Supply Chain Security: A Classification of Practices and an Empirical Study of Differential Effects and Complementarity

Guanyi Lu, Xenophon Koufteros, and Lorenzo Lucianetti

***Abstract*—Supply chain security (SCS) breaches (a form of supply chain risk) are distressing supply chains and they have the potential to engender acute pain on the society at large. To counteract such breaches, international bodies, nations, societies, industries, and firms have instituted several countermeasures in the form of standards and respective practices. Given that not all incidences/breaches can be averted, the risk management literature advocates that firms should adopt practices that can thwart incidences/breaches and practices that can provide a swift response once an incident/breach is detected in order to contain damages, ease the pain, and restore operations. Resting on the risk management literature and interactions with professionals, we classify SCS management practices into four categories based on their intent (i.e., detection, prevention, response, and mitigation) and operationalize each via multiple indicators. We then test the relative efficacy of these practices to explain SCS performance using responses from 462 firms operating in the United States and Italy.**

***Index Terms*—Classification, complementarity, differential effects, risk management, supply chain security (SCS).**

I. Introduction

SUPPLY chain security (SCS) has become relevant to both practitioners and academics in recent years because the consequences of SCS breaches can be rather disastrous to the wellbeing of individuals, firms, supply chains, and the society [1], [2]. Serious SCS incidences such as the 9/11 terrorist attacks [3], massive seizures of counterfeit or substandard food and drinks in Europe and elsewhere in 2016 [4], the 2010 Eli Lilly prescription drug heist [5], and the 2015 smuggling of pounds of cocaine in plastic bananas [6] stand as a testament that breaches can inflict serious pain. These examples testify that there is no shortage of will and determination by criminals to engage in illicit activities. The International Organization for Standardization (ISO) articulates that "[any] intentional, unauthorized act ... that is designed to cause harm or damage to, or by, the supply chain is considered as a supply chain security breach [7, p. 2]." Given that motivated offenders are omnipresent, firms feel the pressure to implement a variety of practices to render themselves less vulnerable to breaches [8], [9].

Our research examines whether organizational practices enhance SCS. Given that SCS threats represent a special form of supply chain risk [10], [11], we build upon the supply chain risk and disruption management literature. SCS threats, however, differ from other supply chain risks due to their relatively higher level of intentionality. Their intentional and evolving nature makes them more difficult to predict and the wide spectrum of sources and actors creates pragmatic challenges.

To combat SCS threats and breaches, governments, international bodies (e.g., the EU), as well as professional organizations (e.g., ISO) and leading firms such as IBM have launched a plethora of SCS management (SCSM) standards and programs, each prescribing a number of specific practices. In addition, academic and practitioner manuscripts proffer a number of practices to address SCS; some of these practices resemble routines advocated by the quality management literature at large [12]. Unfortunately, the specific intent of the fairly large number of SCSM practices is not clearly articulated. Based on a literature review and numerous interactions with executives, we first contribute to the literature by adapting conceptualizations developed for general risk management to the context of SCS and by classifying practices according to their intent into four classes (i.e., detection, prevention, response, and mitigation). Through a multiphased project, we operationalize each class of practices with multiple indicators. Our categorization and operationalization may facilitate empirical research in this under-studied area.

We assert that detection and prevention practices share the primary task of thwarting breaches while response and mitigation may be more adept at buttressing recovery when breaches do occur. There is, however, a quandary whether there are differential effects since there is scant empirical research that first examines the differential effects of practices on SCS performance. Williams *et al*. [2] acknowledged the lack of empirical studies relating SCS activities and performance eight years ago and this largely still stands. In the more general field of supply chain

Manuscript received July 24, 2015; revised March 8, 2016, August 10, 2016, and December 22, 2016; accepted January 3, 2017. Review of this manuscript was arranged by Department Editor Srinivas Talluri.

G. Lu is with the Supply Chain and Decision Sciences Department, Oregon State University, Corvallis, OR 97331 USA (e-mail: Guanyi.Lu@oregonstate.edu).

X. Koufteros is with the Information and Operations Management Department, Texas A&M University, College Station, TX 77843 USA (e-mail: XKoufteros@mays.tamu.edu).

L. Lucianetti is with the Department of Management and Business Administration, University of Chieti and Pescara, Pescara 65127, Italy (e-mail: llucianetti@unich.it).

This paper has supplementary downloadable material available at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TEM.2017.2652382

risk management, Ho *et al*. [13] reviewed more than 200 studies. Only less than 10% of quantitative studies adopted an empirical methodology (7 out of 119 individual quantitative methods studies, Table VII, p. 5054) and 4 out of 40 integrated quantitative methods studies (Table VIII, p. 5056), and those studies did not focus on practices; very little has been produced in terms of practices and their relationship with performance. Our study thus contributes to the literature by furnishing large-scale empirical evidence regarding the seldom examined practice–performance relationship with special attention on differential effects. Probing the relative efficacy of each class of practices is vital since firms often have limited resources and they have to make tough choices.

Kleindorfer and Saad [11], however, advocate that a collective approach to the implementation of risk management practices should be considered. They specified a set of principles and argued that these principles must be simultaneously implemented in an integrative way. They allude to an advantage that is engendered by the combinative capabilities afforded when all principles and respective practices are applied concurrently. Materially, we add value to the literature by also examining whether the argument for combinative capabilities can be empirically supported in the realm of SCS. If the empirical evidence favors a combinative approach, then firms should assume a more systemic implementation of practices.

II. Literature Review, Conceptual Development, and Hypotheses

Rothschild [14] offers a historical perspective of definitions and considerations regarding the word security. She writes (p. 61): "The Latin noun 'securitas' referred, in its primary classical use, to a condition of individuals, of a particularly inner sort. It denoted composure, tranquility of spirit, freedom from care, the condition that Cicero called the 'object of supreme desire,' or 'the absence of anxiety upon which the happy life depends'." For Fischer and Green [15] security "implies a stable, relatively predictable environment in which an individual or group may pursue its ends without disruption or harm and without fear of disturbance or inquiry (p. 21)." From an absolute sense, SCS can be viewed as a state of being which is free from breaches. We view SCS as a state with a low level or low potential for breaches caused primarily by intentional acts.

A. Categorization of SCSM Practices

Our review of the SCS literature suggests that our knowledge of the effects of SCSM practices is relatively nonaccumulating and insufficient for delivering meaningful insights for both academics and practitioners [2]. Current SCS research focuses on the impact of institutional forces on the adoption of SCSM practices [16] and relatedly, early adopter benefits [17]. Potential metrics for SCS performance have been developed for only few industries (e.g., shipping and logistics, [18], [19]). Despite some advances, few empirical inquiries about SCS have emerged and our understanding about SCSM is still incomplete at best [20].

SCS breaches represent a special form of supply chain risk [2], [12], [21]. Unlike other sources of risk, SCS breaches, however, emanate almost exclusively from intentional acts (mostly associated with illicit activities) such as theft, terrorism, counterfeit products, smuggling, sabotage, and illicit acquisition and use of data amongst others [22]. Sarathy [23] notes that supply chains are difficult to secure because vulnerabilities span goods, factories, supply chain partners and their facilities, freight carriers, people, and information. Speier *et al*. [8] claim that much of the supply chain is unguarded and emphasize that the breadth of the supply chain infrastructure makes total protection difficult.

A wide search of the literature across journal outlets produced a vast array of SCSM practices that are advocated [24]–[26]. Gutierrez and Hintsa [27] contrasted nine SCS programs and estimated that the degree of similarity in practices amongst the programs varied from 25% to 76%; the majority shared less than 50% similarity. The large scope of SCSM practices reflects that security breaches may affect many firm activities or be attributed to a variety of sources [28], [29].

While in some respects it is a blessing that there is an abundance of practices advocated by the literature, organizing them into a meaningful framework is a challenge. One for instance can categorize all supply management related practices into one class of practices; in other words, all practices that involve the management of the supply base, such as supplier selection and retaining multiple sources, can be grouped into a single class because they all share the "supply management" aspect. However, this can be rather perilous because the intent of each specific practice may be different. Careful supplier selection may boost the capability to avert an SCS breach while deploying multiple sources may enhance the ability to mitigate the impact of a disruption prompted by a breach; each practice may be constructive but in divergent ways. Practitioners may have a vested interest to know the specific intent of each practice so they can invest wisely in practices that aim to fill particular gaps.

Also, the efficacy of practices to explain SCS performance remains largely untested [30]–[33] and thus managers are in a quandary trying to decide whether to invest more or less toward a specific practice or class of practices. This is not due to lack of academic interest; rather, researchers find it increasingly difficult to obtain responses on a topic related to security [20].

