Article:
Lu, G, Koufteros, X, Talluri, S et al. (2019) Deployment of Supply Chain Security Practices: Antecedents and Consequences. Decision Sciences, 50 (3). pp. 459-497. ISSN: 0011-7315

https://doi.org/10.1111/deci.12336

1. Introduction

"The United States and nations around the world depend upon the efficient and secure transit of goods through the global supply chain system…As a nation, we must address the challenges posed by these [supply chain security] threats and strengthen our national and international policies accordingly (National Strategy for Global Supply Chain Security, 2012)."

Breaches in supply chain security (SCS) have the potential to inflict hardship on firms and the welfare of people and society at large (Sheffi, 2005). For instance, cargo theft occurs on a daily basis in the U.S. and bears at least $35 billion in annual losses to companies alone (U.S. News, 2012). In 2010, a gang of thieves made off with around $60 million of pharmaceuticals (https://www.fbi.gov/news/stories/pharmaceutical-theft) from an Eli Lilly warehouse and cost the company about 75 million including goodwill costs (ABC News, 2010). Further investigation by FBI revealed that the same group was responsible for four other significant heists totaling over 30 million. Smuggling of people, weapons, and illegal substances via global supply chains has also been a constant and worrisome affair to firms and nations alike (Rice and Spayd, 2005). BBC (2014) reports that drug smugglers used a food supply chain to smuggle a large quantity of cocaine from Colombia to Germany; the shipment of cocaine made it to five branches of ALDI-Nord in and around Berlin, the German capital. Adulteration of products is also a current issue of concern. Adulteration includes biological, chemical or physical hazards and can be associated with economic or terroristic motives (Voss and Whipple, 2008). Eshkenazi (2013) notes that counterfeit food is becoming a big challenge in light of several scandals such as when horsemeat was mixed with beef in Europe via a complex network of slaughterhouses, processors, and other intermediaries. Especially worrisome is the potential use of supply chains by terrorists. In 2010, explosive material stuffed in printer cartridges was detected on cargo planes in the United Kingdom while in transit to the U.S. (The Telegraph, 2010). Consider a situation where a terrorist group embeds contaminated ingredients in a food/beverage or pharmaceutical supply chain. Wein and Liu's (2005) simulation, which is based on California dairy data, shows that, on average, contaminated milk can result in 568,000 casualties within 3–6 days. These examples demonstrate that offenders have the capacity to exploit global supply chains in order to conduct illicit activities.

Although the consequences of SCS breaches are immense and potentially devastating, little is known about what provokes firms to deploy SCS specific practices given that these practices also have the

potential to harvest adverse effects. On one hand, firms are investing in SCS to avert a crisis while satisfying governmental and customer policies/programs. On the other hand, SCS practices may have an adverse effect on costs, customer delivery lead time (Lee and Whang, 2005), and delivery reliability (Dobie, 2005) if more scrutiny is warranted. Thus, some firms may opt not to substantively deploy SCS practices. Additionally, since the probability of a catastrophic event is relatively scant (Fayol, 1989), justifying SCS investments may prove to be a futile exercise if relying merely on prototypical financial justifications (Lu and Koufteros, 2014). Unlike other strategic initiatives, which aim to directly improve financial performance (ROI, annual sales, etc.), the value of security and protection is only appreciated after failures do emerge. The effect on performance is often indirect and relatively covert. In addition, quantifying the financial impact of an averted incident is difficult and thus demonstrating a positive Return on Investment (ROI) becomes even more challenging. Williams et al. (2008) write specifically that some firms view security as an expense without a benefit. As a result, there is significant variance regarding the level of deployment of SCS practices across firms. A central challenge for advancing research, therefore, is to demonstrate why some firms deploy SCS practices and probe the efficacy of these practices to explain SCS performance.

To address this issue, we first examine the antecedents of the deployment of SCS practices and subsequently study the impact of these practices on SCS performance using data from 166 U.S. manufacturing firms. We are particularly interested in coercive institutional pressures (Berrone et al., 2013) serving as antecedents because these pressures are principally salient in the realm of SCS management (Lu and Koufteros, 2014; Ritchie and Melnyk, 2011) where organizations attempt to safeguard their legitimacy (Berrone et al., 2013) with the respective government(s) and customers. As noted earlier, SCS is unique as positive return on investment is not always assured (Williams et al., 2008) and therefore external pressure alone cannot fully explain why organizations deploy SCS practices. Two salient internal forces, top management involvement (Balogun et al., 2015; Heavey and Simsek, 2015) and organizational culture, play a pivotal role in organizational action (Hult et al., 2002) and thus firms may demonstrate variance in their responses to similar institutional stimuli (Oliver, 1991; 1997). Pragmatically, external forces relate their pressure via the agency of top management (Liang et al. 2007). Top management may probe performance against aspiration levels and invest in practices that can raise SCS performance above a reference point (Arrfelt et al., 2013). Furthermore, culture has the capacity to shape practices through a process Bertels et

al. (2016) coined as *cultural molding*. Organizational culture may ease or debilitate the work of managers to exercise leadership and oversight over security management (Williams et al., 2008). Thus, we postulate that the effects of top management involvement on the deployment of SCS practices would be strengthened when the culture is sensitized to SCS concerns.

This study contributes to the literature through its novel model, context, and positioning. First, our model is novel as we integrate both internal and external forces to study a context where organizational action is perhaps effectively mobilized only when *both* external and internal pressures are salient (Williams et al., 2008, 2012) and where financial justification is a thorny issue. Investments in prototypical environments usually rest on financial justifications (such as ROI) which are imposed or demanded by stockholders (Jensen and Murphy, 1990; Srivastava, 1983). The extant strategic management literature is primarily focusing on the role of top leaders when profit maximization or market performance are the dominant motives for strategic decision making. In essence, the literature has been preoccupied with decision making in an environment where there is very little strategic contradiction (Smith and Tushman, 2005); the assumption is that top managers make decisions with profit maximization/market performance as the sole underlying criterion. In the realm of SCS, there is a strategic contradiction because on the one hand top leaders are expected to attend to profit and market expectations while on the other hand they are expected to invest in SCS, which has definitive costs, uncertain ROI, and perhaps breeds adverse effects on operational performance. Based on our lengthy interactions with SCS practitioners, we deducted that the demands for SCS are instead imposed by the government and customers rather than typical constituents such as stockholders. In addition, returns on SCS investments cannot often be substantiated (Sheffi, 2005; Williams et al., 2008) despite that the consequences of SCS security breaches can be devastating, as we alluded earlier. Some of the practitioners we interviewed noted that investments in SCS can perhaps be paralleled to obtaining an insurance policy; the cost of insurance is real and certain but it is not definite that the insurance policy will be needed, at least on a regular basis. This is in line with the findings in both the network security literature and supply chain security literature—the value of security investments is not-so-visible (Siponen and Oinas-Kukkonen, 2007). Materially, we invoke both the top management involvement and institutional theories to explain their concomitant role on SCS practice deployment where firms have to make investments that cannot be fully justified financially, at least on the outset.

Second, the examination of both types of coercive institutional pressures (i.e., government and customer) and their role is novel. Firms frequently do not face formidable coercive pressures from both the government and customers simultaneously. Typically, only one of those two forces exerts immense pressure in a given situation. For instance, Toyota as a customer may apply serious pressure on its supplier of speakers to improve the sound quality but the government has no interest in pressuring the supplier in this respect. On the other hand, the government may apply formidable pressure on a supplier to lower emissions but Toyota may only deliver minimal pressure. The case of SCS is an exception however as both entities demand compliance concurrently. In addition, our study offers new insights regarding the potential relationship between the two external coercive pressures. While the institutional literature proposes three types of pressures (coercive, normative, and mimetic), it seldom examines different sources of pressure within each type nor does it explore the potential relationships between these sources (see a comprehensive review in Johnston, 2013). To the best of our knowledge, Johnston (2013) is the only study in the literature that discusses whether institutional forces within the same type may affect each other, although its context (sport management) is very different from ours. Our results demonstrate that (1) coercive pressures can emanate from diverse sources; the institutional theory literature generally treats coercive pressure as a unidimensional entity but coercive pressure may emanate from multiple sources such as customers and respective governments, and (2) coercive pressures from different sources may affect each other; we found that the effect of government pressure on top management involvement is partially transmitted via customer pressure.

Third, a significant gap in the SCS literature is that the practice-performance link is yet to be established empirically via a large sample of firms. There is a laundry list of practices prescribed/advocated by governments, international organizations (e.g., ISO), and leading firms (e.g., IBM) but yet we know very little regarding the efficacy of practices to explain SCS performance. Insights from few empirical inquiries (primarily qualitative interviews) produced mixed findings. For example, Sheu et al.'s interviews suggested that the value of the Customs-Trade Partnership Against Terrorism (C-TPAT) program was unclear. However, Ritchie and Melnyk (2011) demonstrated that firms could benefit if they were early C-TPAT adopters. There are also a number of conceptual papers in the literature advancing the notion that security related practices can engender better security performance. However, given the very topic being security,

firms are reluctant to disclose their choices of practices, their level, and performance implications because they do not want others (especially offenders) to know what actions/practices they undertake and they do not want to suffer any adverse effects on their insurance premiums, reputation, and public image. Despite the continuous call for more empirical validation (Williams et al., 2008; Cigolini et al., 2016), the effect of security related practices on security performance is still understudied (Ni et al., 2016; Williams et al., 2012). Similarly, Hu et al. (2007) state that one of the major hurdles in conducting empirical research on information systems security "is acquiring access to organizations and individuals who are willing to discuss information which is understandably sensitive. In general organizations and individuals are reluctant to talk about security issues for fear of being negatively impacted" (p. 160). Practically, our findings furnish some empirical evidence for firms to justify investments in their SCS. Furthermore, our robustness analyses probed different types of salient SCS practices (Lu et al., 2017) and discussed which type of practices may yield the strongest protection for supply chains.

Fourth, our model also embraces the moderating effects of organizational culture. Specifically, it explores the effect of top management involvement on SCS practices in light of different levels of organizational culture. Surprisingly, we found that culture reaches its maximum potential when at moderate levels of sensitivity. While the organizational theory literature generally suggests that organizational culture positively moderates (i.e., monotonically increase) the effect of purposive actions on designed goals, our post-hoc analysis shows that such effect is complicated. When cultural sensitivity to SCS is low, management and employees may not be overly convinced to adopt SCS practices, which they may see as a threat/burden to their current job routines. On the other hand, when management and employees are highly sensitized to SCS issues (i.e., cultural sensitivity to SCS is high), purposive actions (i.e., top management involvement) may not be all that necessary as employees will undertake necessary practices out of their own volition. In this sense, our study is unique as it identifies an important and largely ignored phenomenon that has great managerial implications. Firms can rest on our empirical findings for support in order to fine tune their respective cultural climates in the context of SCS.

2. Literature Review and Context

We review two related literature streams: supply chain security literature and network security literature. The latter is included because government and customers also place coercive pressure on organizations to improve information security (e.g., banking security, health information security, etc.).

Closs and McGarrell (2004) define SCS 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" (p. 8). Sarathy (2006) notes that supply chains are difficult to protect because vulnerabilities span goods, factories, supply chain partners and their facilities, freight carriers, people, and information. In addition, given that supply chains are becoming geographically longer, they are susceptible to more disruptions, which breed opportunities for illicit activities. Speier et al. (2011) note that much of the supply chain is unguarded and emphasize that the breadth of the supply chain infrastructure makes total protection difficult. Following the literature, SCS breaches can emanate from numerous sources. Supply chain security pertains to threats such as theft, terrorism, counterfeit products, product adulteration, smuggling of goods or people, illicit use and acquisition of data, and sabotage. The same definition and scope have been adopted in recent SCS studies (e.g., Lu et al., 2017; Peleg-Gillai et al., 2006; Williams et al., 2012).

Our literature review uncovered several important gaps which merit investigation. First, the empirical SCS literature (Williams et al., 2012) mainly focuses on the effects of SCS practices on collateral benefits (e.g., Rice and Spayd, 2005) but rarely attends to the antecedents of SCS practice deployment and its impact on SCS performance. The scarce empirical SCS literature attempts to explain SCS practice deployment via the lenses of the institutional theory. DiMaggio and Powell's (1983) seminal work on institutional theory stipulates three types of pressures that explicate firms' conformance to institutions: coercive, mimetic, and normative. Ritchie and Melnyk (2011) examined whether the institutional context (i.e., weak or strong coercive and normative forces) moderates the relationship between investments in SCS, speed through customs, and competitive advantage. Although this research study focused only on one type of SCS threat (i.e., terrorism) via the deployment of the C-TPAT program, it did demonstrate that institutional forces do play a significant role, albeit indirectly. We note that Ritchie and Melnyk (2011) considered the role of institutional forces only implicitly; they assumed that early adopters of C-TPAT face a weak institutional environment while late

adopters face a strong institutional environment. In addition, the authors did not account for the potential mediating impact of internal forces.

