/01/09/business/company-news-disney-recalls-video-over-objectionable-image.html. [last accessed: August 03, 2012].

Thibault, M., Brook, M.R., Button, K.J., 2006. The response of the US maritime industry to the new container security initiatives. Transportation Journal 45(1), 5-15.

Thomas, A.R., 2010. Supply Chain Security: International Practices and Innovations in Moving Goods Safely and Efficiently. Greenwood Publishing Group, Santa Barbara, CA.

Thomas, D.B., Baas, L.R., 1992. The issue of generelization in Q methodology: "Reliable schematics" revisited. Operant Subjectivity 16(1), 18-36.

Thong, J.Y.L., Yap, C-S., Raman, K.S., 1996. Top management support, external expertise and information systems implementation in small businesses. Information Systems Research 7(2), 248—267.

Thornton, P.H., 2004. Markets from culture: institutional logics and organizational decisions in higher education publishing. Stanford, CA: Stanford University Press.

Thorsen, T., 2011. PSN data leak cost could top $24 billion. Available at: http://www.gamespot.com/news/psn-data-leak-cost-could-top-24-billion-report-6310436. [last accessed, August 03, 2012].

Tomlin, B., 2006. On the value of mitigation and contingency strategies for managing supply chain disruption risks. Management Science 52 (5), 639–657.

Tonegawa, S., 1983. Somatic generation of antibody diversity. Nature 302, 575-581.

Truckinginfo, 2012. Mexico cargo theft increased 13% year-over-year, lower than normal. Available at: http://www.truckinginfo.com/channel/fleet-management/news/story/2012/02/mexico-cargo-theft-increased-13-year-over-year-lower-than-normal.aspx. [last accessed: August 03, 2012].

Trunick, P.A., 2005. What price security. Logistics Today 46(8), 1-11.

Tushman, M., Romanelli, E., 1985. Organizational evolution: A metamorphosis model of convergence and reorientation. In Cummings, L.L., Staw, B.M., (Eds.), Research in organizational behavior, vol. 7: 171-222. Greenwich, CT: JAI Press.

Unisys, 2005. Secure commerce roadmap: the industry's view for securing commerce. Unisys Corporation White Paper.

USA Today, 2012. FDA finds more fake Avastin cancer drug in U.S. Available at: http://content.usatoday.com/communities/ondeadline/post/2012/04/fda-finds-more-fake-avastin-cancer-drug-in-us/1#.UZk6v8oV_9U. [last accessed: August 03, 2012].

Villena, V.H., Gomez-Mejia, L.R., Revilla, E., 2009. The decision of the supply chain executive to support or impede supply chain integration: a multidisciplinary behavioral agency perspective. Decision Sciences 40 (4), 635–665.

Venkatraman, N., Grant, J.H., 1986. Construct measurement in organizational strategy research: a critique and proposal. Academy of Management Review 11(1), 71-87.

Voss, M.D., Closs, D.J., Calantone, R.J., Helferich, O.K., Speier, C., 2009a. The role of secrutiy in the food supplier selection decision. Journal of Business Logistics 30, 127–155.

Voss, M.D., Whipple, J.M., Closs, D.J., 2009b. The role of strategic security: Internal and external security measures with security performance implications. Transportation Journal 48(2), 5-23.

Vuong, Q.H., 1989. Likelihood ratio tests for model selection and non-nested hypotheses. Econometrica 57, 307-333.

Wacker, J.G., 2004. A theory of formal conceptual definitions: Developing theory-building measurement instruments. Journal of Operations Management 22, 629-650.

Wagner, S.M., Bode, C., 2006. An empirical investigation into supply chain vulnerability. Journal of Purchasing & Supply Management 12, 301-312.

Walley, N., Whitehead, B., 1994. It's not easy being green. Harvard Business Review 72 (3), 46–51.

Walsh, J.A., 2000. Employee theft. IFPO report, available at http://www.ifpo.org/articlebank/employee_theft.html.

Walt, S., 1991. The renaissance of security studies. International Studies Quarterly 35(2), 211-239.

Wang, G.C.S., 1996. How to handle multicollinearity in regression modeling. The Journal of Business Forecasting (spring), 23-27.

Weiss, D., Maher, M.W., 2009. Operational hedging against adverse circumstances. Journal of Operations Management 27(5), 362-373.