Since SCS breaches represent a special form of supply chain risk [21], it may be conducive to rely on the contributions advanced by the risk management literature for guidance when categorizing practices into classes. While again large empirical inquiries are scarce, there is a significant body of conceptual work that can offer direction. Juttner *et al*. [31] suggest that risk management should include avoidance (e.g., selecting more apposite suppliers), control (e.g., maintaining excess capacity), cooperation (e.g., share risk related information), and flexibility (e.g., multiple sourcing). In their detailed treatise, Kleindorfer and Saad [11] specify ten principles to tackle vulnerabilities. These include respective practices toward identification and mitigation of disruption risks, diversification of

TABLE I
CLASSIFICATIONS OF RISK AND DISRUPTION MANAGEMENT PRACTICES (AND PRINCIPLES)

Study	Classification
Helferich and Cook [43]	Planning, mitigation, detection, response, recovery
Juttner *et al*. [31]	Avoidance, control, cooperation, flexibility
Closs and McGarrell [22]	Identification of alternative source of supply, reduction of risk, deployment of detection equipment, response to incidents, anticipatory establishment of incident recovery
Kleindorfer and Saad [11]	Identification & mitigation of disruption risks, diversification of risk, incentive alignment & collaboration, prevention, balancing robustness vis-à-vis efficiency, back-up systems & contingency plans, sharing information, risk assessment, agility/flexibility, use of TQM principles
Autry and Bobbitt [26]	Preparation & planning, partnerships, organizational adaptation, communication, technology
Ponomarov and Holcomb [63]	Analysis and assessment, event readiness, response, recovery
Blome and Schoenherr [36]	Identification, analysis, mitigation, monitoring
Speier *et al*. [8]	Prevention/ Planning, detection, response, recovery
Sodhi *et al*. [34]	Identification, assessment, response, mitigation
Kern *et al*. [37]	Identification, assessment, mitigation
Starr and Van Wassenhove [35]	Anticipation, prevention, mitigation
Ho *et al*. [13]	identification, assessment, mitigation, monitoring

risk, incentive alignment and collaboration, prevention of incidents, building robustness vis-à-vis efficiency, readiness, collaboration, risk assessment, agility/flexibility, and application of total quality management (TQM) principles. While this is an informative and fairly exhaustive list, there is significant overlap amongst the principles, and the sheer number of ten principles is not overly parsimonious. Sodhi *et al.* [34] organize the supply chain risk management literature along four key elements. These include identification, assessment, mitigation, and response and underline the processes that firms embark on to cope with supply chain risk. Starr and Van Wassenhove [35] discuss three overall processes to cope with humanitarian disasters and risk management at large. These include anticipation, prevention, and mitigation. Similarly, Speier *et al*. [8] theorize that to engender sustainable supply chains when subjected to product safety and security risks, firms need to develop capabilities to prevent, detect, respond to, and recover from breaches within their supply chains. Blome and Schoenherr [36] ascertained what they coined "stages" of supply chain risk management. These include risk identification, risk analysis, risk mitigation, and risk monitoring. The authors, however, place little emphasis on prevention activities. Their stages and respective practices are reflected by our detection, response, and mitigation practices. Kern [37] stands as a rare exception in the literature, since it operationalized some of the practices and related them to each other and performance using a fairly sizable sample ($n = 162$). He specifically tested a model relating risk identification, risk assessment, and risk mitigation to risk performance. The author overemphasized some aspects but the concept of prevention is absent. Sheffi *et al*. [38] note that efforts to secure the supply chain can be split into two main categories. The first category includes practices aimed at averting breaches, i.e., detection and prevention. The second category entails practices that enable prompt response to a disruption and practices to mitigate their adverse consequences.

In order to be more cognizant of actual practices it is also conducive to study largely popular standards, such as ISO, for guidance. ISO has introduced a standard (i.e., ISO 28000) for SCS in 2007. This standard implicitly acknowledges a variety of practices that can engender higher levels of security. ISO is also very explicit in terms of the domain or scope of SCS [ISO 28000:2007(E)]:

> "The organization shall establish, document, implement, maintain and continually improve an effective security management system for identifying security threats, assessing risks and controlling and mitigating their consequences" [7, p. 3].

> "The organization shall establish, implement and maintain appropriate plans and procedures to identify the potential for, and responses to, security incidents and emergency situations, and for preventing and mitigating the likely consequences that can be associated with them" [7, p. 9].

It is apparent that the scope of SCSM, as conceptualized by ISO, extends beyond mere prevention of incidences; it includes practices to identify threats, prevent threats from manifesting as breaches, and lessen the impact of breaches when they occur. In summary (see Table I), the elements of detection and prevention are cited by most of the respective literature as means to thwart breaches. In other words, these practices are salient prior to a threat becoming a breach. Similarly, the elements of response and mitigation appear to be more germane once a breach emerges. We note that there is a clear distinction between response and mitigation in SCSM [41]; Tomlin [42] articulates that mitigation practices are invoked in advance of an incident while response tactics are deployed once an incident has emerged. Similarly, Helferich and Cook [43] refer to mitigation as ongoing actions undertaken ex ante of a disaster.

We also delved into the TQM literature for guidance as it has a long and rich tradition examining the efficacy of prevention and inspection practices. TQM is a holistic management philosophy [44], [45]. While the broad scope of TQM renders little agreement on the list of best TQM practices [46], many studies have highlighted the role of prevention vis-a-vis inspection practices [47]. Failure to prevent defects results in extra time, money, and workload to rectify defects and thus many researchers have argued that prevention is the most effective TQM practice [48]. Lee and Whang [12] draw the parallel between security and quality and propose that prevention is essential because an SCS

threat has the potential to engender havoc. However, not all defects can be detected and prevented and thus some firms opt to further inspect products before they exit the line. Inspection is similar to detection in the sense that both scrutinize the integrity of products. However, inspection in TQM is a reactive practice [48] that occurs after a defective product is already manufactured. Firms can place less emphasis on inspection if effective defect prevention is in place [48]. Progressive firms invest in detecting abnormal trends or anomalies before a defect materializes. Detection is thus more proactive in nature. Detecting potential threats is arguably the first step in combating SCS breaches and cannot be overlooked [22].

The classification of SCSM practices into detection, prevention, response, and mitigation is parsimonious and espouses the principles advocated by the literature. For instance, the aspect of "anticipating disasters" [35] is acknowledged by the *response* class of practices. The essence of the ten principles for managing risks as articulated by Kleindorfer and Saad [11] is covered when all four classes of practices are considered. Our classification is closest to Speier *et al*. [8] (i.e., prevent, detect, respond, and recover) but we consider "respond" and "recover" practices as belonging to a single class while we argue that mitigation is a separate class as we articulated above.

B. Classes of Practices and Hypotheses

1) Detection: Speier *et al*. [8] define detection as the supply chain's ability to recognize or sense an incident. They note that it is vital that a threat is detected before it materializes as a security breach. Detection practices generally rely on sophisticated technologies or processes to discover whether or not containers, equipment, or facilities are about to be breached [28]. For instance, firms utilize real-time cargo tracking via a variety of technological solutions. They also actively monitor the (un)loading processes to identify potential SCS breaches. Such actions empower firms to synthesize information regarding supply chain operations in real time and reduce the opportunity for theft, smuggling, and employee sabotage. In addition, criminal activities (e.g., employee theft, terrorist attacks, counterfeiting) are carried out by different people with divergent methods and intents and thus require different detection resolutions [38]. Detection practices can expose a variety of illicit activities, prompting preemptive organizational action. They may also involve conducting periodic assessments of suppliers' security operations [11], [29]. This enables firms to detect "near misses" in SCS breaches and notify supply chain partners to enact corrective action. Highly effective detection practices reduce the probability that potential SCS threats are overlooked or ignored [29] and thus improve SCS performance.

2) Prevention: Prevention practices focus on averting security breaches [28], [29]. Prevention practices are necessarily proactive in nature as they attempt to stop an event from materializing [21]. Given that current supply chains involve numerous suppliers across tiers and a security breach can occur at any node or link, firms deploying such practices not only exercise due diligence internally but they also hold all suppliers accountable for SCS [17]. They often secure containers at their facilities, which deters criminal activities [18]. They educate employees and suppliers about SCS, which reduces the probability that potential SCS threats are under-identified. Communication channels are established so that supply chain partners across tiers can be notified if potential threats emerge in order to halt them. As these practices prevent SCS breaches, firms may preserve resources to resolve other SCS challenges. In addition, if the firm can prevent most SCS breaches, only a limited number of threats may need to be tackled by the reactive and mitigation practices of the firm. Consequently, security risk is lowered and therefore SCS performance can be enhanced. Note that detection is alike to quality control charts that can identify whether variation is abnormal. It does not reflect appraisal-type practices which aim to appraise quality (inspect for defects) after the product is already produced.

3) Response: Firms cannot prevent all SCS breaches and thus they should anticipate different types of breaches that they may face. Speier *et al*. [8] suggest that processes can be implemented to assure continued organizational reliability. Having strategies, processes, and personnel in place to respond to a breach enables the firm to retort more effectively [20]. Response practices involve activities designed to prepare the firm to counter emerging SCS breaches. Typical response practices invoke developing protocols for communication when a crisis arises [28], delegating authority so that teams/individuals can take necessary action, deploying a quick reaction force [38], and utilizing disaster recovery plans. These practices afford early intervention and provide significant value to counter the adverse effects of a breach. They ensure firms can make efficient and effective problem resolution possible, improving SCS performance.

4) Mitigation: Finally, firms cannot overlook the need for deploying mitigation practices [33]. Mitigation practices attempt to reduce losses of supply chain assets (life and property) by lessening the impact of security breaches; they rest on the interrelated concepts of redundancy and flexibility [3], [11], [38]. Firms have to quickly resume normal operations because any breakdown caused by SCS breaches can be very costly [3]. In an endeavor to mitigate these detrimental effects and ease the painful consequences of a breach, firms may simplify product design, develop alternative material sources, or maintain strategic inventories [29]. A firm could also cross-train employees that can assume a variety of roles, and simplify jobs to the extent that unskilled workers can perform them, if and when the firm endures a crisis. The development of back-up processes furnishes access to critical resources at times of crises [11]. Mitigation practices enhance the ability of firms to recover before serious and long-term effects materialize. Moreover, mitigation practices pertaining to product design or the development of alternative supply sources compel firms to carefully review their internal and external operations, improving organizational learning toward SCS performance. Taken together, we propose:

H_{1a-d}. *Detection (a), prevention (b), response (c), and mitigation (d) practices are positively associated with SCS performance.*

While the four types of practices all aim at enhancing SCS, they have idiosyncratic or diverse approaches in coping with SCS threats. For example, detection practices are designed to uncover SCS threats before they emerge as breaches. Response

practices, on the other hand, denote corrective actions after SCS incidences emerge. Given the diverse roles of such practices, we posit that their efficacy in explaining SCS performance varies. Specifically, we assert that detection practices play the most prominent role. Conventional wisdom suggests that many supply chain threats—when detected early—can be addressed before causing damages and needing further treatment [8], [11]. The value of detection is in general underestimated since the damages from averted breaches cannot be easily estimated. In addition, detection makes effective protection and reaction possible. Alike the quality management literature, we argue that it is best to discover prospective defects before they emerge as real defects. Potential defects need to be identified first if they are to be prevented. When a breach surfaces, the early detection affords more time for the firm to counter the breach before it causes substantive damage. Detection practices provide synthesized and timely information for other SCSM practices to activate. The information enables multiple constituents within a firm (or along the supply chain) to coordinate their efforts to combat forthcoming SCS breaches. Since quite a few types of SCS breaches can be effectively cured or contained only when they are diagnosed early [33], a failure to detect them early would greatly compromise SCS. Detection not only directly affects SCS performance, but is also credited to be a catalyst for other SCS practices. Due to its unique role, we argue that the impact of detection on SCS performance will be the most potent.