While there is some prior evidence that institutional forces may affect the deployment of specific practices, Dacin (1997) suggests that not all institutional pressures may impress firm action simultaneously and notes that the power (presence and effect) of institutional forces varies over time. Similarly, Berrone et al. (2013, p. 893) posit that the three institutional pressures "display varying degrees and their relevance is context-specific." Precisely in the domain of SCS, Williams et al. (2009a) examined all three types of institutional forces, resting on 17 interviews. They found that the coercive pressure emanating from the host government(s) in the form of regulation, force, or persuasion is more forceful compared to other types of pressure. Lu and Koufteros (2014) argue that government and customer pressures are very salient in the introduction and growth stages of security program lifecycles while mimetic and normative pressures assume more prominence later on. They note that the effects of mimetic and normative pressures are not expected to bear significant impact on organizational behavior early on because security practices have not had enough time to prove themselves and thus attain legitimacy. They argue specifically that coercive pressures likely dominate the early stages. Our intimate interactions with practitioners (see the method section for details) corroborate with the literature. Specifically, our long and active engagement with a professional association dedicated to SCS afforded us the opportunity to interact with high level SCS executives. Collectively, these executives underscored that mimetic and normative pressures were not at play in their decision to implement SCS practices. They noted that pressure emanates from government regulations and incentives as well as subsequent customer pressure to assure supply chain level conformity and compliance. We thus purposively focus on coercive pressures which may be more salient presently. In our context, a government needs to secure supply chains not only to promote global trade but also to protect its citizens, their lifestyle, and livelihood (Sheffi, 2001, 2005). Customers, on the other hand, demand SCS to avoid losses associated with potential disruptions and to uphold their own legitimacy and reputation (Rice and Spayd, 2005).

While Williams et al. (2009a) and Ritchie and Melnyk (2011) focus on institutional forces, our study offers substantially different insights because we posit that the effect of institutional forces on SCS practices deployment is not direct (it is instead mediated via the agency of top management) and these forces may be

related to each other (government pressure affects customer pressure). Furthermore, the impact of top management involvement is subject to the prevailing organizational culture. Thus, our model is more comprehensive as it recognizes that both external and internal mechanisms impact SCS practice deployment.

Second, organizational theory posits that organization action markedly rests on culture but the SCS literature focuses primarily on direct effects to the exclusion of important contingency factors. Smircich (1983) stresses that culture is an expression of values or social ideals and beliefs that are shared by organizational members. Rice and Spayed (2005, p. 43) refer to SCS culture as "socializing security." If the organizational members believe that SCS is high priority and the sentiment is widely shared, the work of top managers would be facilitated as the employees would have a buy-in and assume the responsibility to protect the supply chain. Employees would not only acquiesce to top management's action but would become strong advocates.

Third, we identified only a few empirical studies concerning SCS practices and SCS performance but they largely rest on qualitative interviews. While this approach is necessary at an early stage of empirical inquiry, it suffers from generalizability due to small sample size considerations and sample selection bias (McGrath, 1982). Among the studies we reviewed, we found none have used large scale data to examine the antecedents of SCS practices and their effects on SCS performance. This is somewhat surprising given that the conceptual literature has repeatedly argued that SCS practices enhance SCS performance. For example, Closs and McGarrell (2004) explicitly suggest that adopting SCS practices could reduce theft, smuggling and terrorism attacks. Sarathy (2006) concurs and argues that firms should embed SCS practices into their overall supply chain risk management portfolio of practices rather than seek solutions on the aftermath of SCS breaches. Furthermore, the scant empirical findings are largely inconsistent and pertain to specific programs. On one hand, Thibault et al. (2006) produced results that the Container Security Initiative (CSI) imposed by the U.S. government has positive effects. Similarly, Ritchie and Melnyk (2011), using data obtained via the Customs and Border Protection (CBP) agency of the U.S., demonstrate that benefits regarding custom clearance speed are contingent on whether the firm is an early or late C-TPAT adopter. On the other hand, Sheu et al.'s (2006) findings regarding the C-TPAT program are questioning its merits. While conceptual advances (Sarathy, 2006) and analytical models (Lee and Whang, 2005) suggest that the short-term costs associated with SCS practice deployment can be balanced out or out-weighted by long-term

gains from improved SCS performance, the impact of SCS practices on SCS performance has not been adequately established.

While the SCS literature has remained relatively stagnant, the network security literature might offer some insights. Stakeholders such as government and customers have pressured firms to enhance network security in order to protect sensitive information. The recent Equifax data breach had exposed personal information (including social security numbers and birth dates) of 143 million U.S. consumers (https://www.csoonline.com/article/3223229/security/equifax-says-website-vulnerability-exposed-143-million-us-consumers.html). The cost of the data breach in late 2013 at Target is reported to be over $200 million, as published by Reuters on May 23, 2017. These are yet another reminder of the importance of security.

Von Solms and Von Solms (2004) were some of the first to acknowledge the critical role of top management towards information security. The number one item in their list of top ten deadly sins in information security management is "not realizing information security is a corporate responsibility." Puhakainen and Siponen (2010) and Chang and Lin (2007) represent some of the few studies that examined the instrumental role of top management and culture in the context of information security.

The network security literature is generally concerned with four major security issues: access to information systems, secure communication, security management, and development of secure information systems (Siponen and Oinas-Kukkonen, 2007). Unlike supply chain security (the focus of our study), a strong emphasis is placed on technology (Kizza, 2017, Hu et al., 2007), and individual user compliance (Hu et al., 2007, Hu et al., 2012). The supply chain security literature, on the other hand, acknowledges the positive role of technology but it generally advocates a plethora of other approaches to security.

In an empirical study using case study methodology in one company, Hu et al. (2007) studied the role of external and internal pressures on information systems security. Relying on institutional theory, they examined the role of coercive, normative, and mimetic pressures. They found that coercive pressure demonstrated the most compelling force (via the example of Sarbanes-Oxley Act of 2002) but normative and mimetic pressures played a different role. Specifically in reference to mimetic pressure, the authors state "When we asked interviewees in general about whether their behavior was influenced by the actions of other companies, the general response was 'not really'" (p.166). Hu et al. (2007) found that the role of top

management was pivotal as government pressure required implementation of apposite controls over critical business processes and served "as a wake-up call and an important opportunity to initiate change management (p. 161)."

The most proximal study to our inquiry is an empirical examination of employee compliance in the context of IT security (Hu et al., 2012); though, Hu et al. (2012) did not consider external institutional forces. In addition, they proposed a mediational model: they posited a direct effect from top management involvement to organizational culture and then from organizational culture to employee beliefs (i.e., culture served as a mediator) and policy compliance intention. Our study differs from it by modeling organizational culture as a moderator, akin to Tsui et al. (2006) who proposed a contingency perspective. Both models are theory-driven, yet competing in their explanation. Given this prior work, albeit in a different domain, we examined a mediation model in the robustness analyses section.

3. Hypotheses Development

Figure 1 depicts our research model and we elaborate the rational for each hypothesis below.

--Insert Figure 1 about here--

3.1. Coercive Pressure and Top Management Involvement

The institutional theory suggests that firms operate within a framework of assumed rules and values about what represents appropriate social behaviors (DiMaggio and Powell, 1983; Meyer and Rowan, 1977). Compared to closed rational theories (e.g., quantitative oriented economic analysis), the institutional theory emphasizes social effects rather than just economic outcomes (Zukin and DiMaggio, 1990). Conformity to social requests contributes to firm success and survival because conforming firms are likely to gain social acceptance and thus reap societal resources (Baum and Oliver, 1991; Carroll and Hannan, 1989). As a result, many organizational decisions can be explained as ways to garner, influence, and maintain social justifications yet without careful efficiency consideration of these activities (DiMaggio and Powell, 1983; Zukin and DiMaggio, 1990). As elaborated earlier, we focus on coercive pressure. Coercive pressure results from both formal and informal influences exerted on firms by agencies upon which they are dependent. In our context, coercive pressures are mainly manifested by government pressure and customer pressure.

There are three reasons why government pressure can provoke top management involvement. First, the failure to adhere to legal prescriptions and regulations will likely result in loss of legitimacy (Lu and Koufteros, 2014). Atwater et al. (2010) report that about 110,000 motor carriers exited the industry in 2002. Many of these carriers ceased operations because they could not meet the stringent security regulations imposed by the U.S. government after the 9/11 terrorist attacks. Top management, being at the helm of an organization, is subject to a copious amount of pressure to abide by government regulations/programs. Second, prior studies have demonstrated that firms that acquiesce to government pressure would in turn apply pressure to non-conforming firms to assent as well by treating non-conforming firms as meaningless, irrational and unnecessary (Meyer and Rowan, 1991). As a result, top managers may exploit compliance with government requirements and expectations to avoid questioning by peers. Finally, compliance with government programs (such as the C-TPAT program) could potentially lead to operational benefits (Closs and McGarrell, 2004; Ritchie and Melnyk, 2011). For instance, a failure to pursue and attain C-TPAT certification, though participation is "voluntary," may culminate in longer lead times due to extra inspections and further scrutiny at ports (Ritchie and Melnyk, 2011) and can lead to market share losses as many firms only seek suppliers that are C-TPAT certified (Ritchie and Melnyk, 2011; Williams et al., 2009a). As one CEO states (Williams et al., 2009a, p. 603), "C-TPAT is the most voluntary, "non-voluntary" program in the history of the U.S. government."

Based on the extant literature, Oliver (1991, p. 150) cites a plethora of rewards that compliance or conformity may engender: These include elevated prestige, stability, legitimacy, social support, internal and external commitment, access to resources, attraction of personnel, acceptance in professions, and invulnerability to questioning. Given the direct and subtle pressure the government exerts on organizations, and given that government directives/policies are largely nonnegotiable (Berrone et al., 2013), top management involvement appears to be inevitable, although at varying levels. Top management develops a vision, forms strategic plans, and orchestrates resources (Sirmon et al., 2011) to pursue organizational action which is needed to assure compliance. We thus propose the following hypothesis:

H_1: Government pressure is positively associated with top management involvement.

In a similar vein, customer pressure is also consequential to top management involvement. First, customers provide business opportunities. Complying with customer demands garners legitimacy and renders a supplier more attractive (Delmas and Montiel, 2009). As an early participant of C-TPAT, IBM asked/required its suppliers in 2002 to participate in this effort through a memorandum signed by its top procurement officer:

> *"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. We are asking IBM's suppliers to assess, and enhance if necessary, their security processes in the following areas recommended by U.S. Customs: Physical Security, Access Control, Procedural Security, Personnel Security, Education and Awareness Training. Guidelines for establishing, improving, or amending supply chain security procedures are available on the U.S. Customs Web site, under Security Recommendation. 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."*(www-3.ibm.com/procurement/proweb.nsf/ContentDocsBytitle/United+States~29+Jul+02:+Supply+Chain+Security?OpenDocument&Parent=Supplier+letters)

A failure by top management to succumb to customer pressure and deploy necessary SCS practices, will be rather consequential to the relationship.

Second, full compliance with customer pressure increases the opportunity of establishing new business with existing or new customers (Delmas and Montiel, 2009). Prior research relying on case study methodology demonstrates that non-compliance and loss of customers are correlated (Williams et al., 2009a). Recent studies suggest that buying firms are likely to turn to suppliers who have an established record of compliance (Williams et al., 2009a). Finally, a supplier "deep in the network" can significantly affect its customer's operations (Kim et al., 2015). Lack of security on the supply side could significantly jeopardize the buying firm's market share and reputation (Rice and Spayd, 2005; Williams et al., 2009a) due to the potential disruptions that can emerge. These disruptions have the capacity to generate adverse effects on shareholder wealth and operational performance (Hendricks and Singhal, 2003; 2005). Therefore, when customers demonstrate a strong desire to enhance SCS performance, top management will be subjected to pressure to assume leadership and orchestrate resources to heighten SCS. Hence, we argue:

H_2: Customer pressure is positively associated with top management involvement.

Although government pressure and customer pressure are generally treated as separate forces in the SCS literature (Lun et al., 2008; Williams et al., 2009), a recent study in a different context suggests that they may be related to each other (Johnston, 2013). Johnston (2013) notes that institutional pressures are not exclusively distinct, particularly in an environment where stakeholders affect each other. This argument is also credible within the context of SCS where scholars have highlighted the need of interaction between government authorities and business firms (Lee and Whang, 2005). We posit that government pressure affects customer pressure. Customers are buying firms who are also subject to government regulations and demands. In many cases, they can fully comply with government regulations/demands only when their suppliers are also in compliance (http://www.cbp.gov/border-security/ports-entry/cargo-security/c-tpat-customs-trade-artnership-against-terrorism). For instance, to obtain the highest level of C-TPAT certification, an accredited auditor is typically hired and is authorized to audit a focal firm's *supplier's* warehouse without advance notice. If the supplier is found to be non-compliant, or suspicious activities surface, the auditor has the authority to prevent the facility from releasing shipments and subsequently suspend the focal firm's C-TPAT certification. Thus, buying firms have the motivation to exert pressure on their suppliers to deploy SCS practices to ensure their own compliance. A buying firm's security efforts can be easily nullified if its suppliers are non-compliant. Thus, customer pressure is related to government pressure.