Wein, L.M., Liu, Y., 2005. Analyzing a bioterror attack on the food supply chain: The case of botulinum toxin in milk. Proceedings of the National Academy of Sciences 102(28), 9984-9989.

Wellcome Trust report, 2009. Opinion formers' conference on counterfeit medicines: perspectives and action. Available at: http://www.wellcome.ac.uk/stellent/groups/corporatesite/@policy_communications/documents/web_document/WTX057518.pdf. [Last accessed: August 03, 2012]

Wen, X., Cook, R.D., 2007. Optimal sufficient dimension reduction in regressions with categorical predictors. Journal of Statistical Inference and Planning 137, 1961-1979.

Westney, D.E., 1982. The emulation of western organizations in Meiji Japan: the case of the Paris prefecture of police and the Keishi-Cho. Journal of Japanese Studies 8, 307–342.

Westphal, J.D., Gulati, R., Shortell, S.M., 1997. Customization or conformity? An institutional and network perspective on the content and consequences of TQM adoption. Administrative Science Quarterly 42 (2), 366–394.

Whipple, J.M., Voss, M.D., Closs, D.J., 2009. Supply chain security practices in the food industry: do firms operating globally and domestically differ? International Journal of Physical Distribution & Logistics Management 39(7), 574-594.

Williams, D.H., 2004. The strategic implications of Wal-Mart's RFID mandate. Available at: http://www.directionsmag.com/articles/the-strategic-implications-of-wal-marts-rfid-mandate/123667, [Last accessed: April 24, 2012].

Williams, Z., Lueg, J.E., LeMay, S.A., 2008. Supply chain security: an overview and research agenda. International Journal of Logistics Management 19(2), 254-281.

Williams, Z., Lueg, J.E., Taylor, R.D., and Cook, R.L., 2009a. Why all the changes? An institutional theory approach to exploring the drivers of supply chain security. Internal Journal of Physical Distribution & Logistics Management 39(7), 595-618.

Williams, Z., Ponder, N., Autry, C.W., 2009b. Supply chain security culture: measure development and validation. International Journal of Logistics Management 20(2), 243-260.

Wooldridge, B., Schmid, T., Floyd, S., 2008. The middle manager perspective on strategy process: contributions, synthesis, and future research. Journal of Management 34, 1190–1221.

Wu, Z, Choi, T.Y., 2005. Supplier-supplier relationship in buyer-supplier triad: building theories from eight case studies. Journal of Operations Management 24, 27-52.

Yin, R.K., 1981. The case study crisis: some answers. Administrative Sciences Quarterly 26, 58-65.

Yin, R.K., 1994. Case Study Research: Design and Methods. Sage Publications, Thousand Oaks, CA.

Zbaracki, M.J., 1998. The rhetoric and reality of total quality management. Administrative Science Quarterly 43(3), 602–636.

Zedner, L., 2003. The concept of security: an agenda for comparative analysis. Legal Studies 23(1), 153–76.

Zucker, L. G., 1987. Institutional theories of organization. Annual Reviews of Sociology 13, 443-464.

Zukin, S. DiMaggio, P. J. 1990. Introduction. In Zukin, S. & DiMaggio, P. J. (eds.). Structures of Capital: The Social Organization of the Economy, 1-56. Cambridge University Press, Cambridge, UK.

APPENDIX A

A SEMI-STRUCTURED INTERVIEW PROTOCOL

Step 1: Ice break

Step 2: Briefly state the purpose of our research project—advance the understanding of SCS. Explain the benefits of participation—learn status of your firm and other firms across different industries; identify areas that your firm potentially needs to improve in order to manage supply chain security and risk.

Step 3: Examining the background (e.g. why supply chain security is important, etc.). Assure the anonymity regarding the information provided. Plus, let the interviewee know we can sign a confidentiality agreement.

Step 4: Ask the interviewee to provide basic information about his/her company (e.g., history, major products, etc.) and himself/herself (e.g., title, years with the firm, etc.).