H_{2a-c} *Detection has a greater positive association with SCS performance than prevention (a), response (b), and mitigation (c).*

Lee and Whang [12] draw an informative parallel between security and quality. They articulate that just like defects can be rather costly to a firm, breaches in security can also be devastating. The TQM literature has long advocated that the management of quality should not be merely corrective; rather firms ought to cope with prospective defects by preventing them from materializing. Rectifying damages or injuries sustained due to defects can be a lengthy and expensive proposition. Instead, the firm is best served when it invests in practices to prevent them from culminating into breaches [12], [32] because it often takes less effort to prevent something than to cure it. Quinn [49, p. 41] states that "it makes far more sense in terms of time, money, resources and aggravation to dedicate your efforts to preventing problems from happening." From an economic perspective, prevention provides a better return on investment (ROI) than response and mitigation which are mobilized during and on the aftermath of an SCS breach. Consider the analogy of the internal/external costs of quality vis-à-vis prevention costs. If a defect does materialize and the product leaves the premises of the firm, the costs to rectify a defect can be significantly higher than prevention costs, especially if customers sustain damages. Materially and perceptually, quality will suffer. On the other hand, when products are defect-free because defects are prevented, it enhances the stock of quality and reputation of the firm. Similarly, breaches that are prevented add significantly to the stock and level of SCS. Thus, we hypothesize:

H_{3a-b} *Prevention has a greater positive association with SCS performance than response (a) and mitigation (b).*

While we posited that practices may have differing effects on SCS, a synergistic effect may also exist. Kleindorfer and Saad [11] allude that the simultaneous implementation of principles to manage risk can generate combinative returns. For instance, if a threat is detected early, the supply chain can be alerted to the threat and prevention and reaction mechanisms can be mobilized. Prevention and reaction practices can be more effective in reducing vulnerabilities as the firm can amass assets to fend off the threats in due time. The early warning can alert organizational actors to prepare a swift response and assemble resources to mitigate an impending breach. In other words, the crisis management team can respond more effectively and efficiently because of the advance notice. Craighead *et al*. [50, p. 147] state "In essence, the quicker a supply chain disruption is detected and the quicker the pertinent information about it is communicated, the more time the supply chain would have to inoculate itself from the negative effects of the disruption and the less severe a supply chain disruption would likely be." Mitigation practices signify significant preparation and anticipation regarding the supply base, product development, logistics, and redundancy. Such preparation can enhance the efficacy of response practices because when the firm needs to react to a breach it offers options via flexibility or redundancy. We also noted above how detection practices can enhance the efficacy of other classes of practices. Essentially, this systemic approach suggests that the four types of practices may complement each other and their complementarity has the potential to improve SCS. SCS specific programs, such as ISO 28000, clearly assert that firms need to constantly assess the security environment in which they operate (i.e., detection practices are needed) in order to effectively respond to SCS events and mitigate SCS damages. Prevention practices, such as those associated with supplier management for instance, may facilitate early detection and quick response. We thus conjecture that firms usually deploy SCSM practices as a bundle as part of a formal/informal program such as ISO 28000. If the complementarity argument can be supported, then practices should perhaps be implemented as a system in order to garner the best returns.

H_{4a} *There is a complementarity amongst the detection, prevention, response, and mitigation practices.*

H_{4b}. *The complementarity of the four groups of practices is positively associated with SCS performance.*

III. Research Methods and Results

A. Research Design and Sample

We used a survey-based methodology to solicit responses from practicing executives. In order to assure the integrity of our measurement instrument, we undertook a three-staged preliminary inquiry (see Fig. 1). We targeted manufacturing units (a firm or a strategic business unit) located in the U.S. and Italy. We included Italy for two reasons. First, Europe also faces SCS threats, such as terrorism, drug smuggling, and theft, and has developed a variety of SCSM programs at the continental level [e.g., authorized economic operator (AEO) program]. Second, we sought to include an industrialized European country in our sample to render our results more generalizable. The questionnaire was translated into Italian and then back-translated [51].

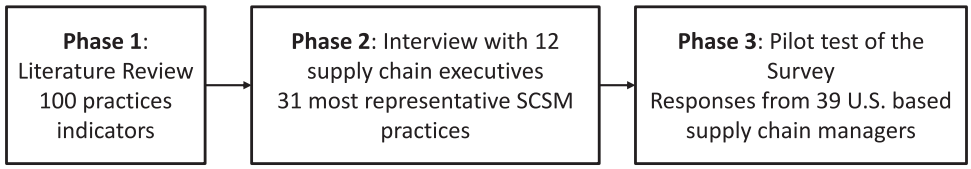


Fig. 1. Multiphased methodology of deriving indicators.

A group of supply chain managers from three large Italian firms were intimately involved to increase clarity and avoid misinterpretations.

Having realized the sensitivity of the topic and its potential adverse effect on response rate [20], we did not limit our target pool of firms to any specific manufacturing related SIC code. Given the wide representation we observed at practitioner meetings specific to SCS, we conjecture that manufacturing firms across industries would face SCS challenges and would realize some pressure to adopt SCSM practices. We targeted high- and middle-level supply chain executives, because they typically have sound knowledge of operations related to SCSM practices as well as SCS performance. Thus, we pursued respondents who hold at least a managerial (or equivalent) designation, work in the manufacturing sector, and work in areas which are directly related to supply chain management and security. A panel of 1855 potential respondents who are Council of Supply Chain Management Professionals (CSCMP) members was identified by relying on our selection criteria. The authors made advanced personalized phone calls to explain the purpose of the study and encourage participation. Although we attempted to reach all targeted respondents by phone multiple times (where information was available), we were not able to communicate with all of them for a variety of reasons such as participants being absent or could not get through "gate keepers." About 400 respondents were contacted via phone and we believe that this played a significant role in obtaining responses to the survey. The list of potential respondents from Italy was obtained from Associazione Italiana Acquisti e Supply Management, the Italian association of supply chain managers. Using the same criteria for targeting respondents, we identified 1125 potential participants. Two spaced reminders (two weeks apart) were sent after the survey was launched. All participants read a statement providing the context of the study and an explanation for their selection as participants.

The data collection process yielded 229 usable responses from the U.S. $(229/1855 = 12.3\%)$ and 233 usable responses from Italy $(233/1125 = 20.7\%)$ with an overall response rate of 15.5% (462/2980). The response rate compares favorably with other survey-based studies in the overly sensitive domain of SCS (e.g., [20], [52]). Table II reports the sample characteristics. The typical designation of the respondents includes President or VP Manufacturing or SCM Director/Manager or Managers with similar designations. About 40% of the respondents held positions at the Director level or above. In fact, 14% of respondents were Vice Presidents or held a "C" level designation. A majority of participating firms (85%) have annual sales of over $10 million while 39% have annual sales of over $1 billion.

TABLE II
SAMPLE CHARACTERISTICS

Number of employees		Frequency	Percentage
Less than 100		65	17%
100 to 499		100	26%
500 to 999		35	9%
1000 to 9999		84	22%
Over 10 000		100	26%
	Total	384	100%
Annual sales			
Less than 10 million		59	15%
10 to 99.9 million		84	22%
100 to 999.9 million		92	24%
1 to 10 billion		88	23%
More than 10 billion		61	16%
	Total	384	100%
Position			
President/Chairman		16	4%
CEO/COO/VP		38	10%
Director		100	26%
Managers		211	55%
Others		19	5%
	Total	384	100%
Country			
U.S.A		182 (229)	47% (49%)
Italy		202 (233)	53% (51%)
	Total	384 (462)	100%

Number in parentheses includes firms who did not provide profile information.

B. Variables and Survey Instrument

1) Identification of Representative SCSM Practices and Allocation Into Classes: As noted earlier, the identification of representative SCSM practices and the assignment of these practices reported here emerged out of a multistage research project. In stage one, we undertook a detailed review of the academic and practitioner literature and devised a list of 100 representative indicators. The literature we reviewed included academic studies (e.g., [12], [19], [33], [52]), practitioner-company reports (e.g., the IBM special report series for SCS), and a number of SCS programs developed by either governments or international organizations (e.g., AEO, ISO 28000, etc.). We also had day-long in-person interviews with practitioners at three Fortune 500 corporations. The purpose of the interviews was to assure that the domain of variables is adequately covered without leading the participants toward a specific set of practices. In stage two, we interviewed a number of supply chain executives who are subject matter experts (i.e., qualitative validation) to identify the most representative and currently implemented SCSM practices. These executives represented several industries: Food, high tech

TABLE III
SAMPLED COMPANIES FOR INTERVIEWS

Company	Industry	Interviewee	Size	Ownership	Major Business
Master Baker	Food & Beverage	General Manager & Quality Assurance/Compliance Manager	Small	Private	Produces bakery items for over 2500 fast food outlets
Seal Maker	Discrete Part Manufacturing	Plant Manager	Medium	Public	Division of a large corporation—Manufactures remote seals for the oil and gas industry
Electronics Savvy	Electronics/IT	Global Supply Chain Security Manager	Very Large	Public	Very large firm—Manufactures primarily consumer electronic products
Retail Guru	Retailing	A group of eight managers/directors from security, procurement, logistics, & compliance	Large	Private	Large Retailer—Sells national brand and private label products to consumers