H_3: Government pressure is positively associated with customer pressure.

3.2. The Effects of Top Management Involvement on SCS practices

Top management involvement is characterized as "the force that pulls different functional groups together (Swink, 2000; p. 211)." It is vital as SCS management faces several obstacles and top management is "indisputably important for strategic change" (Balogun et al. 2015, p. 960). First, employees may not understand SCS practices and their significance in averting and/or combating potential breaches. Many practices require that work is performed differently to assure the integrity of the supply chain and may impose additional job demands. This may lead employees to generate workarounds in order to simplify their work while however putting the supply chain at risk. Second, unless employees are motivated to adapt to new practices, they may informally rely on "old" ways and sometimes may even try to discredit the efficacy of "new" practices. Third, adopting and exploiting a SCS system demands additional financial and human

resources. Top management is needed to devise clear objectives, have an active oversight, provide funding for education, technology, and continuous improvement, and encourage frank discussion (Hu et al., 2012, Speier et al., 2011) about SCS and its implications. Williams et al. (2008) suggest that some firms decline to invest in SCS because of cost considerations. In other words, the significant costs to implement SCS initiatives coupled with the low probability of a major breach may motivate some firms to abstain from substantive investments in SCS and may instead be investing in *window-dressing*. Finally, top management's boundary spanning role (Heavy and Simsek, 2015) can play a pivotal role. Top managers import external knowledge and integrate internal knowledge and can benchmark benefits against those derived by other firms in order to make proper adjustments to organizational action (Hu et al., 2012).

We argue that the effects of coercive pressures are first felt by top management who then translates those demands into organizational action. Top management is responsible to alter procedures, rules, and routines. This explains why firms in the same industry, subject to the same coercive pressures, exhibit diversity in SCS practice deployment. The deployment of SCS practices rests on top leaders who may invest to bolster SCS without necessarily have the bona fide evidence on ROI as noted earlier. Taken together, we argue:

H_4: Top management involvement is positively associated with the deployment of SCS practices.

3.3. Mediational Effects

While we did not specify direct effects between coercive pressures and the deployment of SCS practices (which we test in our robustness analysis), it is likely that the effects are enduring but they might be indirect; the effects of coercive pressures on SCS practices are perhaps mediated via top management involvement through legitimization and commitment (Hu et al., 2012). Also, since top management plays a significant boundary spanning role, it serves as a focal interface with the environment and thus is likely to be the subject of institutional pressure. According to Liang et al. (2007), external pressure can only impact organizations when it affects the behavior of human agents such as top managers. Thus, we posit a mediational hypothesis.

$H_{5a\text{-}b}$: The effect of government pressure (a) and customer pressure (b) on the deployment of SCS practices is mediated by top management involvement.

3.4. The Moderating Role of Organizational Culture

Organizational culture has been referred to "the personality of the firm" (McAfee et al., 2002). It facilitates employees to understand how the firm functions and furnishes behavioral norms (McAfee et al., 2002). Organizational culture stimulates employees to support and value behaviors it promotes (Barney, 1986; Gray and Massimino, 2014). It also has the capacity to "perpetuate institutionalized structures and behaviors (Oliver, 1997, p. 700)." As a result, top management action can be enhanced when congruency exists between organizational culture and operations strategies (Alvesson and Willmott, 2002).

A culture that is supportive of SCS can facilitate the deployment of SCS practices for at least two reasons. First, culture can energize employees. Firms with a culture that views SCS with respect will subsequently rally their employees around a set of meaningful values and goals toward SCS (Autry and Bobbitt, 2008). These values boost employee commitment, identification, and effort (Hu et al., 2012) because employees are inherently engaging with issues that matter to them and believe they should take some responsibility for SCS (Williams et al., 2009b). Harris (1994) examined how organizational culture influences the mental schema employees deploy for sense making and articulating apposite responses. Employees become more proactive and vigilant regarding SCS and go above and beyond the "requisite" activities; they actively detect and resolve threats as they perform daily tasks. Resolving SCS issues becomes a routine.

Second, supporting cultures facilitate the effects of top management involvement on SCS practices deployment by shaping and coordinating employees' behaviors. Norms guide employee behavior and decision making (McAfee et al., 2002). Unlike formal control systems, cultural norms imply social control and influence how social members perceive and interact with one another (Bettenhausen and Murnighan, 1991). Employees are likely to autonomously coordinate actions to assure excellence in SCS performance via SCS practices when the culture is supportive of SCS (Williams et al., 2009b). When the culture is well entrenched, the need for security as reflected by top management involvement can engender "congruency" within the firm and facilitate the deployment of SCS practices. On the other hand, managers "…can be trumped by employee actions that uphold some aspect of an existing culture (Bertels et al. 2016, p. 576)." Thus, we propose:

> *H_6: The effect of top management involvement on the deployment of SCS practices will be moderated by organizational culture such that the effects are heightened when organizational culture is supportive of SCS.*

3.5. The Impact of SCS practices

The extant literature has advocated (but rarely empirically examined) the positive link between the deployment of SCS practices and SCS performance (Giunipero and Eltantawy, 2004; Jüttner et al. 2003; Knemeyer et al., 2009; Sheffi, 2005). Based on the literature, SCS practices involve a variety of approaches to detect, diagnose and protect against SCS breaches, and continuously improve the system to combat SCS breaches. For example, practices tasked with detecting potential SCS breaches or practices that protect the supply chain (e.g., securing containers) from emerging security breaches will ease the pain because many of the security breaches can be simply averted (Knemeyer et al., 2009). Using an analogy from the quality management literature, companies find it more effective to prevent defects from emerging rather than coping with the defects that materialize (Lee and Whang, 2005). Diagnostic practices, on the other hand, reduce the probability that potential SCS threats are under-identified or ignored (Peleg-Gillai et al., 2006). Firms that deploy these practices usually scrutinize operational processes along the supply chain to uncover flaws and attempt to establish an effective and clear communication channel with suppliers, leading to better supply chain visibility (Knemeyer et al., 2009). Contingency planning fashions resilience which results in sustained business continuity (Sheffi, 2005; Bakshi and Kleindorfer, 2009). Consequently, the supply chain can effectively respond to potential breaches. The adoption of these practices puts firms in a better position to cope with SCS challenges and thus attain better SCS performance. In line with the literature, we propose:

H_7: The deployment of SCS practices is positively associated with SCS performance.

4. Methods and Results

4.1. Research Design and Sample Characteristics

Our targeted population included manufacturing units (a firm or a strategic business unit) located in the U.S. Appreciating the sensitivity of the topic and its potential adverse effect on response rates (Williams et al., 2012), we did not limit our target pool of firms to any specific manufacturing related SIC code. Given the pervasive impact of SCS breaches, we conjecture that firms across industries would face SCS challenges to some degree, and would realize the pressure to adopt SCS practices.

We undertook a multi-staged preliminary inquiry prior to collecting data from a large sample of firms. To inform and enrich our understanding of SCS issues, the authors first actively attended by invitation

numerous meetings of the Transported Asset Protection Association (TAPA) over the last six years. This is a closed group of SCS executives from a variety of industries that are tasked to protect their respective supply chains. Regular participation draws also from law enforcement at local, state, and federal levels. We had the opportunity to benefit from discussions regarding government regulations, new threats and strategies and how they affect SCS, and gathered that there is very little knowledge regarding the efficacy of SCS practices to explain SCS performance. We also had short interviews with TAPA members to assure that relevant variables are adequately embodied in our inquiry. During the interviews, we not only discussed practices advocated in promising SCS programs but also sought to understand practices that were employed by practitioners but ignored by the literature. We also learned, for instance, that often the same practice may be labeled differently by firms or security programs. This allowed us to curb content redundancy in our survey. Furthermore, we solicited their insights regarding coercive institutional pressures. It became abundantly clear in our discussions that the government and customers serve as the two most pivotal forces exerting pressure for the adoption of SCS practices. The executives cited numerous government programs (such as the C-TPAT, Importer Security Filing - ISF, FAST, etc.) that emerged over the years and their specific impact on organizational practices. In addition, the executives noted that top management involvement varied across firms; leadership at firms that sustained recent serious incidences was in general more engaged and championed organizational action.

In the next stage, we interviewed 11 supply chain executives who are subject matter experts and four academics who work in the area of SCS. Our objective was to solicit their feedback on the clarity, and content and face validity of the survey questions, which we gathered based on our literature review and our interactions with practicing executives. The authors then officially presented their findings to the TAPA audience on multiple meetings and obtained valuable feedback. At the last stage of instrument development, we also undertook a pilot study to obtain tentative assessments of validity and reliability by relying on responses from 39 supply chain executives who are members of the Council of Supply Chain Management Professionals (CSCMP).

We targeted high and middle-level supply chain executives, since these are the individuals who have sound knowledge of external pressures and internal forces leading to the deployment of SCS practices. They would also be knowledgeable about specific SCS practices and SCS performance. Interactions with TAPA

members helped us understand who are the best-fitting respondents and helped us craft "filter" questions for our survey. Based on the conversation with these high-ranking executives, we also learned more details about the attributes of SCS managers working in respective industries, which lead to the confidence that our sample is representative. For example, the average number of years of experience (reported in the next paragraph) is very close to what we expected based on our inquiries with TAPA members. We targeted respondents who (1) hold at least a managerial (or equivalent) designation, (2) work in the manufacturing sector, (3) and work in areas which are directly related to supply chain management and security. A panel of 1,543 potential respondents was identified via Qualtrics.com panels by relying on our selection criteria which included firm size in excess of 100 employees and several other screening questions, in addition to the three criteria above. In our description to practitioners, we did not want to limit threats only to a given specific source. Instead, we indicated that supply chain security pertains to threats such as theft, terrorism, counterfeit products, product adulteration, smuggling of goods or people, and sabotage. Qualtrics.com sent two spaced reminders (five days apart) on behalf of the authors. The IP addresses recorded by Qualtrics.com suggest that the responses are unique and are geographically dispersed. Using a random sample of 25 firms, we were able to match each IP address with specific locations of businesses in order to assure that we obtained legitimate responses. On average, each respondent completed the survey in 15.53 minutes with a median of 13.10 minutes. This was a very reasonable duration given the length of the survey. The research team paid Qualtrics.com $50 for each useable response.

The data collection process yielded 166 usable responses with a response rate of 10.8% (166/1543). The response rate compares favorably with other survey studies in the overly sensitive domain of SCS (e.g., Williams et al., 2009b, 2012). Table 1 reports the characteristics of the sample. The typical designation of the respondents includes President or VP Manufacturing/SCM/Operations/Logistics, and Director and Manager of similar functional areas. About 45% of the respondents held a position at the director level or above. In fact, 22% of respondents were Vice Presidents or held a “C” level designation. On average, each respondent had 13.40 years of experience at the firm (median=11) suggesting a wealth of knowledge regarding specific organizational issues. Our research design included only respondents that had indicated direct knowledge of the practices/activities (individuals that indicated lack of such knowledge were automatically excluded from responding to the survey via screening questions) their respective organization undertakes to protect itself

against security threats. Thus, we have confidence that our participants have subject matter knowledge. A majority of participating firms (95%) have annual sales of over $10 million while 34% have annual sales of over $1 billion. In terms of commerce type, a total of 54% of firms operate in the business-to-business environment, 26% operate in the business-to-consumer environment, and the rest serve both business partners and consumers.

--Insert Table 1 about Here--

4.2. Variables and Survey Instrument

We developed the survey indicators based on extensive interviews with subject matter experts and a thorough review of the strategic management, organizational theory, and supply chain management literatures. All survey indicators were scored on a seven point Likert type scale, where 1 represented "Not at all" and 7 represented "A great deal." All variables were operationalized via multi-item scales.

Coercive isomorphism results from both formal and informal pressures exerted on organizations by agencies upon which they are dependent. The typical sources of coercive pressure in our context could be traced to the *government* who sets, for example, trade regulations or major *customers* who provide business opportunities. In many cases, organizational change is a direct response to a government mandate: for example, the 100% inspection of U.S.-bound containers policy forces importers and international carriers to implement internal controls and processes such that they can work within the legal framework prescribed by U.S. laws. Customers can exert a strong impact on suppliers and their leadership because simply customers are the main business or resource providers (Tolbert et al., 2011). The indicators of government pressure and customer pressure were largely adapted from prior studies; i.e., Liang et al. (2007), Heugens and Lander (2009), and Williams et al. (2008). These indicators reflect formal and informal pressure imposed on an organization to conform by virtue of requirements or incentives.