Step 5: Semi-constructed questions:

1. Can you talk about what supply chain security is?
2. What is the domain of supply chain security management?
3. What strategies and practices [company name] has implemented to improve supply chain security?
4. Based on an extensive review of academic literature, industry reports, and industry standards, we categorize SCSM mechanisms into four clusters based on their intent: prevention, detection, reaction, and restoration. We would like to hear from you whether this categorization of security practices is a valid representation.
5. If you agree with the categorizations, what does [company name] (or even other manufacturing firms you know) do to prevent (detect, react to, and restore from) supply chain security events?
6. Can you talk about your company's understanding of SCSM? For example, what strategies or practices has your firm implemented and for what purposes?

7. Besides prevention, detection, reaction, and restoration, have your firm implemented any other mechanisms to enhance SCS?
8. Do you think a systematic classification of SCSM mechanisms will be helpful for (1) effective implementation of those mechanisms and (2) decision making?
9. Does [company name] see improved performance other than supply chain security due to the implementation of SCSM mechanisms?
10. Which SCSM mechanism(s) is most conducive to specific performance dimensions (e.g., visibility, operational costs, responsiveness, resilience, etc.)?
11. Can you talk a little bit about the supply chain security related governmental regulations in your industry?
12. Can you talk a little bit about the influence your firm has perceived from the government when it comes to supply chain security?
13. Do customers put specific supply chain security requirements in the contracts?
14. Can you talk about your customers' attitude towards supply chain security?
15. Do customers require your firm to improve supply chain security through formal/informal communications?
16. Have your competitors adopted supply chain security programs and initiatives? If yes, does this also drive your company to adopt similar programs?
17. Can you talk about how your competitors respond to supply chain security needs? Did their responses influence your company's decisions?
18. Can you talk about industry/professional norms when it comes to supply chain security?
19. Which institutional pressure is the most important one that drives your company to implement SCSM mechanisms?
20. Do the top managers of your company treat supply chain security seriously? Do they assume an active role in enhancing SCS? Does this have an impact on the adoption and implementation of SCSM mechanisms?
21. Do employees share the viewpoints that supply chain security is important? Do you think this has an impact on the implementation of SCSM mechanisms?

APPENDIX B

Q-SORTING RESULTS

1: Prevention; 2: Detection; 3:Reaction; 4:Restoration; 0: N/A						
	Q-Sorter 1	Q-Sorter 2	Q-Sorter 3	Q-Sorter 4	Q-Sorter 5	Q-Sorter 6
Q1	2	2	2	2	2	2
Q2	1	1	1	2	2	1
Q3	1	1	2	1	1	1
Q4	1	2	1	2	1	1
Q5	2	1	1	3	1	1
Q6	1	1	1	3	1	1
Q7	1	1	0	1	1	0
Q8	3	3	3	3	3	1
Q9	1	3	0	1	1	1
Q10	1	1	1	1	1	1
Q11	1	1	1	1	1	1
Q12	1	1	1	1	1	1
Q13	2	1	1	1	1	1
Q14	1	1	1	1	1	1
Q15	1	1	1	1	1	1
Q16	1	1	1	1	1	1
Q17	2	1	3	2	2	2
Q18	3	4	4	4	4	0
Q19	2	2	2	2	2	2
Q20	3	3	3	3	2	2
Q21	1	2	2	2	1	2
Q22	1	2	2	2	2	2
Q23	1	2	1	1	1	1
Q24	1	4	4	3	1	1
Q25	1	1	2	2	2	1
Q26	1	1	1	1	1	1
Q27	1	3	3	3	3	1
Q28	2	2	2	2	2	2
Q29	1	2	2	2	2	3
Q30	1	1	2	2	2	3
Q31	1	1	1	1	1	3
Q32	1	2	2	2	2	3
Q33	4	4	4	4	1	1
Q34	4	3	3	2	2	3
Q35	1	1	1	1	1	3
Q36	1	1	1	1	1	1