TABLE IV
KEY SCSM PRACTICES IMPLEMENTED BY PARTICIPANT FIRMS

Key SCS Practices	Implemented by	Overlap with Literature
Develops a proactive strategy to deal with SCS breaches	M,E,R	Q3
Holds suppliers accountable for SCS breaches	M,S,E,R	Q4
Educates employees/suppliers about SCS breaches	M,S,E,R	Q6
Selects only qualified suppliers	M,S,E,R	Q5
Secures physical locations (e.g., manufacturing facilities and warehouses)	M,S,E,R	Q1, Q9
Sets high priority for SCS	M,S,E,R	Q2
Monitors physical movement of raw materials and products	M,S,E,R	Q8–Q10
Detects existing SCS breaches and near SCS breaches	M,S,E,R	Q7, Q11
Synthesizes information regarding SCS breaches	M,S,E,R	Q11
Monitors supply network instead of focusing only on first tier suppliers	M,S,E,R	Q13
Conducts periodic reviews both internally and externally about SCS	M,S,E,R	Q12
Notifies supply chain partners about SCS breaches	M,S,E,R	Q16
Cross-trains employees	M, E,R	Q24
Builds backup processes	M,S,E,R	Q19, Q25
Designates a group of employees as the first respondents to SCS breaches	M,S,E,R	Q14–Q17, Q20
Develops flexible contracts with suppliers	M,S,E,R	Q27
Develops a clear chain of command	M,S,E,R	Q17–Q18
Establishes effective communication channels with both suppliers and internal security staff	M,S,E,R	Q17–Q18
Utilizes product design to react to SCS breaches	M, E,R	Q26, Q28–Q29, Q31,
Develops recovery plans	M,S,E,R	Q21–Q23
Develops alternative material sources	M,S,E,R	Q27, Q30

M: Master Baker; S: Seal Maker; E: Electronics Savvy; R: Retail Guru; Practice indicators (last column) are provided in Table VII.

and consumer electronics, traditional discrete part manufacturing, and grocery/retailing. The food and grocery/retailing industries may be quite sensitive to SCS breaches because their products (if adulterated for instance) can directly impact public health. Firms classified as High-tech and consumer electronics epitomize an industry which has been targeted by a variety of threats such as theft and counterfeit products. Discrete part manufacturing firms represent the manufacturing sector at large and also endure a variety of threats such as theft, sabotage, counterfeit products, smuggling of drugs or people, etc. The selection was meant to go beyond the analysis of "low hanging fruit" (i.e., something that everyone does; [53]) and acknowledge that firms with different traits are more or less interested in securing their supply chains. This blend of firms also creates a more representative sample from which findings can be generalized. Table III displays the profiles of the firms. We probed our interviewees to describe specific SCSM practices their firm has implemented; we did not share with them the set of measures we assembled earlier. This would engender a more cogent triangulation process which allowed us to identify representative SCSM practices actually implemented by firms and match the practices that the interviewees described with SCSM indicators we assembled earlier. We uncovered that managers discuss security management programs rather than individual practices. For example, most SCSM practices implemented at Master Baker (see Table III) were embedded in a corporate-level program coined as the global food security initiative. We thus encouraged the interviewees to discuss with us the details of the programs they adopted. In addition, whenever we gathered that a practice was implemented by a firm but the manager(s) never explicitly mentioned it, we asked for a clarification. Typical responses were: "Yes, we did it. It (the practice) is part of our X program." or "We did not do the same thing, but it is very similar to our X." Furthermore, the same practice might be labeled differently. For instance, both "we only use pre-approved suppliers" and "we only use qualified suppliers" are referring to the same elemental activity regarding supplier selection. We extracted the information from the interviews, accumulated the representative SCSM practices in general terms, and mapped the common practices these firms have embraced to the practices we identified earlier. Some measures, however, were subsequently removed from the list due to duplication and conceptual overlap (as the supplier

TABLE V
GENERAL CHARACTERISTICS OF THE FOUR CLASSES OF SCSM PRACTICES

	Characteristics	Typical example	Implications
Prevention	Before an SCS breach	Select only qualified suppliers Educate suppliers about SCS Develop a proactive strategy to deal with SCS breaches Secure containers	Cost efficient Requires managerial efforts to set SCS as a high priority
Detection	Before or sometimes during an SCS breach	Monitors physical movement of raw materials and products Synthesizes information regarding SCS breaches Monitors supply network instead of focusing only on first tier suppliers	Acts as an alert system Improves SC visibility May prompt prevention, reaction, & mitigation
Response	During or after an SCS breach	Uses a group of employees as the first respondents to SCS breaches Uses a clear chain of command Uses a quick reaction force Engages in recovery efforts	Needs to be fast and effective, to contain damages; Provides first-aid Develops contingency plans if an SCS breach cannot be effectively eliminated
Mitigation	Before an SCS breach	Cross-trains employees Develops alternative material sources Reconsiders supply chain design & focuses on flexibility Maintains redundancy (e.g., strategic inventory of materials, machinery, etc.)	Preplanned Has the potential to reinforce response practices

selection example demonstrated) or relevancy (e.g., inspection of imported goods at U.S. ports is carried out by government entities rather than firms and thus such activities cannot be classified as firm practices). We ultimately retained 31 indicators. The last column of Table IV suggests that the practices identified via our earlier work are materially the same practices implemented at the four firms of our inquiry, but the literature and our earlier work describes them with more granularity (see Table VII).

We also presented our findings by invitation at two transported asset protection association meetings and sought feedback from the practitioners, who are mostly corporate-level directors of SCS at major corporations. We elicited feedback regarding the conceptual and practical integrity of our classification. We also sought to understand whether a classification based on intent (our approach) is more conducive than a classification based on type as we discussed earlier through the example of operationalizing supply base management. The consensus was that a classification based on intent resonates with the subject matter experts more forcefully. They stated that if a firm was to address a specific area, it would be advantageous to know all the tactics at its disposal.

In stage three, we pilot-tested the survey using data from 39 U.S. based supply chain managers who are members of the CSCMP. 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 latent variables were operationalized via multi-item scales. Table V describes the characteristics of the four classes of practices.

Apart from the measures of SCSM practices, we also relied on the literature and our interviews to derive indicators of SCS performance [54]. Seven items were included in order to embody the different nuances of SCS discussed in prior studies [28], [29].

C. Research Methodology and Results

1) Nonresponse Bias and Common Method Bias: We assessed nonresponse bias by comparing firm characteristics of early respondents and late respondents via an ANOVA procedure [55], [56]. The results suggest that there was no statistical difference in terms of market share ($p = .17$) and annual sales ($p = .38$). We addressed common method bias (CMB) through both procedural and statistical approaches [57]. We used the following procedural remedies: we assured respondent anonymity, reduced item ambiguity via interviews and the pilot study, and dispersed the indicators of a given theoretical latent variable so we can avoid "yeah saying" responses. Next, we employed a confirmatory factor analysis (CFA) marker technique to assess CMB. Richardson *et al.* [58] suggest that a CFA marker methodology is advantageous compared to other methods because it can account for random error in the marker and other latent constructs and it models common method variance (CMV) at the item level; thus, it accounts for noncongeneric and congeneric CMV. The latent marker variable we selected measures shipment accuracy and it includes three indicators. In the past three years, our firm has experienced an improvement in shipment data accuracy, fewer shipments with the wrong quantity, and fewer shipments with the wrong parts. Theoretically, this measure of shipment performance should have relatively little relation with the SCS focused variables we deploy in our study. The shared variance between the marker construct and the theoretical constructs of interest that is believed to be a function of CMV is captured by specifying paths between the latent marker variable and each of its own unique indicators as well as the indicators of the theoretical constructs of interest [58]. Comparing the change in model fit between a model where all marker variable indicators are freely estimated to one where only the marker variable's own indicators are freely estimated but the indicators of theoretical constructs are constrained to zero is posited as a test for detecting CMV. The χ^2 difference $(1695.08 - 1665.47 = 29.61 < 47.40)$ is not statistically significant with 33 (753–720) degrees of freedom (df) at the $\alpha = .05$ level, suggesting that CMV is not salient.

2) Measurement Model: Before we tested for the substantive hypotheses, we evaluated the measurement model. First, we specified a measurement model and assessed model fit, convergent and discriminant validity, and reliability. The measurement model produced acceptable model fit indices: $\chi^2(644) = 1384.81$, $\chi^2/\text{df} = 2.15$, RMSEA $= .05$, 90% CI for RM-

TABLE VI
MEAN, STANDARD DEVIATIONS, AND CORRELATIONS OF THE NONCATEGORICAL VARIABLES

	Mean (SD)	1	2	3	4	5	6	7
1. Annual sales	3.02 (1.31)							
2. No. of employees	3.14 (1.49)	.85**						
3. Profit margin	3.08 (.87)	.27**	.24**					
4. Prevention	4.14 (1.29)	.25**	.29**	.12				
5. Detection	4.14 (1.35)	.25**	.28**	.11	.89**			
6. Response	4.41 (1.33)	.33**	.32**	.14	.84**	.82**		
7. Mitigation	4.30 (1.10)	.18**	.20**	.21**	.79**	.81**	.88**	
8. SCS performance	4.16 (1.20)	.22*	.23**	.19*	.59**	.61**	.57**	.57**

SEA (.046, .053), CFI = .93, TLI = .92, SRMR = .05. All standardized item-factor coefficients were substantive (only two items had coefficients below .60) and significant at the .001 level, suggesting convergent validity. To address discriminant validity, we also conducted a χ^2 difference test for all pairs of constructs included in this study. Each pair-wise χ^2 difference was greater than 3.84 (i.e., significant at .05), providing evidence of discriminant validity. Composite reliabilities (CR) ranged from .88 to .94 and average variance extracted (AVE) ranged from .51 to .62. In summary, there is sufficient evidence demonstrating construct validity and construct reliability. Table VI reports the means, standard deviations, and correlations for the noncategorical variables. Table VII depicts the items with their respective standardized coefficients, CRs, and AVEs.

Since data were collected from two different locations, we tested for measurement invariance following the procedures recommended by Koufteros and Marcoulides [59]. The results suggest that the two data sets can be combined as there were no significant differences across the two respective measurement models in terms of number of latent variables, factor loadings, intercepts, and error variance (see online Appendix A).