Top management involvement reflects the degree of engagement of top leaders and goes above and beyond mere sensitivities regarding SCS. This involvement is rather salient in the realm of SCS as the firm and its supply chain are subject to a significant number of threats; some imminent and some distant, some minor and some potentially catastrophic. Top management is responsible to set clear objectives for securing the supply chain and allocate requisite levels of resources to assure proper execution. Top

management assumes an active leadership and oversight role in order to signal to the rest of the supply chain constituents that security does matter (Hu et al., 2012). Top management involvement (Mintzberg, 1979; Lambert et al., 1998) reflects the active engagement of top management but also reflects its sensitivity toward risk management (Rodríguez et al., 2008). We specified five indicators which measure the extent to which top managers appropriately allocate resources and orchestrate managerial effort for SCS (Hu et al., 2012; Knemeyer et al., 2009).

Schein (1986) characterizes culture as a coping mechanism that employees use to deal with problems of external adaptation and internal integration and describes it as ‘‘the basic assumptions and beliefs that are shared by members of an organization, that operate unconsciously and define in a ‘taken for granted’ fashion, an organization’s view of itself and its environment’’ (p. 6). Rice and Spayed (2005, p. 43) refer to SCS culture specifically as “socializing security.” Alternatively, we can view SCS as a cultural phenomenon (Cameron and Sine, 1999). In essence, culture in our study reflects the shared beliefs of organizational members regarding SCS. It reflects their sensitivities to security breaches and whether SCS is a sentiment widely shared within the organization (Hu et al. 2012). If individuals believe that even minor security breaches can cause havoc in their respective supply chain, they would be more willing to personally invest in SCS and thus be the catalyst in translating top management’s involvement into action. Security-oriented organizational culture was operationalized via shared beliefs regarding SCS (Williams et al., 2009b; Speier et al., 2011). This conceptualization is consistent with Leidner and Kayworth (2006).

Since SCS breaches represent a special form of supply chain risk, it is conducive to borrow concepts from the extant literature on risk management and SCS specific programs such as ISO 28000. ISO 28000 clearly asserts that the organization needs to constantly assess the security environment in which it operates (i.e., detection and diagnostic practices are needed) along with the respective risk in order to decipher whether adjustments and countermeasures are needed (i.e., contingency planning) in terms of structure or personnel and its training (i.e., continuous improvement). To prevent breaches, the organization has to deploy protective practices (i.e., protection) along the supply chain which may be accompanied with opting for suppliers (i.e., supplier selection) based on their SCS performance. We specified six first-order constructs that reflect the most salient practices of ISO 28000 and represent the core aspects of risk management as advocated by Starr and Van Wassenhove (2014); SCS practices include detection, diagnostic, protection,

supplier selection, contingency planning and continuous improvement (Closs and McGarrell, 2004; Peleg-Gillai et al., 2006; Rice and Spayd, 2005; Sheffi, 2001, 2005). The deployment of these six SCS practices received tacit endorsement from TAPA members who we interviewed and who also had the opportunity to attend our presentations and our Q & A sessions. They thought that our treatment of practices was fairly comprehensive, covering the domain of SCS practices. Each of these is described in (online) Appendix A. We believe that SCS practices share their intent to protect the supply chain and usually organizations deploy them as a bundle as part of a SCS program such as ISO 28000. Thus, their levels should be highly correlated and subsequently the construct of SCS practice was specified using a second-order latent variable orientation. The items of SCS performance included seven indicators in order to embody the different nuances discussed in prior studies (Closs and McGarrell, 2004; Peleg-Gillai et al., 2006; Rice and Spayd, 2005; Lu et al., 2017).

The survey instrument was first administered, as noted earlier, to 39 supply chain management executives as a means to pilot-test it. The responses indicated that one meaningful factor can be extracted when each variable was examined via within block EFA; in addition, all Cronbach's alpha reliability estimates were above 0.67. These findings were rather reassuring but some changes were made to assure validity (face, content, convergent, and discriminant) and reliability. For instance, we added an additional indicator for supplier selection and changed the wording on other indicators.

4.3. Research Methodology and Results

Before we tested the substantive hypotheses, we assessed measurement issues and common method bias. First, we examined via Mplus 7.2 whether a 2nd order latent factor specification for SCS practices can be supported. In addition, due to the number of latent variables at the first level of abstraction (i.e., 11) and the number of indicators (i.e., 51), we specified two measurement models; the first included the two coercive pressures, top management involvement, and culture while the second included the SCS practices and SCS performance. We subsequently assessed model fit, convergent validity, and reliability within each measurement model. To assure discriminant validity across the two measurement models, we tested for all pairs of variables across both measurement models using a χ^2 difference test. Details about the measurement models appear in (online) Appendix D.

Using a series of nested models, the χ^2 associated with the second-order model for SCS practices is statistically invariant (χ^2_{diff}=13.54, 9 df, p>0.14) from the χ^2 generated when a first-order correlated variable model is specified (online Appendix C). Given its conceptual simplicity and considering that firms think of a "system" of interrelated practices, the second-order model can be supported.

Furthermore, the first measurement model produced acceptable model fit statistics (Hult and Ketchen, 2001; Shook et al., 2004): $\chi^2(98)=139.41$, $\chi^2/df=1.42$, CFI=0.95, TLI=0.93, SRMR=0.06 and RMSEA=0.07. The second measurement model produced acceptable fit indices as well: $\chi^2(521)=759.12$, $\chi^2/df=1.46$, CFI=0.91, TLI=0.90, SRMR=0.06, and RMSEA=0.07. These fit indices suggest congruence between the models we specified and the data. In both measurement models, all item-factor loadings were substantive in magnitude (only two items had coefficients below 0.60) and statistically significant at the 0.001 level, suggesting convergent validity. Each pair-wise χ^2 difference test was significant at the level of 0.01, providing evidence of discriminant validity. Composite reliabilities (CR) (Hult and Ketchen, 2001; Shook et al., 2004) ranged from 0.76 to 0.93 and average variance extracted (AVE) ranged from 0.51 to 0.83. Collectively, there is sufficient evidence demonstrating construct validity and construct reliability. Table 2 reports the means, standard deviations, and correlations of the non-categorical variables. Appendix E (Online) displays the indicators of each construct and their respective standardized factor loadings, CRs, and AVEs.

--Insert Table 2 about here--

In order to examine the indirect effects of coercive institutional pressures on SCS practices deployment and performance, we performed mediation analysis using a bootstrapping approach (Preacher and Hayes, 2008); we attained bias corrected confidence intervals by specifying 5,000 iterations.

A number of control variables were included to ensure that we can isolate the effects of our explanatory variables. We included several control variables describing firm characteristics: size, profit margin, and market share. Firm size was operationalized by annual sales. Large firms and those with high profit margin (those with broader resource availability, Ritchie and Melnyk (2011), or those with sufficient slack, Berrone et al. (2013)) may have more resources to deploy towards SCS practices. Firms with large market share are more visible and thus perhaps more sensitive to their reputation, leading them to invest more heavily to protect their supply chains. On the other hand, small firms may be more agile in responding to environmental stimuli (Dean et al., 1998). We also controlled for industry effects (Short et al., 2007) as

some industries may be more sensitive to SCS breaches; for instance, the food, beverage, and pharmaceutics industries may be more vigilant because their products are consumed by humans and thus breaches are laden with more risk. Overall, the data included responses from 11 sectors: food and kindred products (10.2%), paper and allied products (4.2%), chemical and allied products (7.2%), primary metal products (5.4%), fabricated metal products (6.6%), commercial machinery (5.4%), electronic products (6.6%), transportation equipment (9.0%), analyzing and controlling instruments (6.6%), general equipment (21.7%), and others (16.5%).

We centered explanatory variables at the individual indicator level to mitigate potential multicollinearity. Given that multiple independent variables are posited as explanatory variables of SCS practices, we used SPSS to obtain variance inflation (VIF) scores and condition indices aside from our main SEM analysis. We also assessed for the presence of outliers, influential observations, and normality. The data analysis did not produce any worrisome information that would demand further action.

Before we assessed the hypotheses we also addressed common-method bias (CMB) (online Appendix F). Using a variety of methodologies (such as a marker variable technique), there was no evidence to suggest that CMB merits concern.

4.4. Hypotheses Results

Given the satisfactory measurements, we proceeded with the examination of the structural model; the fit indices χ^2=616.07 (465), χ^2/df = 1.32, CFI=.931, TLI=.919, RMSEA=.063, 90% C.I. RMSEA (.048, .075) suggest a well-fitting model. It is noted that deployment of SCS practices was modeled here as a second-order factor via total aggregation at the first level of abstraction as practices are often implemented as a program or system. Firm size was the only control variable that demonstrates a significant effect (+) on the deployment of SCS practices. Other control variables exhibited negligible effects. We identified no counter-intuitive findings related to control variables. Table 3 reports the results.

--Insert Table 3 about here--

H_1, H_2 and H_3 hypothesized direct relations amongst the coercive pressures and with top management involvement. The results provide support for H_1 which proposed that government pressure is positively associated with top management involvement (γ=0.598, p=0.000). The analysis also supports H_2

which hypothesized that customer pressure is positively associated with top management involvement (β=0.370, p=0.013). Our findings are consistent with the institutional logic which posits that external coercive pressures have a sizable direct impact on top management involvement (Liang et al., 2007). H_3 proposed that customer pressure is positively related to government pressure. The results provide support for this hypothesis (γ =0.757, p=0.000) and suggest that the relationship amongst coercive pressures might exist at least within the realm of SCS.

H_4 proposed that top management involvement is positively related to the deployment of SCS practices. The results support this assertion (β=0.409, p=0.013). Collectively, the results suggest that the effects of government pressure and customer pressure on the deployment of SCS practices can perhaps be transited through top management involvement (Liang et al., 2007). Using a bootstrap process (Table 4), we found all indirect paths (total and specific) from government pressure (H_{5a}) and customer pressure (H_{5b}) to the deployment of SCS practices and then to SCS performance to be statistically significant; all the confidence intervals were positive and did not include zero.

--Insert Table 4 about here--

H_6 argued that the relationship between top management involvement and the deployment of SCS practices would be more salient in the presence of an organizational culture that is sensitive to SCS. The results (Table 3) illustrate that such culture positively interacted with top management involvement (β=0.225, p=0.001). In order to examine the interaction effect more closely, we examined the conditional effect of top management involvement on the deployment of SCS practices at different values of the moderator using the Johnson-Neyman technique via the Process Model in SPSS (Table 5). These results are rather interesting and reveal where exactly on the spectrum of organizational culture the effect of top management involvement on SCS practices is statistically significant. Table 5 suggests that when the organizational culture is not sensitive at all to SCS concerns, the effect of top management involvement on the deployment of SCS practices is not statistically significant. On the other hand, when the organizational members become more concerned about SCS issues, top management involvement becomes consequential for SCS practices. However, it is apparent that although at the very high levels of cultural sensitivity the effects of top management involvement on the deployment of SCS practices are still positive and statistically significant, they are diminishing vis-à-vis the effects of top management involvement at moderate levels of cultural

sensitivity. In essence, the effects of top management involvement on the deployment of SCS practices appear to be the strongest when the organization is moderately sensitized to SCS issues. This was confirmed by running three supplementary regression models via SPSS relating top management involvement and the deployment of SCS practices, one for each level of organizational culture (low, moderate, and high – based on quartiles) while controlling for the same variables as our prior models. The standardized coefficients for top management involvement are .528 (p=0.004), .598 (p=0.000), and .465 (p=0.002) at the three cultural levels respectively. The interaction was also probed via ANCOVA (Figure 2). Figure 2 illustrates that the marginal mean of SCS practice deployment is in general higher when the organizational culture is more sensitive to SCS. It is evident that the marginal effects are more pronounced at moderate levels of cultural sensitivity.

--Insert Figure 2 and Table 5 about here--

H_7 predicted that the deployment of SCS practices positively impact SCS performance. Consistent with H_7, the deployment of SCS practices exhibits a significant positive effect on SCS performance (β=0.939, p=0.000). Thus, H_7 is supported.

4.5. Post-hoc Analysis

The literature generally suggests that organizational culture will positively moderate the effect of purposive action on its designed goals when the action is in line with what the culture promotes. However, it carries an implicit linear assumption that the moderation effect will increase monotonically with the moderator. Nonetheless, our test of H_6 suggests that the moderation effect can be complicated under some circumstances. The moderation effect may be non-linear. As we observed, organizational culture reaches its strongest marginal effect at moderate levels and not the highest levels. To further explore our finding, we tested a model using a higher-order model. The model included *top management involvement (top), security-oriented culture (culture), square of culture (culture^2), top x culture, top x culture^2*, and the same set of control variables used in our main analysis. The results reveal that top x culture^2 is marginally significant at 0.1 level (p-value = 0.10) when the first order interaction is controlled for. This provides some empirical evidence of a phenomenon that is largely ignored in the literature but has great managerial implications: organizational culture may serve as a non-linear moderator. Low levels of culture do not motivate additional response to

purposeful actions (top management involvement in our case) while very high levels of culture may render purposeful actions redundant. We discuss these findings in the discussion section.