Q37	1	1	1	2	4	1
Q38	4	4	3	3	3	3
Q39	2	3	3	3	3	3
Q40	4	4	3	4	4	3
Q41	3	3	2	2	4	1
Q42	3	3	3	3	4	1
Q43	1	2	2	1	3	3
Q44	4	4	3	4	4	2
Q45	1	1	2	2	3	2
Q46	4	3	4	4	3	3
Q47	2	2	2	2	1	3
Q48	1	1	0	1	1	1
Q49	1	1	1	1	4	1
Q50	1	4	3	2	4	1
Q51	4	4	4	3	4	1
Q52	1	2	2	2	2	2
Q53	1	1	1	2	1	1
Q54	1	3	1	1	1	1
Q55	1	2	2	2	1	1
Q56	1	0	4	1	1	1
Q57	1	2	2	2	2	1
Q58	1	1	2	2	2	2
Q59	2	2	2	2	2	2
Q60	1	0	0	1	0	1
Q61	3	3	3	3	1	3
Q62	3	3	3	3	1	1
Q63	1	1	1	3	1	1
Q64	2	2	2	2	2	2
Q65	3	4	4	4	4	3
Q66	3	3	3	3	3	3
Q67	1	3	3	1	1	3
Q68	2	2	2	2	2	2
Q69	1	3	0	0	1	3
Q70	3	4	4	3	4	3
Q71	3	3	3	3	3	3
Q72	2	1	2	2	2	1
Q73	2	2	2	2	2	2
Q74	1	3	4	4	4	3
Q75	4	3	3	2	3	2
Q76	3	3	3	2	1	3
Q77	1	4	3	3	4	3
Q78	2	2	2	2	2	2

Q79	3	3	3	3	4	3
Q80	3	4	3	3	3	4
Q81	2	2	1	3	1	1
Q82	1	2	1	1	1	1
Q83	3	3	3	3	1	1
Q84	1	1	1	0	1	1
Q85	1	4	3	3	2	1
Q86	1	4	3	3	4	4
Q87	2	1	1	1	2	1
Q88	4	3	3	3	3	3
Q89	4	4	1	4	3	1
Q90	1	4	1	0	4	3
Q91	1	1	4	1	1	1
Q92	3	3	0	0	3	0
Q93	4	3	3	4	3	4
Q94	3	4	4	3	4	4
Q95	4	3	4	3	4	4
Q96	3	3	3	3	3	3
Q97	4	4	4	3	4	1
Q98	1	1	1	1	1	1
Q99	2	2	2	2	2	2
Q100	1	4	1	1	1	1

	Statement
Q1	Our strategy emphasizes an ability to detect security breaches early
Q2	We conduct unannounced security assessments of our logistics systems
Q3	We have visibility of supplier practices across all tiers
Q4	We regularly audit the security of our IT systems
Q5	We simulate supply chain disruptions to assure our readiness
Q6	Our supply chain risk management strategy can be characterized as proactive
Q7	The supply chain risk management strategy reflects the scale of the firm’s operations
Q8	We have designated a group of employees as first respondents in case of a crisis
Q9	We have a well defined supply chain security strategy
Q10	We secure containers at our facilities to assure they are not compromised
Q11	We are actively managing suppliers across all tiers of our supply network
Q12	All of our employees are trained for security and risk mgmt whenever they assume new roles
Q13	We have systems that provide good cyber protection
Q14	Supplier security is an important criterion when selecting our suppliers
Q15	When it comes to supply chain security, our strategy focuses on prevention
Q16	We offer incentives to our suppliers to enhance supply chain security
Q17	We regularly assess supplier security performance against security standards
Q18	We have complete and accurate documentation of our processes for an effective recovery effort
Q19	We use sophisticated technologies to detect if containers have been compromised
Q20	We have protocols for communication when a crisis arises
Q21	Performance indicators for supply chain security are tracked
Q22	We use RFID or other similar technology for tracking purposes throughout our supply chain