To test H_1, we included all four practices in the model in order not to avoid bias that can emerge due to omitted variables. Given that the four practices are all aimed at enhancing SCS performance and are usually deployed concurrently as part of a program such as ISO 28000, multicollinearity cannot be ignored. Both the Farrar–Glauber multicollinearity test and the variance inflation factor (VIF) suggested that some level of multicollinearity may be present. The highest VIF was 5.13 for detection. However, because multicollinearity only inflates the standard errors and the estimates are unbiased, it does not reduce the predictive power or reliability of the model as a whole [60]. Thus, some suggest that a VIF score less than 10 should not be a concern as long as the effect is significant. Nonetheless, we decided to use iterative generalized ridge regression to address multicollinearity. Ridge regression reduces the standard errors by adding a degree of "bias" to the estimates.

To test H_2 and H_3, we first compared the effects of each pair of practices at a time on SCS performance via a regression model specified as $Y = \beta_0 + \beta_1 \mathrm{IV}_1 + \beta_2 \mathrm{IV}_2 + \beta_i \mathrm{Control}_i$ [61] (the list of control variables is provided at the end of this subsection). The test in essence examines whether the coefficients relating the independent variables and the dependent variable differ statistically ($\mathrm{H}_0 : \beta_1 = \beta_2$, $\mathrm{H}_1 : \beta_1 \neq \beta_2$). First, SCS performance (DV) was regressed on two IVs (IV_1 and IV_2) at a time. The standard errors of the two β (i.e., SE_1 and SE_2) and the covariance of the two β (i.e., COV_{12}) were then attained. Second, the joined standard error of β_1 and β_2, SE_{12}, was calculated. Third, since $\frac{\beta_1 - \beta_2}{\mathrm{SE}_{12}}$ follows a t distribution with $(n - k - 1)$ df, the value of the t-statistic, $\frac{\beta_1 - \beta_2}{\mathrm{SE}_{12}}$, was calculated and probed for its significance. Because the respective df exceeds 120, a t-statistic value of 1.96 or above suggests a difference between β_1 and β_2 (at $\alpha = .05$ level). Since our hypotheses are one-sided rather than two-sided, we divided the p-value by two[1] and the corresponding cutoff t value becomes 1.65. We performed the comparison between all pairs of practices which allows ranking the practices based on their impact on SCS performance.

To test H_{4a}, we adopted a test approach articulated by Venkatraman [62]. Essentially, Venkatraman [62] suggested that the complementarity of a set of first-order factors can be probed via a second-order latent factor specification. If a second-order latent factor can effectively represent the first-order latent variables (via a nested model approach, see [59]), then there is statistical evidence demonstrating complementarity. The process begins by specifying one first-order factor (Model 1), followed by four first-order uncorrelated factors (Model 2), four first-order correlated factors (Model 3), and finally four first-order factors-one 2nd order factor (Model 4). To support complementarity, the fit indices are compared across Models 3 and 4 to determine if they differ statistically. If the model fit of the complementarity model (Model 4) is not significantly different from the first-order correlated model (Model 3), then complementarity can be inferred [62]. Furthermore, if the coefficients relating the first-order latent factors with the 2nd order latent factor are sizable and significant, then there is additional evidence demonstrating complementarity. To test H_{4b}, we linked the higher-order factor to SCS performance in a structural equation model and probed its path coefficient for significance.

A number of control variables were included in all models described above. We included several control variables describing firm characteristics: size (i.e., annual sales; large firms are generally more visible and thus perhaps more sensitive to their reputation, leading them to invest more heavily to protect their

[1]We thank one of the reviewers for pointing this out.

TABLE VII
FACTOR LOADINGS, CRONBACH'S α, AVES, AND CRS FOR PRACTICE AND PERFORMANCE FACTORS

Factor and Indicators	Std. Coefficient
Prevention: $\boldsymbol{\alpha} = .\mathbf{9}0,\ CR = .\mathbf{9}0,\ AVE = .\mathbf{5}8$	
Q1 We secure containers at our facilities to assure they are not compromised	.688
Q2 Our supply chain risk management strategy can be characterized as proactive	.851
Q3 When it comes to supply chain security, our strategy focuses on prevention	.852
Q4 We hold all suppliers accountable for supply chain security	.801
Q5 We only approve suppliers (irrespective of tier) that have a risk management program in place	.676
Q6 We educate suppliers about supply chain security practices	.710
Q7 We have a process that notifies supply chain partners across tiers if the supply chain is threatened	.715
Detection: $\boldsymbol{\alpha} = .\mathbf{8}9,\ CR = .\mathbf{9}0,\ AVE = .\mathbf{6}0$	
Q8 We use active measures such as video and sensors to be able to detect security breaches	.638
Q9 We monitor the loading/unloading process of cargo to identify potential security breaches	.786
Q10 We use sophisticated technologies to detect if containers have been compromised	.694
Q11 We monitor and synthesize information regarding security breaches	.820
Q12 We do conduct periodic assessments of our supply chain security	.862
Q13 We have procedures to detect supply chain security failures or near failures	.810
Response: $\boldsymbol{\alpha} = .\mathbf{9}5,\ CR = .\mathbf{9}4,\ AVE = .\mathbf{6}2$	
Q14 We know what to do when we encounter supply chain security breaches or crises	.779
Q15 We have designated a group of employees as first respondents in case of a crisis	.847
Q16 There is effective communication across our supply chain when a crisis hits	.729
Q17 There is a definite chain of command in case of an emergency	.830
Q18 We have protocols for communication when a crisis arises	.764
Q19 We have a well-defined contingency plan to react to serious supply chain security breaches	.777
Q20 We have a quick reaction force to deal with a crisis or a serious disruption in our supply chain	.856
Q21 We do have a disaster recovery plan	.751
Q22 We have a specific process to reinstate operations in case of a major crisis/disruption	.761
Q23 We have strategies for recovery action after supply chain disruptions	.799
Mitigation: $\boldsymbol{\alpha} = .\mathbf{8}6,\ CR = .\mathbf{8}8,\ AVE = .\mathbf{5}1$	
Q24 We cross-train our employees as a mechanism to deal with potential supply chain disruptions	.798
Q25 We have backup processes that can assist us at times of crises	.818
Q26 We have strategies to use more standard parts to reduce the risk of supply chain disruptions	.670
Q27 We developed alternative material sources in case of supply chain disruptions	.804
Q28 We have strategies to simplify product design as part of our risk management strategy	.656
Q29 In order to reduce supply chain risk we design products where suppliers can easily be replaced	.510
Q30 We established alternative carrier arrangements for use in case of supply chain disruptions	.693
Q31 We simplified jobs to the extent that unskilled labor can perform a variety of them in case of a crisis	.624
SCS Performance: $\boldsymbol{\alpha} = .\mathbf{8}9,\ CR = .\mathbf{9}0,\ AVE = .\mathbf{5}6$	
A reduction/less potential for theft/loss	.731
An improved capability to detect counterfeit parts/products	.790
A lower probability that our supply chain will be compromised	.785
A lower probability of cargo misuse	.662
Lower levels of supply chain vulnerability	.704
An improvement in security	.799
A reduction/less potential for smuggling of drugs	.769

Model fit: $Q^2(644) = 1384.81$, $Q^2/\mathrm{df} = 2.15$, $\mathrm{RMSEA} = .05$, 90% CI for RMSEA (.046, .053), $\mathrm{CFI} = .93$, $\mathrm{TLI} = .92$, $\mathrm{SRMR} = .05$.

supply chains), number of employees (as a measure of complexity to deploy SCS practices and attain requisite commitment), and profit margin (relative to rivals; firms with high profit margin may have more resources to apportion toward SCS practices and reap better performance). We also controlled for industry effects as some industries may be more sensitiveto SCS breaches; for instance, the food industry may be more vigilant because their products are consumed by humans and thus SCS breaches are laden with more health risks. Based on the SIC code provided by the respondents, we created categorical variables to represent six sectors: food and beverage (9.9%), chemical and pharmaceutical (14.6%), auto (6.0%), electronics (7.8%), commercial machinery and controlling instruments (41.7%), and others (20.1%).

D. Hypotheses Testing Results

H_{1a-d} hypothesize that the SCSM practices are positively related to SCS performance. The results suggest that except for mitigation ($\beta = -.05$, $p-\mathrm{value} = .522$), all others are positively associated with SCS performance (detection $\beta = .28$, $p-\mathrm{value} = .005$; prevention $\beta = .23$, $p-\mathrm{value} = .015$; response $\beta = .20$, $p-\mathrm{value} = .050$). The results (see Table VIII) imply that mitigation has a marginal impact when the other three types of practices are present.

H_{2a-c} and H_{3a-b} collectively propose that detection and prevention are the most and second most potent SCSM practices, respectively. The results (see Table IX) demonstrate that the effect of prevention is weaker than detection ($t = -2.38$, $p-\mathrm{value} = .02$), prevention is indifferent from response ($t =$

TABLE VIII
RIDGE REGRESSION RESULTS

DV SCS Performance	*B*	Std. Err.	*t*-value	*p*-value		
Constant	**4.24**	.44	9.54	.000	Wald test = 85.22	$p-\text{value} > Chi^2\,(9) = .000$
Annual sales	.13	.15	.90	.368	*F*-test = 9.47	$p-\text{value} > F\,(9,\,452) = .000$
No. of employees	.03	.05	.66	.510	R^2h = .4016	$p-\text{value} > F\,(9,\,452) = .000$
Profit margin	**.17**	.07	2.50	.013	R^2h Adj. = .3592	$p-\text{value} > F\,(9,\,452) = .000$
SIC code	–.01	.04	–.28	.782	Ridge *k* value = .32	
Region dummy	–.18	.15	–1.23	.220	Significant coefficients are bold	
Prevention	**.23**	.10	2.44	.015		
Detection	**.28**	.10	2.86	.005		
Response	**.20**	.10	1.96	.050		
Mitigation	–.06	.09	–.64	.522		

TABLE IX
DIFFERENTIAL EFFECT TEST RESULTS

DV: SCS Performance	β_1	β_2	SE_1	SE_2	COV_{12}	SE_{12}	*t*-statistic	*p*-value
Prevention (β_1) *vs.* Detection (β_2)	.10	.59	.05	.05	–.02	.21	**–2.38**	**.02**
Prevention *vs.* Response	.40	.17	.11	.11	–.02	.25	.91	.36
Prevention *vs.* Mitigation	.35	.24	.06	.06	–.01	.88	.13	.89
Detection *vs.* Response	.57	.02	.13	.12	–.02	.25	**2.21**	**.03**
Detection *vs.* Mitigation	.53	.06	.07	.10	–.02	.22	**2.17**	**.03**
Response *vs.* Mitigation	.27	.28	.11	.12	–.02	.27	–.05	.96

Control variables included; a *t*-value of 1.65 is statistically significant in a one-sided test when $n > 200$.

