JOURNAL OF BUSINESS LOGISTICS
STRATEGIC SUPPLY CHAIN RESEARCH

Journal of Business Logistics, 2013, 34(4): 320–334

Public–Private Partnerships and Supply Chain Security: C-TPAT as an Indicator of Relational Security

M. Douglas Voss[1] and Zachary Williams[2]

[1]*University of Central Arkansas*
[2]*Central Michigan University*

Following the attacks of September 11th, public and private entities recognized a need to protect the global supply chain from terrorist disruption. In response to this need, the U.S. Government partnered with industry to create the Customs-Trade Partnership Against Terrorism (C-TPAT) program. This research investigates the public–private partnership (PPP) relational aspects of C-TPAT. C-TPAT encourages firms to voluntarily improve their security competence and that of their supply chain partners. We introduce the concept of relational security in the context of PPPs. We define relational security as *all activities that establish, cultivate, and maintain successful security exchanges between parties*. We establish C-TPAT as one indicator of relational security by demonstrating its ability to establish, cultivate, and maintain successful security exchanges between parties. Results indicate certified firms outperform noncertified firms in security performance, firm performance, and resilience.

Keywords: public–private partnerships; supply chain; security; C-TPAT; performance; relational security

INTRODUCTION

Following the attacks of September 11th, public and private entities recognized a need to protect the global supply chain from terrorist intrusion. Beyond the loss of human life, supply chain disruptions can have other negative impacts. These include decreased revenue and customer satisfaction resulting from delayed deliveries as well as decreased brand equity if customer perceptions of the firm are altered. Hendricks and Singhal (2005) demonstrate these impacts can significantly devalue the affected firms' stock price.

Efforts to control supply chain security are hampered by the complexity, size, and interdependency of the network (Speier et al. 2011). The complexity and increased length inherent to global supply chains, coupled with the need to maintain an efficient and effective flow of goods, necessitated an innovative response. Transaction cost analysis (TCA) (Williamson 1985; Rindfleisch and Heide 1997) would argue that the U.S. Government (USG) could have structured the security response in several ways. First, the USG could insource security by placing security personnel at every firm, similar to the Transportation Security Administration in airports. However, such an action would have been prohibitively expensive and difficult to enforce outside the United States. Second, the USG could rely on market forces by asking firms to employ proper security measures and providing incentives based on measurable security performance outcomes. However, security performance outcomes are notoriously hard to measure in the absence of a security incident. The determination was made that a hybrid governance mechanism based upon public–private partnership (PPP) between the USG and private firms was necessary. The formalization of this PPP strategy was embodied in the Customs-Trade Partnership Against Terrorism (C-TPAT) (Kleindorfer and Saad 2005).

C-TPAT is administered through U.S. Customs and Border Protection (CBP), a division of the U.S. Department of Homeland Security (DHS). CBP describes C-TPAT as a, "voluntary government/private sector partnership program…for securing global supply chains and facilitating legitimate cargo and conveyances" (U.S. Customs and Border Protection 2004, 11–12). C-TPAT seeks to create a critical mass of supply chain security. This is accomplished by ensuring certified firms employ proper security measures and requiring their supply chain partners to increase security as well. In this way, C-TPAT is able to reach beyond certified firms to more widely implement security best practices in nonparticipating companies on a global basis.

PPPs have been applied in many contexts outside of security including transportation, education, construction, and financial management (Wettenhall 2003; Stewart et al. 2009). Their continued application is a function of past PPP success. One measure of C-TPAT's success is the growth of certified firms. C-TPAT was proposed in November 2001 and implemented in April 2002 (Sheu et al. 2006). By November 2004, its membership had grown to 7,400 partners (U.S. Customs and Border Protection 2004). This number increased to 10,572 by July 2013, 41% of whom were domestic importers, 29% carriers (motor, rail, sea, and air), 12% foreign manufacturers, 9% third-party logistics, 8% customs brokers, and 0.6% marine port authorities and terminal operators (U.S. Customs and Border Protection 2013).

Stewart et al. (2009) have called for research defining the effects of PPPs on firm performance. Conflicting evidence exists regarding the private sector benefits of C-TPAT (Furia et al. 2011). C-TPAT implementation can be expensive and its benefits may be hard to quantify because it is difficult to assess the number of prevented security events or their effects. Few works have investigated the impact of security measures on performance. Even fewer have specifically examined the impact of C-TPAT certification on performance.

Corresponding author:
M. Douglas Voss, Department of Marketing and Management, University of Central Arkansas, 312 Business Administration Building, Conway, AR 72035, USA; E-mail: voss@uca.edu

The purpose of this study was to explore performance differences associated with C-TPAT certification. We specifically determine whether C-TPAT is associated with reduced security breach severity, improved security performance, greater resilience, and improved firm performance. In doing so, the concept of relational security is introduced and C-TPAT is positioned as an indicator of relational security. Relational security is defined as *all activities that establish, cultivate, and maintain successful security exchanges between parties*. We establish that C-TPAT is designed to promote security exchanges between parties and examine whether these relationships are related to successful outcomes.