Q23	We have well defined supply chain security objectives/targets
Q24	We are building redundancies in our supply chain systems in case of a crisis
Q25	Our supply chain strategy ensures that threat and risk assessments are conducted regularly
Q26	We encourage suppliers to constantly enhance supply chain security
Q27	We delegate authority so that teams/individuals can take necessary action in case of a crisis
Q28	We have procedures to detect near misses in supply chain security
Q29	We actively evaluate the significance of various supply chain threats
Q30	We verify that all shipments are legitimate
Q31	We have positioned our facilities in separate locations to minimize risks of disruption
Q32	We examine all tiers in our supply chain to identify potential security vulnerabilities
Q33	Our supply chain strategy specifies the selective use of slack resources in anticipation of disruptions
Q34	We do conduct in-depth analysis of supply chain security breaches
Q35	We require comprehensive security capabilities from carriers
Q36	We mandate that suppliers adhere to established supply chain security standards
Q37	We segment and manage suppliers according to their risk profile
Q38	We use interchangeable or generic parts as a strategy to deal with potential disruptions in the supply chain
Q39	We have IT procedures for system lockout if violations/intrusions are detected
Q40	We have flexible capacity contracts with suppliers in order to improve our ability to react to a crisis
Q41	We have a mechanism to manage suppliers that are more vulnerable to disruptions
Q42	We have a well defined contingency plan to react to serious supply chain security breaches
Q43	We make use of anti tampering technologies on containers
Q44	We have a process to preserve knowledge in case of a crisis
Q45	We have metrics for evaluating supplier security
Q46	We have corrective procedures when security lapses are detected
Q47	We maintain an incident data base of supply chain security breaches
Q48	We have systems that ensure secure data exchange with partners
Q49	Our supply chain strategy spells out security priorities
Q50	Our strategy prioritizes efforts based on the magnitude of potential supply chain disruptions
Q51	Our supply chain strategy includes building knowledge redundancy in case of a crisis
Q52	We monitor our supplier network to identify suppliers at risk
Q53	We do background checks before we hire employees
Q54	We hold all suppliers accountable for supply chain security
Q55	We visit supplier facilities to assure the integrity of their supply chain security practices
Q56	We share our knowledge about supply chain security and risk management with suppliers
Q57	We do conduct periodic assessments of our supply chain security
Q58	We use technology to monitor facility access
Q59	We have procedures to detect supply chain security failures or near failures
Q60	Our supply chain risk management strategy has realistic objectives/targets
Q61	We pre-position resources to deal with crises effectively
Q62	We cross-train our employees as a mechanism to deal with potential supply chain disruptions
Q63	We educate suppliers about supply chain security practices
Q64	We monitor and synthesize information regarding security breaches
Q65	We do have a disaster recovery plan
Q66	There is effective communication across our supply chain when a crisis hits
Q67	Our strategy assigns clear responsibilities for security matters
Q68	We have the ability to track and trace our cargo in real time
Q69	The supply chain security strategy is consistent with the type of threats to the organization

Q70	We build flexibility in our manufacturing/assembly plants to reduce the impact of disruptions
Q71	We have a process that notifies supply chain partners across tiers if the supply chain is threatened
Q72	We evaluate whether any suppliers across tiers are financially vulnerable
Q73	We use active measures such as video and sensors to be able to detect security breaches
Q74	We have strategies for recovery action after supply chain disruptions
Q75	We spell out what to do in the event of a security breach or crisis
Q76	Our supply chain partners help us craft our response to a crisis
Q77	We established alternative carrier arrangements for use in case of supply chain disruptions
Q78	We actively assess whether our critical suppliers are at risk of business failure
Q79	We have a quick reaction force to deal with a crisis or a serious disruption in our supply chain
Q80	We have redundant communication systems which can be used if a crisis arises
Q81	We identify vulnerabilities so we can prepare ourselves in case of a crisis
Q82	We evaluate the risk related to potential terrorist attacks on our supply chain
Q83	We have a specific crisis management room that is appropriately equipped
Q84	We have strategies to simplify product design as part of our risk management strategy
Q85	We operate parallel or mirrored IT systems in order to deal with potential crises
Q86	We have contracted with suppliers that can provide additional capacity at times of emergency
Q87	We have access restrictions in our IT systems
Q88	We know what to do when we encounter supply chain security breaches or crises
Q89	We back-up our data to withstand potential disruptions
Q90	We have strategies to use more standard parts to reduce the risk of supply chain disruptions
Q91	We cooperate with suppliers to assure higher levels of supply chain security
Q92	Decisions to handle a crisis are planned to be made at the proper level of authority
Q93	We have backup processes that can assist us at times of crises
Q94	We developed alternative material sources in case of supply chain disruptions
Q95	We have a specific process to reinstate operations in case of a major crisis/disruption
Q96	There is a definite chain of command in case of an emergency
Q97	We maintain strategic inventory stocks to deal with potential crises
Q98	We only approve suppliers (irrespective of tier) that have a risk management program in place
Q99	We monitor the loading/unloading process of cargo to identify potential security breaches
Q100	In order to reduce supply chain risk we design products where suppliers can easily be replaced