.91, $p-\text{value} = .36$), prevention is indifferent from mitigation ($t = .13$, $p-\text{value} = .89$), detection is more efficacious than response ($t = 2.21$, $p-\text{value} = .03$), detection is more efficacious than mitigation ($t = 2.17$, $p-\text{value} = .03$), and response is indifferent from mitigation ($t = -.05$, $p-\text{value} = .96$).

The results suggest that detection practices are the most efficacious when SCS performance is concerned, which is not surprising. Please note β of prevention is greater than that of response and mitigation in the ridge regression when testing H_1. We suspect that prevention may have a stronger impact than mitigation and response but such conclusion is not statistically supported by our data.

H_4 postulates that there is complementarity between the four classes of SCS practices (H_{4a}) and such synergy should be positively associated with SCS performance (H_{4b}). Our analysis (see Table X) demonstrated that the 2nd order latent factor (Model 4) exhibits almost identical model fit ($\Delta\chi^2 = 3.74$, $\text{df} = 2, p > .05$) compared to the correlated first-order latent model (Model 3), supporting complementarity. The coefficients relating first-order latent variables to the second-order latent variable are all high in magnitude and statistically significant at the .001 level, further supporting the co-alignment of the four variables. Furthermore, the target coefficient [62] is .995, which renders additional support for hypothesis H_{4a}. The higher-order latent variable underlying the first-order latent variables was strongly associated with SCS performance [$\chi^2\,(766) = 1333.73$, $\chi^2/\text{df} = 1.74$, RMSEA = .05, $90\%\,CI$ for RMSEA (.048, .058), CFI = .91, TLI = .90, SRMR = .07; $\beta_{\text{higherorder}} = .592$, $p-\text{value} = .000$]. The results provide support for H_{4b}, suggesting that complementarity substantively enhances SCS performance.

E. Robustness

We performed robustness tests in order to triangulate our findings. First, we retested H_1 by including only one practice at a time (the same set of control variables are included). We find each of them to be positively associated with SCS performance. These results along with our earlier results collectively suggest that those firms that implement the practices do reap the benefits in the form of higher SCS performance. However, their efficacy in explaining SCS performance variance differs. Second, we use an alternative approach (i.e., via interactions) to assess complementarity (i.e., H_{4a}). Considering that the model includes four variables, there are six two-way interactions, four three-way interactions, and one four-way interaction; the number and nature of interactions legitimately raise multicollinearity concerns. We thus deployed a ridge regression approach. The results demonstrate that the four-way interaction is positive and significant ($\beta = .185$, $p = .014$), furnishing additional evidence for complementarity.

Third, in order to examine the legitimate concern whether efforts in SCS can have adverse effects on cost, we correlated a composite measure of cost [i.e., in the last three years we have experienced: 1) a reduction in overall cost, 2) a reduction in excess inventory, 3) a reduction in insurance premiums, and 4) reduced costs associated with supply chain disruptions] with the practices and performance variables. The correlations were all positive and highly significant: detection ($r = .42$, $p < .001$), prevention ($r = .44$, $p < .001$), response ($r = .48$, $p < .001$), mitigation ($r = .51$, $p < .001$), 2nd order practice variable ($r = .54$, $p < .001$), and SCS performance ($r = .64$, $p < .001$). These positive correlations suggest that investments in SCS do not necessarily have adverse

TABLE X
ALTERNATIVE MEASUREMENT MODEL STRUCTURES

	Model 1 One first-order factor	Model 2 Four uncorrelated first-order factors	Model 3 Four correlated first-order factors	Model 4 Four first-order factors and one second-order factor
Factor loadings				
Prevention				**1.002 (.007)**
Detection				**.978 (.009)**
Response				**.942 (.010)**
Mitigation				**.921 (.013)**
Q1	**.690 (.031)**	**.703 (.032)**	**.699 (.030)**	**.707 (.029)**
Q2	**.845 (.015)**	**.848 (.018)**	**.859 (.014)**	**.860 (.014)**
Q3	**.774 (.020)**	**.781 (.023)**	**.792 (.020)**	**.789 (.020)**
Q4	**.704 (.025)**	**.728 (.026)**	**.704 (.026)**	**.705 (.026)**
Q5	**.681 (.027)**	**.693 (.029)**	**.688 (.027)**	**.680 (.027)**
Q6	**.714 (.024)**	**.724 (.027)**	**.718 (.025)**	**.711 (.025)**
Q7	**.781 (.020)**	**.779 (.023)**	**.789 (.020)**	**.788 (.020)**
Q8	**.657 (.033)**	**.595 (.041)**	**.647 (.035)**	**.653 (.034)**
Q9	**.742 (.026)**	**.745 (.030)**	**.764 (.025)**	**.761 (.025)**
Q10	**.692 (.030)**	**.656 (.042)**	**.703 (.032)**	**.703 (.032)**
Q11	**.788 (.022)**	**.792 (.027)**	**.809 (.021)**	**.810 (.021)**
Q12	**.825 (.019)**	**.883 (.020)**	**.870 (.016)**	**.866 (.017)**
Q13	**.773 (.021)**	**.795 (.026)**	**.810 (.019)**	**.809 (.019)**
Q14	**.837 (.018)**	**.838 (.019)**	**.849 (.017)**	**.847 (.017)**
Q15	**.720 (.028)**	**.741 (.027)**	**.741 (.027)**	**.745 (.027)**
Q16	**.813 (.020)**	**.837 (.019)**	**.839 (.018)**	**.837 (.018)**
Q17	**.742 (.026)**	**.783 (.023)**	**.774 (.023)**	**.769 (.024)**
Q18	**.771 (.024)**	**.762 (.026)**	**.779 (.024)**	**.783 (.023)**
Q19	**.866 (.015)**	**.818 (.021)**	**.845 (.017)**	**.852 (.017)**
Q20	**.735 (.027)**	**.723 (.029)**	**.743 (.026)**	**.746 (.026)**
Q21	**.803 (.021)**	**.817 (.021)**	**.820 (.020)**	**.824 (.019)**
Q22	**.805 (.021)**	**.828 (.020)**	**.829 (.019)**	**.832 (.019)**
Q23	**.784 (.020)**	**.794 (.022)**	**.806 (.019)**	**.812 (.018)**
Q24	**.764 (.022)**	**.787 (.027)**	**.796 (.022)**	**.799 (.022)**
Q25	**.782 (.021)**	**.851 (.026)**	**.846 (.020)**	**.839 (.020)**
Q26	**.629 (.031)**	**.658 (.032)**	**.659 (.030)**	**.653 (.030)**
Q27	**.697 (.038)**	**.669 (.044)**	**.814 (.037)**	**.807 (.038)**
Q28	**.708 (.027)**	**.735 (.032)**	**.637 (.025)**	**.640 (.025)**
Q29	**.533 (.038)**	**.596 (.036)**	**.581 (.036)**	**.585 (.035)**
Q30	**.611 (.033)**	**.642 (.034)**	**.648 (.031)**	**.647 (.032)**
Q31	**.584 (.035)**	**.601 (.038)**	**.687 (.034)**	**.689 (.034)**
Model fit				
χ^2 (df)	1581.66 (434)	2617.59 (411)	895.83 (405)	899.57 (407)
χ^2/df	3.64	6.37	2.19	2.21
CFI	.86	.73	.94	.94
TLI	.85	.69	.93	.92
RMSEA	.08	.11	.05	.05
SRMR	.05	.43	.04	.04

Note: Std. errors are in parenthesis and significance is indicated in bold. Indicator details are reported in Table VII.

effects on cost. In fact, the effects appear to be beneficial. These correlations can curb some of the suspicions held by sceptics who doubt the utility of investing in SCS. It is also notable that response and mitigation have higher correlations with reduction in cost than detection and prevention. We have to, however, consider that the effects of detection and prevention may not be fully accounted as many breaches can be averted and the respective cost is not typically traceable.

IV. DISCUSSION, MANAGERIAL IMPLICATIONS, AND LIMITATIONS

A. Contributions

Cicero once called security an "object of supreme desire" [14]. Individuals, organizations, supply chains, and nations alike would like to be in a state of security, free from breaches which often cause havoc. Thus, significant effort and capital resources have been expended toward programs and practices that can engender security. Our first contribution pertains to the classification of SCSM practices into four classes and particularly the development of indicators that reflect each category. Since SCS represents a special case of risk, we relied on the conceptual development advanced by the risk management literature at large but also on contributions specific to SCS. The academic and practitioner literatures have promoted a plethora of practices but we synthesized those practices parsimoniously into a manageable size. A close examination of the literature (see Table I) suggests significant overlap, although the terminology is not always consistent. In essence, some practices are more salient before a breach occurs while other practices assume more prominence during and after a breach is detected. Some practices are more attuned to thwarting breaches while other practices are

more suitable to combating breaches. It is also noteworthy that the studies cited in Table I are primarily conceptual and thus this paper contributes by operationalizing each class of practices and subsequently examining their comparative efficacy to explain SCS. From a managerial perspective, the classification can be utilized to ascertain whether the firm has any gaps in reference to the classification of practices and thus address those that might be deficient. Executives can also benchmark against their peers by class of practice. The results would allow them to identify gaps, leading to the development of SCS plans that move their firm into a more competitive position.