The following sections review literature related to risk, supply chain security, PPPs, and C-TPAT. Hypotheses are then presented followed by a description of the method, results, and implications. Finally, conclusions and future research opportunities are discussed.

LITERATURE REVIEW

Risk and supply chain security

Terrorism, theft, damage, or insertion of unauthorized cargo represent a significant, and deliberate risk facing supply chains (Kleindorfer and Saad 2005). As the risk of terrorism increases so must firm efforts to counter that risk (Christopher and Lee 2004). Supply chain security is defined 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" (Closs and McGarrell 2004, 8).

Security and risk are closely related but distinct concepts. Speier et al. (2011) highlight the differences. Risk is the extent that supply chain activities are variable and susceptible to disruption leading to negative outcomes (Zsidisin 2003; Zsidisin and Ellram 2003). Supply chain security helps mitigate risk and render the supply chain more sustainable (Speier et al. 2011). Firms cannot completely mitigate every risk and depend on other firms to manage their own risks appropriately. These efforts are complicated by the interdependency and lean inventory levels found in global supply chains. Should a security event occur, the consequences are felt by dependent partners and exacerbated by a lack of spare resources. Therefore, when supply chains operate in a lean manner, the interconnectedness of the global supply chain infrastructure actually increases vulnerability to security events (Perrow 1984; Speier et al. 2011). This highlights the need for a program such as C-TPAT that provides standardized security recommendations as a governmental response to global supply chain security challenges.

The role of government and C-TPAT

Firms implement security measures for a number of reasons. Williams et al. (2009a) propose that firms are driven to implement security measures due to coercive, normative, and mimetic pressures. Coercive pressures are those originating from customers or the government. However, the USG has taken a more collaborative role as well. Following September 11th, 2001 the USG was compelled to design a program that would create a critical mass of security throughout the supply chain and devise a governance mechanism to ensure firms employ proper security measures. In designing this mechanism, they would be faced with three basic options: (1) insource security by dictating specific security measures and placing USG enforcement personnel at every firm; (2) outsource security by relying on all firms to implement security initiatives on their own; or (3) rely on a hybrid mechanism such as a partnership between firms and the USG. Their decision of which governance mechanism to employ can be described using TCA and juxtaposed against real-world constraints.

TCA is based on the notion that hierarchies and markets represent two governance structures that vary in their level of transaction costs (Coase 1937). Transaction costs are those "expenses" inherent to a chosen governance mechanism in a given system and include ex ante costs (constructing and negotiating contractual arrangements) as well as ex post costs (monitoring the actors and enforcing compliance) (Rindfleisch and Heide 1997). Ex ante costs increase as decision makers, subject to bounded rationality and environmental uncertainty, are unable to completely predict future contingencies (Williamson 1985). To compensate, the decision makers attempt to construct increasingly costly, complicated, and complete contracts that protect against all possible future events. Ex post costs increase as behavior becomes more uncertain and it becomes more difficult to monitor and determine performance levels of those on whom the decision maker depends.

Decision makers will outsource and rely on market mechanisms when future contingencies are predictable (i.e., environmental uncertainty is low) and performance is easily monitored (i.e., behavioral uncertainty is low). Alternatively, they are more likely to insource functions as it becomes more difficult to detail all future contingencies (i.e., environmental uncertainty is high) and performance becomes more difficult to monitor (i.e., behavioral uncertainty is high) (Anderson 1985).

The global supply chain is dynamic and diverse. Some participants disregard their security obligations due to opportunistic actions or feelings of invulnerability (Wathne and Heide 2000; Williams et al. 2008; Voss et al. 2009b). Furthermore, security performance outcomes are difficult to measure in the absence of a security incident. This would imply that some insourcing of the security function is required as both environmental and behavioral uncertainties are high. However, without completely crippling all U.S. trade, the USG is unable to legally enforce security regulations on firms outside its borders or place security personnel at their facilities. Only other members of the supply chain could demand security compliance from their trading partners. Therefore, the USG had to rely on market mechanisms to some degree and a hybrid governance structure was required.

Relational governance is a hybrid governance structure that supports the concepts embedded in C-TPAT (Heide 1994). More specifically, C-TPAT developed as a PPP between the USG and private entities. C-TPAT reduces transaction costs to the USG by placing a greater burden on industry to enforce security implementation while also providing the USG a degree of hierarchical control over security implementation. Transaction costs are reduced for participating firms via reduced wait time and variability at border crossings (Furia et al. 2011).