4.6. Robustness Analyses

We performed four additional types of analysis. First, while we specified indirect effects between coercive pressures and the deployment of SCS practices (full mediation via top management involvement) in our main analysis, it is possible that the effects can also be direct (partial mediation). We thus specified direct paths between the two coercive mechanisms and deployment of SCS practices and examined the efficacy of a partial mediation model vis-à-vis a full mediation model via a χ^2 test. The difference in χ^2 (616.07-610.58 < 5.99, 2 df) is not statistically significant and this suggests that the full mediation model is preferred over the partial mediation model since the latter does not fit the data any better; the full mediation model is more parsimonious without suffering any statistically significant loss in model fit.

Second, Hu et al. (2012) studied employee compliance in the context of IT security, though they did not consider external institutional forces such as government and customer pressure. They proposed a direct effect from top management involvement to organizational culture and then from organizational culture to employee beliefs and policy compliance intention (i.e., culture served as a mediator). Our inquiry, on the other hand, models organizational culture as a moderator and thus studies the interaction between top management involvement and organizational culture. Both models have their respective theoretical but competing rationales. If we just tested however only a mediation model following this literature, the interesting yet counter-intuitive finding—the moderating effect of organizational culture appears to be non-linear—would be concealed. To consider the competing rationale, we also run a mediational model. The results are in line with Hu et al. (2012) such that top management involvement strongly affects organizational culture (β=0.949, p=0.000) and culture strongly affects the deployment of SCS practices (β=0.865, p=0.000).

Third, we correlated each of the six SCS practices with SCS performance in order to ascertain whether SCS practices impact performance uniformly. As we noted earlier, firms typically implement these practices in a systemic fashion as part of an overarching program such as ISO 28000. We found statistically significant correlations with SCS performance for all practices and the magnitudes suggest substantive significance as well: Detection (p-value=0.729**), Diagnostic (0.742**), Protective (0.667**), Supplier Selection

(0.698**), Contingency Planning (0.733**), and Continuous Improvement (0.734**). While the individual means and standard deviations of these practices somewhat differ (Detection – mean= 4.54, SD=1.35, Diagnostic – mean=4.55, SD=1.60, Protective – mean=5.19, SD=1.31, Supplier Selection – mean=4.68, SD=1.63, Contingency Planning – mean=5.05, SD=1.39, and Continuous Improvement – mean=4.72, SD=1.60), their covariation with SCS performance appears to be fairly uniform.

Fourth, while we did follow the advice of the SCS literature (e.g., Lu et al., 2017) and adopted a second-order construct of SCS practices in an attempt to adequately cover as comprehensively as possible the set of practices firms implement to combat supply chain security threats, we acknowledge that this may conceal the differences among these first-order practices. We thus reran our analysis by using six first-order constructs of SCS practices in lieu of the second-order construct. The results demonstrate that culture only moderates the top management involvement's effect on detection (β=0.116, p=0.044) and supplier selection practices (β=0.098, p=0.091). Collectively, the robustness findings suggest that while all six sets of practices are conducive to better security performance, a security-oriented organizational culture only alters the relationship between top management involvement and SCS practices only for two of them.

5. Discussion

From an external environment perspective, we have demonstrated the cogent impact of governmental and customer pressures on top management involvement, and from an internal standpoint, we showed that top management involvement positively influences the deployment of SCS practices. Harmonizing these two perspectives, our findings suggest that the impact of *external* coercive pressures is mainly transmitted via *internal* mechanisms such as top management involvement. Given the limited empirical research related to the deployment of SCS practices, our findings provide a better understanding of factors that drive firms to deploy such practices. These results argue for a combination of a push and pull approach to deploy SCS practices, i.e., from an external perspective, firms are influenced by the push lever through coercive pressures and from an internal standpoint, top management involvement acts as a pull lever. While one can argue that push comes before pull, it is evident that both levers are critical for deployment of SCS practices and firms may not achieve desired outcomes without either of them. In addition, we have demonstrated that the relationship between top management involvement and deployment of SCS practices

varies by levels of organizational culture. This finding sheds light on internal characteristics that play a vital role in deploying SCS practices, which lead to improved SCS performance.

5.1. Theoretical Contributions

The critical role of top managers has been recognized in the literature (Eisenhardt et al., 1997; Floyd and Lane 2000). However, prior studies largely focus on the personal characteristics of top managers (e.g., Hambrick and Mason, 1984) and the direct impact of top management on organizational strategies. Our theoretical model suggests that top managers not only affect the organizational behaviors directly, but more importantly serve as the medium through which external coercive pressure impacts organizational action. The findings are consistent with Teo et al. (2003) and Liang et al. (2007) who advanced similar arguments, albeit in a different domain.

External coercive pressures often exist within social legal systems. The existence of a legal system can affect many aspects of firm behavior. The classic economic school of thought argues that firms would only adopt initiatives if required by coercive forces (Walley and Whitehead, 1994). However, our *robustness analysis* suggests that the partial mediation model does not explain additional variance to warrant its support. Yet the impact of external forces on internal top management involvement appears to be rather strong, suggesting that the effects of government and customer pressures are mainly transited through top management involvement (i.e., the full mediation model).

The significant and positive relationship between government pressure and customer pressure also deserves further discussion. The extant institutional theory literature largely treats the two types of coercion at the same level of position within a nomological network. However, theoretically, government pressure exists at a higher level because government pressure within the same industry frequently applies to both the focal firm and its customers. Government pressure thus also shapes customer's demands on the focal firm. The strong relation between the two types of pressure indicates that customer pressure on a focal firm reflects partly the government pressure the customer is subjected to. As a result, the effect of customer pressure on top management involvement should be interpreted with caution. If customer pressure serves as an intermediary link between government pressure and top management involvement, then the effect involves more than just the will of the customers. It may reflect the joined effect of both government pressure and

customer pressure. The discovery adds to our understanding regarding how regulations shape organizational behaviors. Furthermore, the finding adds to the institutional theory literature which in general does not acknowledge relationships between the same type of institutional forces.

The findings also illustrate that the effect of top management involvement on SCS practices deployment is subject to organizational culture (Williams et al., 2009b) such that the effects are more positively pronounced when the culture is sensitive to security. We probed the interaction using a variety of techniques and the results are rather interesting. On the aggregate, there is significant evidence to indicate that the effect of top management involvement on the deployment of SCS practices varies with the cultural sensitivity regarding SCS issues. However, when the interaction was examined more closely via the Johnson-Neyman technique it became apparent that at very low levels of cultural sensitivity to SCS, increasing top management involvement will not bear significant returns in the form of higher deployment of SCS practices. Table 5 suggests that as the level of cultural sensitivity regarding SCS increases, the impact of top management involvement becomes more salient but it appears to be most efficacious at moderate levels of such cultural sensitivity. The effects of top management involvement were still positive and statistically significant at very high levels of cultural sensitivity but there is a marked deterioration of the potency of top management involvement. This was also confirmed by running post-hoc supplementary regression models. When the pro-security cultural sensitivity is very low, high top management involvement may be interpreted as micromanagement or unwarranted interference and thus resistance may ensue. Employees may also interpret the push for SCS practices as an attempt by top management to monitor them; SCS may be perceived as a mere guise to institute more surveillance on organizational actors. Gilbert et al. (2012) note that employee stress, decreased job satisfaction, and feelings of social isolation have been linked to employee monitoring. Thus, when employees are not sensitized to SCS and its implications, they may not be overly committed to adopt SCS practices which they may see as a threat. On the other hand, when employees are highly sensitized to SCS issues, top management involvement may not be all that necessary as employees will undertake necessary practices out of their own volition; thus the effects of top management involvement may wane down. As expected, SCS practices are related to SCS performance. The effect size is indicative of a fairly strong impact suggesting that those companies that embrace SCS practices will reap significant benefits.

Our robustness analyses suggest that organizational culture does not uniformly moderate the effect of top management involvement on the six security practices. Instead, its moderation effect is only salient when detection practices and supplier selection practices are considered. We posit that this maybe because some practices are more effective than other practices in combating security threats (Lu et al., 2017). Firms have accumulated experiences and promoted these practices. We note that Lu et al. (2017) found that detection practices have the more potent effects on security performance. Given that detection practices represent one of the most effective means to mitigate supply chain risk (Lu et al., 2017), the findings collectively suggest that detection practices may be the most efficacious action undertaken to secure supply chains and reduce supply chain risks.

5.2. Managerial Implications

The findings carry with them several managerial implications. First, the results identify top management involvement as a pivotal factor in improving SCS performance. The firm's existing structures create inertia which promotes the status quo, even if performance downturns are present (Tushman and Romanelli, 1985). Such inertia is rather robust and often impedes the deployment of new and potentially beneficial organizational actions (Normann, 1977). Without effective involvement from top managers, the implementation of new practices is unlikely to be successful (Liang et al., 2007). Our empirical findings reinforce this point. Pragmatically, firms must understand that top management involvement is the key to substantiate the organizational security efforts. Likewise, top leadership should understand that breaches in security can rattle their own positions and status within the organization. For instance, Starnes (2016) and Southern (2017) note that CEOs do lose their jobs over data breaches. Thus, awareness of the threats and active engagement by top management are vital elements to SCS.

While most studies on top management involvement took a top-down approach by assuming top leaders have ultimate authority within organizations (e.g., Villena et al., 2018), our study provides some empirical evidence that top leaders are subject to external pressures in the context of SCS. Given the pivotal role of top management involvement, our findings suggest that a bottom-up approach can also be crucial in protecting supply chains. That is, supply chain managers should affect top leaders' perception of external pressures, threats, and incite (top leaders') actions. Supply chain managers may proactively advocate the

importance of SCS and draw attention from top leaders through the means of *issue selling and initiative taking* (Bouquet and Birkinshaw, 2008). Hu et al. (2007) also acknowledged the role of a bottom-up approach in the context of information system security. We found top management involvement strongly affects organizational culture in our robustness analyses. Coupled with the finding that the moderating effect of organizational culture is most salient at moderate levels in our main analyses, we conjecture that there may be an optimal level of top management involvement that interacts with the cultural climate to maximize supply chain security outcomes. While a bit out of the scope of this study, we posit that when the organizational culture is not characterized by its sensitivity to SCS, middle managers should engage the top leadership to increase their active involvement by rousing concerns, solutions, and opportunities together. However, when the organizational culture is already highly sensitized about SCS, top management heavy involvement may be somewhat redundant; in fact, such heavy involvement may induce employee sense of over-monitoring.

Further, supply chain managers may also promote an organizational culture which eventually facilitates the deployment of SCS practices. Russell and Saldanha (2003) estimated the cost to protect the supply chains in the U.S. at over $151 billion annually. Without cultivating a mindset that security matters, firms are likely to suffer high security costs which could have been avoided. Our post-hoc analysis suggests that a high level of security-oriented culture may help reduce security related costs, as less managerial effort is needed to promote the implementation of security practices. Relatedly, firms need to be selective because the moderation effect of culture may not apply to all security practices.

Finally, our results show that customer pressure is also affected by government pressure. Demands from customers are partially explained by government pressure. Such insights provide a venue for firms to better comprehend how customer demands pertaining to SCS emerge. Firms in the same industry are subject to similar governmental regulations. Consequently, a firm can be well prepared for customer demands by proactively implementing practices that the government stipulates. This proactive strategy may also bring collateral benefits as Ritchie and Melnyk (2011) demonstrated in their study on early adopters of the C-TPAT program.

5.3. Limitations

Our study is subject to several limitations, which in turn offer opportunities for future research. First, a better understanding of how coercive pressures fasten with internal forces to affect security practices is necessary to advance the SCS literature. Although this study emphasizes the role of top management involvement, future studies might examine other important factors such as a firm's ownership. Public firms and their operations are more visible and thus may be subject to more scrutiny by more constituents. Thus, there may be a difference on how they handle SCS practices. Second, because this research is cross-sectional, it cannot evaluate how the practices supported by the top managers get actually implemented, readjusted, or annulled over time. A longitudinal study may be more apposite to address SCS over time.

Third, we did not specify relationships between organizational culture and top management involvement. Given the cross-sectional research design of our study and considering the long duration it takes for culture to evolve when implicit or explicit attempts are made to alter it, we did not articulate any hypotheses that relate culture and top management involvement (although we tested a mediation model in robustness analysis). However, future studies may acknowledge this relationship. As Bass and Avolio (1993, p. 113) note "Cultural norms arise and change because of what leaders focus their attention on, how they react to crises, the behaviors they role model, and whom they attract to their organization." Finally, due to the topic sensitivity, we were able to collect data of only a few control variables. We encourage future studies to include more contextual variables that may affect supply chain security performance.

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. [Last accessed: April 03, 2012].

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

Alvesson, M., & H. Willmott. 2002. Identity regulation as organizational control: Producing the appropriate individual. Journal of Management Studies, 39, 619-644.

Arrfelt M, Wiseman RM, & Hult GTM. 2013. Looking backward instead of forward: Aspiration driven influences on the efficiency of the capital allocation process. Academy of Management Journal, 56(4), 1081-1103.