Our extensive discussions with high-level executives revealed that they are concerned with choosing germane practices that would generate the best returns. They noted that they would like to fill specific gaps in their security but there is only anecdotal evidence to guide them. Our literature review attests that there is very little in the form of large empirical studies that can offer guidance. As noted earlier, there are significant challenges in collecting data that pertains to SCS and only through a lengthy and painstaking effort we were able to obtain a sizable number of responses across two continents that allow us to study the relative efficacy of each practice to explain performance. In this sense, our results are more generalizable. Our second contribution relates to probing the relative efficacy of each class of practices to explain variability in SCS performance. There was unequivocal evidence suggesting that detection practices are the supreme choice. From a managerial perspective, investing in detection appears to be paramount. Threats that can be detected can be stopped, slowed, or weakened as the firm can orchestrate defenses to fend them off. Without an ability to detect threats and impending breaches, firms may have to invest more to battle breaches that surface without warning.

B. Managerial Implications

Kleindorfer and Saad [11] advanced a compelling argument regarding complementarity; though they did not explicitly articulate complementarity amongst practices they alluded to complementarity amongst their ten principles. They suggested that for optimal performance, firms need to consider and implement the principles holistically. The implementation necessarily involves practices however. We examined whether the complementarity effect of practices on SCS performance is potent when they are viewed collectively or individually. We found sufficient evidence to support the complementarity hypothesis. Firms that implement the practices concurrently do have higher SCS performance. From a managerial perspective, firms are advised to adopt a more systematic implementation where the firm invests in all practices concurrently instead of individual practices. It is, however, a challenge to convince top management to invest in SCSM practices in a systemic manner since many firms tend to "ignore high-impact, low likelihood risks" [10, p. 54]. In fact, there have been some sceptics whether SCSM practices can improve security [40]. The sceptics cite the high cost of implementation and also argue that these efforts "might not guarantee security in the long run because the actual security would depend on the continuous efforts of many parties" [40, p. 35]. Also, the lack of data and accurate estimates of the probability of an SCS event, coupled with unreliable appraisals of the potential impact of each breach [40], would make decisions to invest in SCSM suspect from a financial perspective. Furthermore, it is difficult to give credit for SCS breaches that were averted [63]. Nonetheless, one of our robustness tests reveals that SCSM is positively associated with cost reduction. Furthermore, only few firms rely on insurance to cover losses and disruptions [20] as the premiums to cover major events are high and insurance policies do not protect against losing customers [40]. Managers also have other choices at their disposal; for instance they can rely on redundancy or flexibility [38] or some aspects of SCS as forms of mitigation. Each comes with a different price tag and amount of effort. Coutu [64, p. 5] cites the words of Robert G. Scott (then president and COO of Morgan Stanley) regarding the mitigation practices of having three recovery sites available at the World Trade Center: "Multiple backup sites seemed like an incredible extravagance on September 10," "But on September 12, they seemed like genius". Investing in SCS might be a form of insurance.

C. Limitations and Future Research

The inquiry here suffers from several limitations. First, while the single-respondent approach was necessary to collect data on this sensitive topic, we caution for potential single-respondent bias. Related to the survey approach, the indicators we deployed to operationalize each construct are reflective of the particular class of practice; they are representative of nuances from the content domain of each class of practice. They are not meant to be exhaustive of all practices that a firm can undertake. Unfortunately, the length of our survey prohibited the deployment of more indicators. Second, all practices are aimed to improve security and thus have relatively high correlations. Although we use ridge regression to address this issue, one should be aware that multicollinearity may exist. Third, early on in the research study we attempted to collect objective data in terms of the number of security breaches and even "near misses." We also solicited responses for the number of incidences by category; i.e., minor, major, catastrophic. This proved to be a futile exercise as practitioners were not comfortable sharing with us such potentially meaningful data; upon further discussion with practicing executives we learnt that they do not want the public to know exactly how they perform as this may reflect negatively on the firm. They want to protect their brand and goodwill. Furthermore, firms do not always report all incidences to insurance companies as they are afraid that their insurance premiums will be adjusted upwards. Future research can attempt to solicit such information using alternative routes. We hope that our intimate involvement with a professional society can help us obtain such data in the future.

References

[1] L. M. Wein and Y. Liu, "Analyzing a bioterror attack on the food supply chain: The case of botulinum toxin in milk," *Proc. Natl. Acad. Sci. USA*, vol. 102, no. 28, pp. 9984–9989, 2005.

[2] Z. Williams, J. E. Lueg, and S. A. LeMay, "Supply chain security: An overview and research agenda," *Int. J. Log. Manage.*, vol. 19, no. 2, pp. 254–281, 2008.

[3] Y. Sheffi, "Supply chain management under the threat of international terrorism," *Int. J. Log. Manage.*, vol. 12, no. 2, pp. 1–11, 2001.

[4] INTERPOL, Global scale of food fraud highlighted in INTERPOL—Europol report, 2016. [Online]. Available: https://www.interpol.int/News-and-media/News/2016/N2016-139. Accessed on: Nov. 30, 2016.

[5] ABC News, Clues Sought in $75 million record-breaking drug heist. Reported by Y. Denies and L. Ferran, 2010. [Online]. Available: http://abcnews.go.com/GMA/TheLaw/75-million-drugs-stolen-dramatic-connecticut-heist/story?id=10133205#.T3x29tXy83E. Accessed on: Apr. 03, 2012.

[6] Mirror, Cocaine worth £1million found in box of bananas by stunned Tesco worker, 2015. [Online]. Available: http://www.mirror.co.uk/news/uk-news/cocaine-worth-1million-found-box-6144305. Accessed on: Nov. 4, 2016.

[7] Specification for security management systems for the supply chain, ISO 28000-2007, 2007. [Online]. Available: http://www.iso.org/iso/catalogue_detail?csnumber=44641

[8] C. Speier, J. M. Whipple, D. J. Closs, and M. D. Voss, "Global supply chain design considerations: Mitigating product safety and security risks," *J. Oper. Manage.*, vol. 29, pp. 721–736, 2011.

[9] T. J. Pettit, J. Fiskel, and K. L. Croxton, "Ensuring supply chain resilience: Development of a conceptual framework," *J. Bus. Log.*, vol. 31, no. 1, pp. 1–21, 2010.

[10] S. Chopra and M. S. Sodhi, "Managing risk to avoid supply-chain breakdown," *MIT Sloan Manage. Rev.*, vol. 46, no. 1, pp. 53–61, 2004.

[11] P. R. Kleindorfer and C. H. Saad, "Managing disruption risks in supply chains," *Prod. Oper. Manage.*, vol. 14, no. 1, pp. 53–68, 2005.

[12] H. L. Lee and S. Whang, "Higher supply chain security with lower cost: Lessons from total quality management," *Int. J. Prod. Econ.*, vol. 96, pp. 289–300, 2005.

[13] W. Ho, T. Zheng, H. Yildiz, and S. Talluri, "Supply chain risk management: A literature review," *Int. J. Prod. Res.*, vol. 53, pp. 5031–5069, 2015.

[14] E. Rothschild, "What is security?" *Daedalus, Quest World Order*, vol. 124, no. 3, pp. 53–98, 1995.

[15] R. J. Fischer and G. Green, *Introduction to Security*, 7th ed. Boston, MA, USA: Butterworth-Heinemann, 2004.

[16] G. Lu and X. Koufteros, "Adopting security practices for transport logistics: Institutional effects and performance drivers," *Int. J. Shipping Transp. Log.*, vol. 6, pp. 611–631, 2014.

[17] J. Z. Ni, S. A. Melnyk, W. J. Ritchie, and B. F. Flynn, "Why be first if it doesn't pay? The case of early adopters of C-TPAT supply chain security certification," *Int. J. Oper. Prod. Manage.*, vol. 36, no. 10, pp. 1161–1181, 2016.

[18] C. C. Yang and H. H. Wei, "The effect of supply chain security management on security performance in container shipping operations," *Supply Chain Manage.: Int. J.*, vol. 18, pp. 74–85, 2013.

[19] C. Markmann, I. Darkow, and H. von der Gracht, A "Delphi-based risk analysis—Identifying and assessing future challenges for supply chain security in a multi-stakeholder environment," *Technol. Forecast. Social Change*, vol. 80, no. 9, pp. 1815–1833, 2013.

[20] Z. Williams, J. E. Lueg, S. P. Goffnett, S. A. LeMay, and R. L. Cook, "Understanding supply chain security strategy," *J. Transp. Manage.*, vol. 23, pp. 7–25, 2012.

[21] I. Manuj and J. T. Mentzer, "Global supply chain risk management," *J. Bus. Log.*, vol. 29, no. 1, pp. 133–156, 2008.

[22] D. J. Closs and E. F. McGarrell, "Enhancing security throughout the supply chain," Special Report Series, IBM Center Bus. Gov., Washington, DC, USA, 2004. [Online]. Available: https://www-304.ibm.com

[23] R. Sarathy, "Security and the global supply chain," *Transp. J.*, vol. 45, no. 4, pp. 28–51, 2006.

[24] D. Ekwall, "The displacement effect in cargo theft," *Int. J. Phys. Distrib. Log. Manage.*, vol. 39, no. 1, pp. 47–62, 2009.

[25] J. B. Rice and F. Caniato, "Building a secure and resilient supply network," *Supply Chain Manage. Rev.*, vol. 7, no. 5, pp. 22–30, 2003.

[26] C. W. Autry and L. M. Bobbitt, "Supply chain security orientation: Conceptual development and a proposed framework," *Int. J. Log. Manage.*, vol. 19, no. 1, pp. 42–64, 2008.

[27] X. Gutierrez and J. Hintsa, "Voluntary supply chain security programs: A systematic comparison," in *Proc. Int. Conf. Inf. Syst. Log. Supply Chain*, Lyon, France, 2006, pp. 15–17.

[28] J. B. Rice and P. W. Spayd, "Investing in supply chain security: Collateral benefits," Special Report Series, IBM Center Bus. Gov., Washington, DC, USA, 2005. [Online]. Available: www.ibm.com

[29] B. Peleg-Gillai, G. Bhat, and L. Sept, "Innovators in supply chain security: Better security drives business value," Manuf. Inst., Washington, DC, USA, 2006. [Online]. Available: www.nam.org

[30] L. C. Giunipero and R. A. Eltantawy, "Securing the upstream supply chain: A risk management approach," *Int. J. Phys. Distrib. Log. Manage.*, vol. 34, no. 9, pp. 698–713, 2004.