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

Bakshi, N., & P. Kleindorfer. 2009. Co-opetition and investment for supply chain resilience. Production and Operations Management, 18, 583–603.

Balogun, J., Bartunek, J,M., & Do, B., 2015. Senior managers' sensemaking and responses to strategic change. Organization Science, 26 (4), 960-979.

Barney, J. 1986. Strategic factor markets: expectations, luck, and business strategy. Manage Science, 32(10), 1231-1241.

Bass, B.M., & Avolio BJ. 1993. Transformational leadership: A response to critiques. In Leadership theory and research: Perspectives and directions Chemers MM and Ayman R (eds.). San Diego, CA: Academic Press. 49–80.

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

BBC. 2014. Cocaine worth £40m found in Portsmouth banana shipment. http://www.bbc.co.uk/news/uk-england-hampshire-30300763 [4 January 2015].

Berrone, P., & Gomez-Mejia, L.R., 2009. Environmental performance and executive compensation: An integrated agency-institutional perspective. Academy of Management Journal, 52(1), 103-126.

Berrone P, Fosfuri, A., Gelabert, L., & Gomez-Mejia, L.R., 2013. Necessity as the mother of 'green' inventions: Institutional pressures and environmental innovations. Strategic Management Journal, 34, 891-909.

Bertels, S, Howard-Grenville J, & Pek S. 2016. Cultural molding, shielding and shoring at Oilco: The role of culture in the integration of routines. *Organization Science* 27 (3): 573-593.

Bettenhausen, K.L., & Murnighan. J.K. 1991. The development of an intragroup norm and the effects of interpersonal and structural challenges. Administrative Science Quarterly, 36(1), 20-35.

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

Cameron, K., & Sine, W., 1999. A framework for organizational quality culture. Quality Management Journal, 6 (4), 7-25.

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

Chang, S. E.,& Lin, C.-S. 2007. Exploring organizational culture for information security management. Industrial Management & Data Systems, 107(3), 438–458.

Cigolini, R., Pero, M, Sianesi, A., 2016. Reinforcing supply chain security through organizational and cultural tools within the intermodal rail and road industry, The International Journal of Logistics Management, 27(3), 816-836.

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. [2011-10-18].

Dacin, M.T. 1997. Isomorphism in context: The power and prescription of institutional norms. Academy of Management Journal, 40, 46-81.

Dean, T.J., Brown, R.L., & Bamford, C.E., 1998. Differences in large and small firm responses to environmental context: Strategic implications from a comparative analysis of business formations. Strategic Management Journal, 19 (8), 709–728.

Delmas, M.A., & Ivan. M. 2009. Greening the supply chain: When is customer pressure effective? Journal of Economics & Management Strategy, 18(1), 171-201.

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.

Dobie, K. 2005. The core shipper concept: a proactive strategy for motor freight carriers. Transportation Journal, 44(2), 37-53.

Eisenhardt, K.M., Kahwajy, J.L. & Bourgeois III., L.J. 1997. Conflict and strategic choice: How top management teams disagree. California Management Review, 39(2), 42-62.

Eshkenazi A. 2013. Security in the food supply chain. http://www.apics.org/industry-content-research/publications/apics-magazine-home/apics-magazine---landing-page---members-new/2013/02/15/security-in-the-food-supply-chain. [4 January 2015].

Fayol, H. 1989. Administration Industrielle et generale (Storrs,Trans.). Sir Isaac Pitman & Sons, London.

Floyd, S., & Lane. P. 2000. Strategizing throughout the organization: Managing role conflict in strategic renewal. Academy of Management Review, 25(1), 154-177.

Gilbert, J.A., Ruffino, N.C. Ivancevich, J.M. & Konopaske, R. 2012. Toxic versus cooperative behaviors at work: the role of organizational culture and leadership in creating community-centered organizations. International Journal of Leadership Studies, 7, 29-47.

Giunipero, L., & El Tantawy. R. 2004. Securing the upstream supply chain: A risk management approach. International Journal of Physical Distribution and Logistics Management, 34(9), 698-713.

Gray, J.V., & Massimino, B. 2014. The effect of language differences and national culture on operational process compliance. Production and Operations Management, 23(6), 1042-1056.

Harris, M., 1994. Cultural materialism is alive and well and won't go away until something better comes along. In Assessing Cultural Anthropology, Borofsky R (eds). New York: McGraw Hill.

Heavey, C., & Simsek, Z., 2015. Transactive memory systems and firm performance: An upper echelons perspective. Organization Science, 26 (4), 941-959.

Hendricks, K.B., & Singhal. V.R. 2003. The effect of supply chain glitches on shareholder wealth. Journal of Operations Management, 21(5), 501-522.

Hendricks, K.B., & Singhal. V.R. 2005. Association between supply chain glitches on shareholder wealth. Management Science, 51(5), 695-711.

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.

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

Hu, Q., Dinev, T., Hart, P., & Cooke, D., 2012. Managing employee compliance with information security policies: The critical role of top management and organizational culture. Decision Sciences, 43, 615–660.

Hult, G.T.M., & Ketchen, D.J., 2001, Does market orientation matter? A test of the relationship between positional advantage and performance. Strategic Management Journal, 22(9), 899–906.

Hult, G.T.M., Ketchen, D.J., & Nichols, E.L., 2002. An examination of cultural competitiveness and order fulfillment cycle time within supply chains. Academy of Management Journal, 45(3), 577–586.

Hambrick, D.C., P.A. Mason. 1984. Upper echelons: The organization as a reflection of its top managers. Academy of Management Review, 9, 193-206.

ISO, 2007. ISO 28000: Specification for security management systems for the supply chain. September 15, 1st edition.

Jensen M C, Murphy K J. Performance pay and top-management incentives. Journal of Political Economy, 1990, 98(2), 225-264.

Johnston, M. 2013. Mimetic, coercive and normative influences and decision of national sport organizations to bid for world championship events. Dissertation, Auckland University of Technology, New Zealand.
Jüttner, U., Peck, H. & Christopher. M. 2003. Supply chain risk management: outlining an agenda for future research. International Journal of Logistics: Research & Applications, (6), 197-210.
Kim, Y., Chen, Y. & Linderman. K. 2015. Supply network disruption and resilience: A network structural perspective. Journal of Operations Management, 33-34, 43-59.
Kizza, J.M., 2017. Guide to Computer Network Security. 4th edition. Springer.
Kline, R.B., 1998. Principles and practice of structural equation modeling. The Guilford Press: New York, NY.
Knemeyer, A.M., Zinn, W. & Eroglu. C. 2009. Proactive planning for catastrophic events in supply chains. Journal of Operations Management, 27, 141-153.
Lambert, D.M., Stock, J.R. & Ellram, L.M.. 1998. Fundamentals of Logistics Management. Irwin/McGraw-Hill, Chicago, IL.
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.
Leidner, D.E., & Kayworth, T. 2006. Review: A review of culture in information systems research: Toward a theory of information technology culture conflict. MIS Quarterly, 30(2), 357-399.
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.
Lu, G., & Koufteros. X. 2014. Adopting supply chain security practices for the transport logistics: institutional effects and performance drivers. International Journal of Shipping and Transport Logistics, 6(6), 611-631.
Lu, G., Koufteros, X., Lucianetti, L. 2017. Supply chain security: A classification of practices and an empirical study of differential effects and complementarity. IEEE Transactions on Engineering Management, 64(2), 234-248.
Lun, V.Y.H., Wong, C.W.Y. Lai, K-H. & Cheng. T.C.E. 2008 Institutional perspective on the adoption of technology for the security enhancement of container transport. Transport Reviews, 28(1), 21-33.
McAfee, R.B., Glassman, M. & Honeycutt. Jr. E.D., 2002. The effects of culture and human resource management policies on supply chain management. Journal of Business Logistics, 23(1), 1-17.
McGrath, J. 1982. Dilemmatics: The study of research choices and dilemmas. In McGrath, J.E., Martin, J., & Kulka, R.A. (Eds.), Judgment Calls in Research, 69-102. Sage, Newbury Park, CA.
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, IL.
Meyer, J.W., Rowan, B., 1977. Institutionalized organizations: formal structure as myth and ceremony. American Journal of Sociology 83 (2), 340–363.
Mintzberg, H., 1979. The Structuring of Organizations. Prentice-Hall, Englewood Cliffs, NJ.
National Strategy for Global Supply Chain Security, 2012. Available at: https://www.whitehouse.gov/sites/default/files/national_strategy_for_global_supply_chain_security.pdf. [2013-4-16].
Ni, J.Z., Melnyk, S.A., Ritchie, W.J., Flynn, B.F., 2016. Why be first if it doesn't pay? The case of early adopters of C-TPAT supply chain security certification", International Journal of Operations & Production Management, 36(10), 1161-1181.
Normann, R. 1977. Management For Growth. Wiley, New York.
Oliver, C., 1991. Strategic responses to institutional processes. Academy of Management Review, 16(1), 145–179.
Oliver, C., 1997. Sustainable competitive advantage: Combining institutional and resource-based views. Strategic Management Journal, 18, 697–713.
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. [2011-11-16].

Preacher, K.J., & Hayes A.F. 2008. Asymptotic and resampling strategies for assessing and comparing indirect effects in multiple mediator models. Behavior Research Methods, 40, 879-891.
Puhakainen, P., & Siponen, M. 2010. Improving employees' compliance through information systems security training: An action research study. MIS Quarterly, 34(4), 757–778.
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. [2011-11-16].
Ritchie, W.J., & Melnyk, S.A., 2012. The impact of emerging institutional norms on adoption timing decisions: evidence from C-TPAT—A government antiterrorism initiative. Strategic Management Journal, 33, 860–870.
Rodríguez, N.G., Pérez, M.J.S. & Gutiérrez, J.A.T. 2008. Can a good organizational climate compensate for a lack of top management commitment to new product development? Journal of Business Research, 61, 118-131.
Russell, D.M., & Saldanha. J.P. 2003. Five tenets of security-aware logistics and supply chain operation. Transportation Journal, 42(4), 44-54.
Sarathy, R., 2006. Security and the global supply chain. Transportation Journal, 45(4), 28–51.
Schein, E.H., 1986. Organizational culture and leadership. Jossey-Bass, San Francisco, CA.
Sheffi, Y., 2001. Supply chain management under the threat of international terrorism. The International Journal of Logistics Management, 12(2), 1-11.
Sheffi, Y. 2005. The resilient enterprise: Overcoming vulnerability for competitive advantage. The MIT Press, Cambridge, MA.
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.
Shook, C.L., Ketchen, D.J., Hult, G.T.M., & Kacmar, K.M., 2004. An assessment of the use of structural equation modeling in strategic management research. Strategic Management Journal, 25(4), 397–404.
Short, J.C., Ketchen, D.J., Palmer, T.B., & Hult, G.T.M., 2007. Firm, strategic group, and industry influences on performance. Strategic Management Journal, 28(2), 147–167.
Siponen, M.K., Oinas-Kukkonen, H., 2007. A review of information security issues and respective research contributions. The DATA BASE for Advances in Information Systems, 38(1), 60-80.
Sirmon, D.G., Hitt, M.A., Ireland, R.D., & Gilbert, B.A., 2011. Resource orchestration to create competitive advantage breadth, depth, and life cycle effects. Journal of Management, 37, 1390–1412.
Smircich, L. 1983. Concepts of culture and organizational analysis. Administrative Science Quarterly, 28, 339-358.
Smith, W.K., Tushman, M.L., 2005. Managing strategic contradictions: A top management model for managing innovation streams. Organization Science, 16(5), 522-536.
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.
Srivastava, S. 1983, The Executive Mind, Jossey-Bass, San Francisco.
Starr, M.K., & Van Wassenhove, L.N. 2014. Introduction to the special issue on humanitarian operations and crisis management. Production and Operations Management, 23(6), 925-937.
Starnes, R., 2016. Data breaches often result in CEO firing, Available at: https://www.csoonline.com/article/3040982/security/data-breaches-often-result-in-ceo-firing.html

Southern, C., 2017. Why are CEOs losing jobs over breaches? Reputation. Available at: https://blog.teklinks.com/why-are-ceos-losing-jobs-over-breaches-reputation
Swink, M. 2000. Technological innovativeness as a moderator of new product design integration and top management support. Journal of Product Innovation Management, 17, 208-220.
Teo, H.H., Wei, K.K. & Benbasat. I. 2003. Predicting intention to adopt interorganizational linkages: An institutional perspective, MIS Quarterly, 27(1), 19-49.

The Telegraph, 2010. Ink cartridge bomb reveals innovation of terrorist groups. Available at: http://www.telegraph.co.uk/news/uknews/terrorism-in-the-uk/8098587/Ink-cartridge-bomb-reveals-innovation-of-terrorist-groups.html. [2012-8-5].

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.