[31] U. Jüttner, H. Peck, and M. Christopher, "Supply chain risk management: Outlining an agenda for future research," *Int. J. Log.: Res. Appl.*, vol. 6, pp. 197–210, 2003.

[32] A. M. Knemeyer, W. Zinn, and C. Eroglu, "Proactive planning for catastrophic events in supply chains," *J. Oper. Manage.*, vol. 27, pp. 141–153, 2009.

[33] Y. Sheffi, *The Resilient Enterprise: Overcoming Vulnerability for Competitive Advantage*. Cambridge, MA, USA: MIT Press, 2005.

[34] M. S. Sodhi, B. Son, and C. S. Tang, "Researchers' perspectives on supply chain risk management," *Prod. Oper. Manage.*, vol. 21, no. 4, pp. 1–13, 2011.

[35] M. K. Starr and L. N. Van Wassenhove, "Introduction to the special issue on humanitarian operations and crisis management," *Prod. Oper. Manage.*, vol. 23, no. 6, pp. 925–937, 2014.

[36] C. Blome and T. Schoenherr, "Supply chain risk management in financial crises—A multiple case-study approach," *Int. J. Prod. Econ.*, vol. 134, no. 1, pp. 43–57, 2011.

[37] D. Kern, "Supply risk management: Model development and empirical analysis," *Int. J. Phys. Distrib. Log. Manage.*, vol. 42, no. 1, pp. 60–82, 2012.

[38] Y. Sheffi, J. B. Rice, J. M. Fleck, and F. Caniato, "Supply chain response to global terrorism: A situation scan," in *Proc. 1st Eur. OMA-POMS Joint Int. Conf.*, Como, Italy, 2003, pp. 121–130.

[39] D. R. Towill, "The impact of business policy on bullwhip induced risk in supply chain management," *Int. J. Phys. Distrib. Log. Manage.*, vol. 35, pp. 555–575, 2005.

[40] C. Tang, "Robust strategies for mitigating supply chain disruptions," *Int. J. Log.: Res. Appl.*, vol. 9, no. 1, pp. 33–45, 2006.

[41] M. J. Braunscheidel and N. C. Suresh, "The organizational antecedents of a firm's supply chain agility for risk mitigation and response," *J. Oper. Manage.*, vol. 27, no. 2, pp. 119–140, 2009.

[42] B. Tomlin, "On the value of mitigation and contingency strategies for managing supply chain disruption risks," *Manage. Sci.*, vol. 52, no. 5, pp. 639–657, 2006.

[43] O. K. Helferich and R. L. Cook, "Securing the supply chain," *Council Log. Manage.*, Oak Brook, IL, USA, 2002.

[44] B. B. Flynn, R. G. Schroeder, and S. Sakakibara, "The impact of quality management practices on performance and competitive advantage," *Dec. Sci.*, vol. 26, no. 5, pp. 659–691, 1995.

[45] H. Kaynak and J. L. Hartley, "Exploring quality management practices and high tech firm performance," *J. High Technol. Manage. Res.*, vol. 16, no. 2, pp. 255–272, 2005.

[46] J. Perdomo-Ortiz, J. González-Benito, and J. Galende, "Total quality management as a forerunner of business innovation capability," *Technovation*, vol. 26, no. 10, pp. 1170–1185, 2006.

[47] D. Kim, V. Kumar, and U. Kumar, "Relationship between quality management practices and innovation," *J. Oper. Manage.*, vol. 30, pp. 295–315, 2012.

[48] J. C. Anderson, M. Rungtusanatham, and R. G. Schroeder, "A theory of quality management underlying the Deming management method," *Acad. Manage. Rev.*, vol. 19, no. 3, pp. 472–509, 1994.

[49] F. J. Quinn, "Security matters," *Supply Chain Manage. Rev.*, vol. 7, no. 4, pp. 38–45, 2003.

[50] C. W. Craighead, J. Blackhurst, M. J. Rungtusanatham, and R. B. Handfield, "The severity of supply chain disruptions: Design characteristics and mitigation capabilities," *Dec. Sci.*, vol. 38, no. 1, pp. 131–157, 2007.

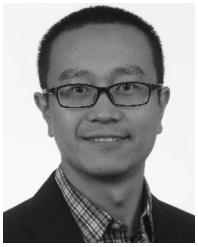
[51] R. W. Brislin, "Translation and content analysis of oral and written materials," in *Handbook of Cross-Cultural Psychology: Methodology*, vol. 2, H. C. Triandis and J. W. Berry Eds. Boston, MA, USA: Allyn & Bacon, 1980, pp. 389–444.

[52] Z. Williams, N. Ponder, and C. W. Autry, "Supply chain security culture: Measure development and validation," *Int. J. Log. Manage.*, vol. 20, no. 2, pp. 243–260, 2009.

[53] K. M. Eisenhardt, "Building theories from case study research," *Acad. Manage. Rev.*, vol. 14, no. 4, pp. 532–550, 1989.

[54] S. Ambulkar, J. Blackhurst, and S. Grawe, "Firm's resilience to supply chain disruptions: Scale development and empirical examination," *J. Oper. Manage.*, vol. 33–34, pp. 111–122, 2015.

[55] J. S. Armstrong and R. S. Overton, "Estimating nonresponse bias in mail surveys," *J. Marketing Res.*, vol. 14, no. 3, pp. 396–402, 1977.
[56] D. R. Krause, "The antecedents of buying firms' efforts to improve suppliers," *J. Oper. Manage.*, vol. 17, no. 2, pp. 205–224, 1999.
[57] M. K. Lindell and D. J. Whitney, "Accounting for common method variance in cross-sectional research designs," *J. Appl. Psychol.*, vol. 86, no. 1, pp. 114–121, 2001.
[58] H. A. Richardson, M. J. Simmering, and M. C. Sturman, "A tale of three perspectives: Examining post hoc statistical techniques for detection and correction of common method variance," *Org. Res. Methods*, vol. 12, no. 4, pp. 762–800, 2009.
[59] X. A. Koufteros and G. A. Marcoulides, "Product development practices and performance: A structural equation modeling-based multi-group analysis," *Int. J. Prod. Econ.*, vol. 103, pp. 286–307, 2006.
[60] A. N. Tikhonov and V. Y. Arsenin, *Solution of Ill-Posed Problems*. Washington, DC, USA: Winston & Sons, 1977.
[61] D. Cramer, *Basic Statistics for Social Research*. Evanston, IL, USA: Routledge, 1997.
[62] N. Venkatraman, "Performance implications of strategic coalignment: A methodological perspective," *J. Manage. Stud.*, vol. 27, no. 1, pp. 19–41, 1990.
[63] S. Y. Ponomarov and M. C. Holcomb, "Understanding the concept of supply chain resilience," *Int. J. Log. Manage.*, vol. 20, no. 1, pp. 124–143, 2009.
[64] D. L. Coutu, "How resilience works," *Harv. Bus. Rev.*, vol. 80, pp. 46–50, May 2002.



Guanyi Lu received the Ph.D. degree in operations/supply chain management from Mays Business School, Texas A&M University, College Station, TX, USA, in 2013.

Prior to his academic career, he served in a leading Asia-based original equipment manufacturer as an Assistant Supply Chain Manager. He is an Assistant Professor with the Department of Supply Chain and Decision Sciences, College of Business, Oregon State University, Corvallis, OR, USA. His research has appeared in refereed journals including *Production and Operations Management*, *Decision Sciences*, the *Journal of Supply Chain Management*, the IEEE TRANSACTIONS ON ENGINEERING MANAGEMENT, and the *International Journal of Production Economics*, among others. His research interests include supply chain security and risk management, supply chain structure, behavioral operations management, supply chain integration, and information and communication technology.

Dr. Lu is a Member of the Editorial Board for the *Journal of Marketing Channels*.

Xenophon Koufteros received the Ph.D. degree from the University of Toledo, Toledo, OH, USA, in 1995, and the MBA degree from Bowling Green State University, Bowling Green, OH, in 1989.

He is a Professor of supply chain management in the Mays Business School, Texas A&M University, College Station, TX, USA, where he also holds the Jenna and Calvin R. Guest Professorship in Business. He has published more than 40 articles in refereed journals including the *Journal of Operations Management*, *Production and Operations Management*, *Decision Sciences*, the *Journal of Supply Chain Management*, *Structural Equations Modeling*, the IEEE TRANSACTIONS ON ENGINEERING MANAGEMENT, the *International Journal of Production Research*, the *International Journal of Production Economics*, and *OMEGA*, among others.

Dr. Koufteros served as an Associate Editor for the *Journal of Operations Management*, the *Journal of Supply Chain Management*, the *Journal of Business Logistics*, and *Decision Sciences*. He received the Best Associate Editor Award from the *Journal of Operations Management* and the *Journal of Supply Chain Management*, and the Best Empirical Paper Award from *Decision Sciences*. He is also a Member of the Editorial Board for *Production and Operations Management, Structural Equation Modeling: An Interdisciplinary Journal, Educational and Psychological Measurement*, and the *Journal of Marketing Channels*. He has received numerous teaching awards, such as the Association of Former Students Teaching Award from Mays Business School. He also received several awards for his service to the profession and students, such as the Distinguished Achievement Award—Individual Student Relationships, at the university level, and the Association of Former Students, Texas A&M University.

Lorenzo Lucianetti received the Ph.D. degree in business administration from the Department of Management and Business Administration, University of Chieti and Pescara, Italy, in 2004.

He is an Associate Professor of business administration with the University of Chieti and Pescara, and a Visiting Research Fellow with the University of Cranfield, U.K. His main research interests include managerial control systems, supply chain performance, and employee performance. His research has appeared in refereed journals such as the *Academy of Management Journal*, the *Journal of Applied Psychology*, the *Journal of Operations Management*, the *Journal of Organizational Behavior*, the *Journal of Business Ethics*, the *International Journal of Operations and Production Management*, and *Management Accounting Research*.