Tolbert, P.S., David, R.J., & Sine, W.D., 2011. Studying choice and change: The intersection of institutional theory and entrepreneurship research. Organization Science, 22(5), 1332-1344

Tsui, A.S., Zhang, Z., Wang, H., Xin, K.R., & Wu, J.B., 2006. Unpacking the relationship between CEO leadership behavior and organizational culture. The Leadership Quarterly, 17(2), 113-137.

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, 7, 171-222. JAI Press, Greenwich, CT.

U.S. News 2012. Pirates on the highways: Cargo theft costing nation billions. Available at: http://usnews.nbcnews.com/_news/2012/08/05/13132047-pirates-on-the-highways-cargotheft-costing-nation-billions?lite. [8-5-2012].

Villena, V., Lu, G., Gomez-Mejia, L., Revilla, E. 2018. Is top management team–supply chain manager interaction the missing link? An analysis of risk-bearing antecedents. International Journal of Operations & Production Management. 38(8), 1640-1663.

Voss, M.D., & Whipple, J.M., 2008, Food Supply Chain Security: Issues and Implications. Chapter 18 in *Supply Chain Risk: A Handbook of Assessment, Management and Performance*, Zsidisin GA, Ritchie B (eds), Springer Science + Business Media.

Walley, N. & Whitehead. B. 1994. It's not easy being green. Harvard Business Review, 72, 46-52.

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.

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., 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.

Williams, Z., Lueg, J.E. Goffnett, S.P. LeMay, S.A. & Cook. R.L. 2012. Understanding supply chain security strategy. Journal of Transportation Management, Spring/summer, 7-25.

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.

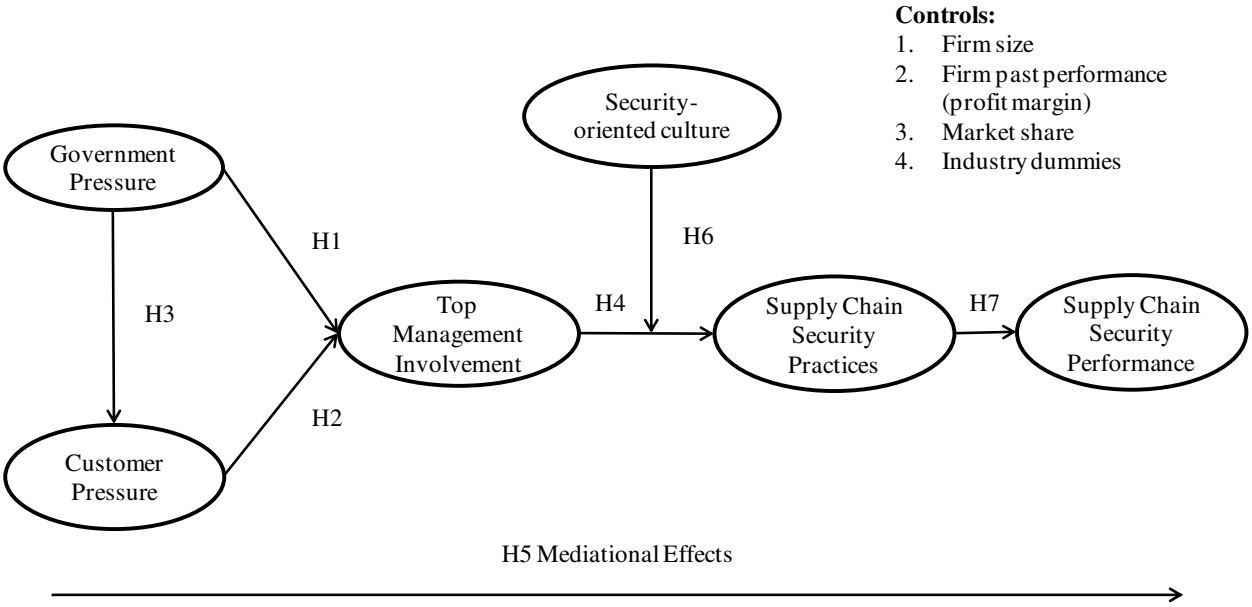

Figure 1. The conceptual model.

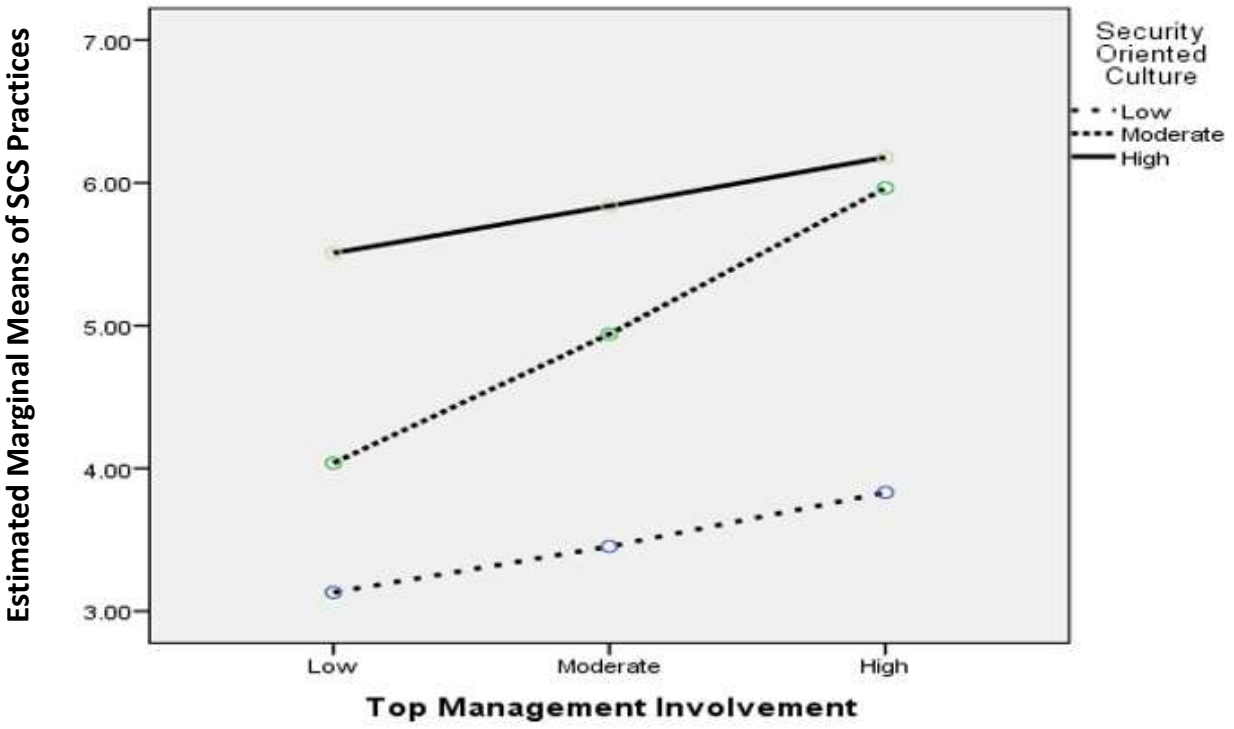

Figure 2. Marginal Means for SCS practices – Interaction Plot

Table 1. Description of sample

Number of Employees	Frequency	Percent	Annual Revenue	Frequency	Percent
Less than 100	21	21	Less than 10 million	8	5%
100 to 499	60	60	10 to 99.9 million	62	37%
500 to 999	20	20	100 to 999.9 million	38	23%
1,000 to 9,999	27	27	1 to 10 billion	36	22%
Over 10,000	38	38	More than 10 billion	22	13%
Total	166	100%	Total	166	100%
Position	**Frequency**	**Percent**	**Type of Commerce**	**Frequency**	**Percent**
VP/Sr. VP/President	19	11%	Business-to-business (B2B)	90	54%
CEO/COO	19	11%	Business-to-consumer (B2C)	43	26%
Director	37	23%	Both	33	20%
Managers	81	49%			
Others	10	6%			
Total	166	100%	Total	166	100%

Table 2. Means, standard deviations, and correlations of the non-categorical variables

	Mean	SD	1	2	3	4	5	6	7	8
1 Firm size (annual sales)	3.00	1.40								
2 Past performance (profit margin, in %)	21.03	17.20	-0.12							
3 Market share (in %)	36.71	29.66	-0.06	0.42**						
4 Government pressure	4.19	1.50	0.19*	0.09	0.08					
5 Customer pressure	4.75	1.49	-0.03	0.16*	0.16*	0.55**				
6 Top management involvement	5.34	1.21	0.01	0.16*	0.18*	0.35**	0.60**			
7 Security-oriented organizational culture	5.13	1.09	0.11	0.13	0.12	0.55**	0.63**	0.73**		
8 SCS practices (2nd order)	4.71	1.48	0.16*	0.12	0.16*	0.40**	0.52**	0.76**	0.80**	
9 Supply chain security performance	4.47	1.27	0.06	0.23**	0.13	0.47**	0.48**	0.59**	0.66**	0.75**

*p < 0.05, **p < 0.01 (two-tailed).

Table 3. Structural Model Results

Path	Standardized Coefficient	T-value	Significance
Control Variables			
Firm size → SCS practices	0.245	4.005	**0.000**
Past Performance → SCS practices	0.110	1.842	0.065
Market Share → SCS practices	-0.072	-1.232	0.218
SIC code → SCS practices	-0.103	-1. 777	0.076
Firm size → SCS performance	-0.018	-0.265	0.791
Past Performance → SCS performance	-0.052	-0.723	0.470
Market Share → SCS performance	0.011	0.172	0.863
SIC code → SCS performance	0.081	1.346	0.178
Main Effects			
Government Pressure → Customer Pressure	0.757	9.420	**0.000**
Government Pressure → Top Mgmt Involvement	0.598	4.421	**0.000**
Customer Pressure → Top Mgmt Involvement	0.370	2.480	**0.013**
Top Mgmt Involvement → SCS practices	0.409	2.478	**0.013**
Security-oriented organizational culture → SCS practices	0.569	3.484	**0.000**
Security practices → SCS performance	0.939	28.013	**0.000**
Interaction Effect			
Security-oriented organizational culture X Top Mgmt Involvement → SCS practices	0.225	3.416	**0.001**

Model Fit: χ^2=616.071 (465 df), χ^2/df = 1.324, CFI=.931, TLI=.919, RMSEA=.063, 90% C.I. RMSEA (.048, .075)

Table 4: **Analysis of mediation effects (full mediation)**

Paths	Bias corrected bootstrapping 95% CI	
	Lower	Higher
Paths ending at SCS Performance		
Total Effects: Government Pressure → SCS Performance	**0.285**	**0.667**
Specific Indirect Effects		
Government Pressure → Customer Pressure → Top Management involvement → SCS practices → SCS Performance	**0.039**	**0.510**
Government Pressure → Top Management involvement → SCS practices → SCS Performance	**0.040**	**0.364**
Total Effects: Customer Pressure → SCS Performance	**0.195**	**0.611**
Specific Indirect Effects		
Customer Pressure → Top Management involvement → SCS practices → SCS Performance	**0.195**	**0.611**
Paths ending at SCS practices		
Total Effects: Government Pressure → SCS practices	**0.316**	**0.724**
Specific Indirect Effects:		
Government Pressure → Customer Pressure → Top Management involvement → SCS practices	**0.045**	**0.395**
Government Pressure → Top Management involvement → SCS practices	**0.042**	**0.557**
Total Effects: Customer Pressure → SCS practices	**0.218**	**0.663**
Specific Indirect Effects:		
Customer Pressure → Top Management involvement → SCS practices	**0.218**	**0.663**

Table 5: **Conditional effect of X on Y at varying levels of the moderator (M) using the Johnson-Neyman technique**

Security-Oriented Org. Culture	Effect	SE	t-value	p-value	LLCI	ULCI
-3.5301	.0081	.1715	.0473	.9623	-.3307	.3469
-3.2601	.0295	.1607	.1838	.8544	-.2880	.3471
-2.9901	.0510	.1503	.3392	.7349	-.2460	.3480
-2.7201	.0724	.1403	.5161	.6065	-.2049	.3497
-2.4501	.0939	.1309	.7172	.4743	-.1647	.3524
-2.1801	.1153	.1220	.9448	.3463	-.1258	.3564
-1.9101	.1367	.1140	1.1995	.2322	-.0885	.3620
-1.6401	.1582	.1069	1.4793	.1412	-.0531	.3695
-1.3701	.1796	.1010	1.7779	.0774	-.0200	.3792
-1.1953	.1935	.0979	1.9759	.0500	.0000	.3870
-1.1001	.2011	.0965	2.0833	.0389	.0104	.3918
-.8301	.2225	.0936	2.3778	.0187	.0376	.4074
-.5601	.2439	.0924	2.6406	.0092	.0614	.4265
-.2901	.2654	.0930	2.8540	.0049	.0816	.4491
-.0201	.2868	.0954	3.0077	.0031	.0984	.4752
.2499	.3083	.0994	3.1019	.0023	.1119	.5046
.5199	.3297	.1048	3.1445	.0020	.1225	.5369
.7899	**.3511**	**.1116**	**3.1475**	**.0020**	**.1307**	**.5716**
1.0599	.3726	.1193	3.1230	.0021	.1368	.6083
1.3299	.3940	.1279	3.0810	.0025	.1413	.6467
1.5999	.4155	.1372	3.0290	.0029	.1444	.6865
1.8699	.4369	.1470	2.9724	.0034	.1465	.7273

[a] Controlled for firm size (annual sales), past performance (profit margin), market share, SIC code.
Culture value is centered; the highest t-value is in bold.
Model summary: R-square=0.466, MSE=0.875, F=18.72 (df1=7, df2=150), p=0.000.

Deployment of Supply Chain Security Practices: Antecedents and Consequences

Online Appendix A. Description of SCS Practices

Materially, the organization needs to engage in practices to help it *detect* whether security breaches are about to occur and study events and vulnerabilities via *diagnostic* practices to anticipate where and when breaches may occur. Speier et al. (2011) define detection as the supply chain's ability to recognize an incident. They note that it is vital that a threat is detected before it materializes as a security breach. Sheffi (2005, p. 155) defines detection as the process of distinguishing a true problem from the sometimes considerable variations of normal day-to-day business. Firms may deploy technology (Williams et al., 2008) to identify threats and monitoring processes to detect deviations and near misses. While it is important to protect the supply chain and detect potential threats, it is also equally vital to conduct in depth analysis of SCS breaches and examine processes across supply chain tiers to identify vulnerabilities (i.e., diagnostics).

To avert breaches from materializing, the organization can adopt *protective* practices to secure the physical supply chain (e.g., carriers, facilities) and minimize risk by apposite *supplier selection* practices that weigh in supply chain security considerations. Given that current supply chains involve numerous suppliers across tiers and given that a breach of security at any node or link can be disastrous, identifying potential suppliers that exhibit strong security capabilities is vital. The supply chain is as strong as the weakest partner. As Speier et al. (2011) note, "Supply chain partners' capabilities need to be verified from a security standpoint as partners who lack sufficient security capabilities might be replaced" (p. 726). In addition, as the overall level of supply disruption risk increases, buyers are more likely to select alternative suppliers who may be more capable of protecting the products throughout the supply chain hand-offs (Ellis et al., 2010).

To mitigate risk, organizations invest in *contingency planning* practices that prepare the organization to cope with a breach once it emerges. This reflects practices that enable the organization to respond to a breach that has already occurred (Williams et al., 2008). Organizations need well defined plans to react to a crisis and definitive plans which spell out what to do. To assure that the organization is able to cope with emerging threats, there is a need for an element of *continuous improvement* practices. New threats demand that the organizational SCS strategy and responses are current and commensurate with the magnitude of the risk the organization may encounter in the near and distant future. It is essential that any program has an embedded element of unceasing development. Williams et al. (2008) note that SCS practices need to be monitored and maintained and warn that failure to do so can be disastrous. As threats change in form and intensity so does the organization needs to reconsider its practices, tools and practices. Training employees for security and risk management when assuming new roles, monitoring whether practices and objectives are met, updating the SCS strategy, and implementing corrective procedures when lapses are observed is critical.

Online Appendix B. Measurement Model Methods

We first wanted to assess whether a second-order specification can describe relationships between our SCS practices. Towards this task alternative measurement model configurations were tested (Koufteros et al., 2009). The results demonstrate that our higher-order specification can be empirically supported. Specifically, the fit indices produced by the second-order model specification are fairly similar to the fit indices of an all first-order correlated variable specification (the fit indices for these two models were vastly superior vis-a-vis the fit indices of other competing models). Statistically, the model fit did not differ across the two specifications (χ^2_{diff}=13.54, 9 df, p>0.14) but the second-order model specification offers clear advantages as SCS practices typically emanate from a specific system or program and work in concert. Therefore, SCS practices are represented in the structural model via a full aggregation specification (see online Appendix C).

Using raw data as input, we stipulated two measurement models via Mplus 7.2; one measurement model included the two forms of coercive institutional forces, top management involvement, and organizational culture. The second measurement model included SCS practices and SCS performance. The two separate models were necessary in order to avert identification problems if a singular model was specified. Given the size of the model and our sample size we would not have enough degrees of freedom to obtain a reliable solution. We mitigate concerns regarding discriminant validity by testing for it for all possible pairs across measurement models. Each measurement model was examined using multiple model fit indices (i.e., χ^2/df, CFI, TLI, SRMR, and RMSEA) to assess congruence between the data and our respective measurement model. To evaluate convergent validity, we probed the size of item-factor loadings (and respective t-values) (Kline, 1998). We evaluated discriminant validity using the χ^2 difference test (Bagozzi and Phillips, 1982) for all pairs of latent variables across measurement models. Construct reliability was appraised through composite reliability (CR) and average variance extracted (AVE).

Online Appendix C. Competing Models for SCS Practices.

	Model 1 One first-order factor with all indicators	**Model 2** Six uncorrelated first-order factors	**Model 3** Six correlated first-order factors	**Model 4** Six first-order factors and one second-order factor
χ^2(df)	652.69(350)	1269.40(350)	547.48(335)	561.02(344)
χ^2/df	1.86	3.63	1.63	1.63
CFI	0.87	0.60	0.91	0.91
TFI	0.86	0.57	0.90	0.90
RMSEA	0.10	0.18	0.07	0.08
SRMR	0.06	0.52	0.05	0.05

Second-order factor: SCS Practices	**Std. loading**	**Std. error**	**t-value**
Continuous improvement practices	0.99	0.01	97.28
Contingency planning	0.98	0.01	79.56
Protective practices	0.98	0.04	28.07
Supplier selection	0.87	0.03	28.83
Detection practices	1.00	0.01	103.13
Diagnostic practices	0.99	0.01	114.31

Online Appendix D. Summary of Discriminant Validity Testing (χ^2 difference values)

	1	2	3	4	5	6	7	8	9	10
1. Government pressure										
2. Customer pressure	12.44									
3. Top management involvement	23.10	43.05								
4. Security-oriented culture	50.25	36.65	85.31							
5. Continuous improvement	35.48	12.82	64.20	70.86						
6. Contingency planning	41.99	15.78	66.94	84.15	153.24					
7. Protective practices	33.68	17.05	48.33	59.06	94.74	96.83				
8. Supplier selection	30.99	13.54	36.42	60.48	97.03	73.49	67.52			
9. Detection practices	30.76	25.91	59.47	75.41	136.04	138.64	106.54	90.33		
10. Diagnostic practices	44.64	14.77	54.43	84.11	156.31	145.74	90.90	98.19	159.35	
11. SCS performance	37.71	11.69	40.64	63.29	81.47	89.33	64.97	62.22	89.06	90.22

Online Appendix E. Measurement scales

Factor and scale items	Std. loading	S.E.	t-value
Government pressure: CR=0.87, AVE=0.69			
There is definite pressure from our government to meet security standards	.899	.038	23.59
We will receive significant benefits if we adopt security standards prescribed by our government	.710	.089	7.98
Our government takes an active role on security matters	.869	.040	21.62
Customer pressure: CR=0.84, AVE=0.66			
Our customers pressure us to do better on security	.655	.076	8.64
We have to meet standards for security as our customers are demanding us to do so	.861	.044	19.64
Our customers hold us accountable for security	.894	.037	24.08
Top management involvement: CR=0.88, AVE=0.61			
Our top management has assumed a leadership role in risk management	.850	.038	22.39
Our top management allocates proper levels of resources to enhance the security of our supply chain	.657	.067	9.78
Our top management provides clear objectives for securing the supply chain	.817	.043	19.51
Top management has an active oversight over supply chain risk management	.847	.038	22.08
Top management is aware of the risks and consequences associated with supply chain disruptions	.702	.061	11.43
Security-oriented organizational culture: CR=0.87, AVE=0.57			
Putting supply chain security first is a sentiment widely shared within the organization	.822	.042	19.43
We believe that supply chain security is the responsibility of everyone in the organization	.634	.071	8.93
We believe that supply chain security concerns should be viewed with respect	.808	.044	18.57
We believe that there are considerable security threats that can impact us	.759	.052	14.61
We believe that even minor security breaches in our supply chain will be devastating to our company	.752	.053	14.23
Measurement Model fit: $\chi^2(98)=139.41$, $\chi^2/df=1.42$, CFI=0.95, TLI=0.93, SRMR=0.06 and RMSEA=0.07			
Continuous improvement practices: CR=0.92, AVE=0.73			
All of our employees are trained for security and risk management whenever they assume new roles	.763	.047	16.27
We monitor whether the organization's SCS strategy and objectives are met	.889	.025	35.89
We update or reassess the supply chain security strategy as conditions change	.895	.023	38.78
We have corrective procedures when security lapses are detected	.873	.028	31.24
Contingency planning: CR=0.88, AVE=0.65			
We know what to do when we encounter supply chain security breaches or crises	.862	.030	29.18
We have a well-defined contingency plan to react to serious supply chain security breaches	.916	.020	46.35
We spell out what to do in the event of a security breach or crisis	.853	.031	27.09
Someone follows up when we raise a serious concern or identify a problem	.554	.079	7.04
Protective practices: CR=0.76, AVE=0.51			
We require comprehensive security capabilities from carriers	.755	.059	12.86
We secure containers at our facilities to assure they are not compromised	.661	.067	9.91
We authenticate the identity of visitors in our facilities	.726	.077	9.43
Supplier selection: CR=0.94, AVE=0.83			
Supplier security is an important criterion when selecting our suppliers	.967	.012	82.16
We only approve suppliers (irrespective of tier) that have a risk management program in place	.808	.041	19.50
When selecting suppliers we weigh in whether the supplier has a secure supply chain	.955	.013	73.13
Detection practices: CR=0.89, AVE=0.52			
We use active measures such as video and sensors to be able to detect security breaches	.687	.059	11.63
We use sophisticated technologies to detect if containers have been compromised	.734	.052	14.16
We use RFID or other similar technology for tracking purposes throughout our supply chain	.714	.083	8.60
We verify that all shipments are legitimate	.575	.075	7.71
We make use of anti tampering technologies on containers	.570	.075	7.58
We monitor the loading/unloading process of cargo to identify potential security breaches	.793	.042	18.84
We have procedures to detect supply chain security failures or near failures	.741	.052	14.37
We have procedures to detect near misses in supply chain security	.883	.026	32.27
Diagnostic practices: CR=0.93, AVE=0.70			
We regularly assess supplier security performance against security standards	.836	.035	23.74
We do conduct in-depth analysis of supply chain security breaches	.853	.031	27.10
We do conduct periodic assessments of our supply chain security	.883	.026	34.10
We maintain an incident data base of supply chain security breaches	.824	.037	22.19
We examine all tiers in our supply chain to identify potential security vulnerabilities	.867	.028	30.86
We conduct unannounced security assessments of our logistics systems	.761	.048	15.95
SCS performance: **(in last three years, our firm has experienced)** : CR=0.88, AVE=0.52			
A reduction/less potential for theft/loss	.603	.076	7.93
An improved capability to detect counterfeit parts/products	.750	.083	9.04
A lower probability that our supply chain will be compromised	.889	.032	27.70
A lower probability of cargo misuse	.681	.065	10.51
Lower levels of supply chain vulnerability	.646	.069	9.37
An improvement in security	.812	.043	18.91
A reduction/less potential for smuggling of drugs	.633	.075	8.44
Measurement Model fit: $\chi^2(521)=759.12$, $\chi^2/df=1.46$, CFI=0.91, TLI=0.90, SRMR=0.06 and RMSEA=0.07.			

Online Appendix F. Common Methods Bias

We addressed common method bias (CMB) through both procedural and statistical approaches (Craighead et al., 2011). We used the following procedural remedies: we assured respondent anonymity, scrambled measurement items for the theoretical constructs, reduced item ambiguity via interviews and a pilot study, and included several marker variables in the survey. Next, we used statistical approaches to assess CMB. We first fitted a model with all measurement items loaded on a common-method factor (i.e., Harman's single factor) via a CFA approach. If CMB exists, a latent variable will account for all indicators (Podsakoff et al. 2003). The fit indices failed to support a single factor: χ^2 (1224) =2452.39, χ^2/df=2.00, CFI=0.71, TLI=0.69, SRMR=0.08, and RMSEA=0.11.

We also used a marker variable technique by deploying three indicators which are theoretically unrelated to the variables of interest (Malhotra et al., 2006; Craighead et al., 2011). The correlations of marker variables with the variables of interest in the structural model were low and statistically non-significant. For example, the marker indicators and their correlations with government pressure were: (1) Our customers require us to play soccer (r=0.094), (2) We eat dinner at a restaurant on an everyday basis (r=0.092), and (3) We only hire employees who support the San Antonio Spurs (r=-0.024). We also correlated the marker variables with SCS performance and the correlations were (1) r=0.033, (2) r=0.050, (3) r=-0.069 respectively. The low correlations suggest that CMB is not a worrying concern.