Sheffi (2001) calls for executives to begin considering the government as a partner in their security efforts. C-TPAT is based on past, successful joint efforts between CBP and industry partners and asks for firms' commitment to improve supply chain security to gain benefits including reduced inspections and expedited shipment processing (Bakir 2008). Once certified, firms are granted access to the benefits of C-TPAT including Free And Secure Trade (FAST) lane priority at border crossings and use of the Automated Targeting System—which seeks to determine shipment risk and whether an inspection is required (Bakir 2008)—and NonIntrusive Inspection technology to speed processing (Russell and Saldanha 2003). These and other benefits of C-TPAT certification are provided in Table 1 (U.S. Customs and Border Protection 2004).

Public–private partnerships

PPPs are not a new phenomenon. Historical cooperation between governments and private entities include private tax collectors in the Bible, private English citizens cleaning publically owned street lamps in the 1700s, privately owned railways in the 1800s, and Sir Francis Drake's extensive use of private vessels to best the Spanish Armada in the 1500s (Hodge and Greve 2007). Public–private interaction is also not unusual in a supply chain management context. Public and private entities are involved in various supply chains, which often intersect leading to collaboration (Stewart et al. 2009).

Several definitions of PPPs exist. PPPs are defined by the National Council for Public–Private Partnerships, as "a contractual agreement between a public agency (federal, state, or local) and a private sector entity. Through this agreement, the skills and assets of each sector are shared in delivering a service or facility for the use of the general public. In addition to the sharing of resources, each party shares in the risks and rewards potential in the delivery of the service and/or facility" (NCPPP: National Center for Public-Private Partnerships 2008). Through PPPs, public agencies attempt to protect the interests of the population by sharing risk while increasing accountability and transparency (Stewart et al. 2009).

This study utilizes Van Ham and Koppenjan's (2001) definition of PPPs who view them as, "cooperation of some sort of durability between public and private actors in which they jointly develop products and (or) services and share risks, costs, and resources which are connected to these products" (p. 598). This definition highlights that PPPs involve: (1) long-term cooperation; (2) risk-sharing; (3) joint production of some product or service; and (4) mutual gain (Hodge and Greve 2007). C-TPAT fits this definition. First, the USG and its industry partners have expectation of long-term cooperation. The USG conducts a detailed review of applicants' security programs before certification then expects ongoing improvement. Second, risk is shared among parties. It is impossible for the USG to secure every supply chain. By offering C-TPAT certification, the USG is outsourcing some risk and cost to private sector partners. Private partners are implementing security best practices, which should improve security performance and reduce risk. C-TPAT certification allows CBP to focus inspection efforts on noncertified firms and allocate resources to higher-risk areas. Third, by joint cooperation through C-TPAT, supply chain and ultimately national security is improved. Fourth, mutual gains are achieved. For the USG, the risk of attack is decreased without compromising the efficient flow of goods while certified firms enjoy reduced supply risk as C-TPAT certification allows for less—and less variable—inspection time.

PPP key success factors: their relationship with business to business partnerships and C-TPAT

PPPs share many similarities with business to business (B2B) partnerships such as long-term cooperation, risk-sharing, joint production of some product or service, and mutual gain (Dwyer et al. 1987; Bowersox et al. 1999). Therefore, it can be expected that successful relational exchanges between government and private entities entail similar characteristics.

Jacobson and Choi (2008) posit key PPP success factors, which are presented in bold in Table 2. Table 2 also details citations from the relationship marketing, social capital, supply chain and security literature streams establishing the link between B2B and PPP relationships. We have extended this to include corollary tenants of C-TPAT. The literature presented coupled with Table 2 illustrates that: (1) C-TPAT is a PPP that promotes secu-

Table 1: Benefits of C-TPAT certification

1. A reduced number of inspections and reduced border wait times.
2. A Customs-Trade Partnership Against Terrorism (C-TPAT) supply chain specialist to serve as the Customs and Border Protection (CBP) liaison for validations, security issues, procedural updates, communication, and training.
3. Access to the C-TPAT members through the Status Verification Interface.
4. Self-policing and self-monitoring of security activities.
5. In the Automated Commercial System (ACS), C-TPAT-certified importers receive reduced selection rates for Compliance Measurement Examinations and exclusion from certain trade-related local and national criteria.
6. C-TPAT-certified importers are eligible for Free And Secure Trade (FAST) lanes on the Canadian and Mexican borders, the Office of Strategic Trade's (OST) Importer Self-Assessment Program (ISA), and have been given priority access to participate in the Automated Commercial Environment (ACE).
7. C-TPAT-certified highway carriers benefit from their access to the expedited cargo processing at designated FAST lanes on the Canadian and Mexican borders. These carriers are eligible to receive more favorable mitigation relief from monetary penalties.
8. C-TPAT-certified Mexican manufacturers benefit from their access to the expedited cargo processing at the designated FAST lanes.
9. All C-TPAT-certified companies are eligible to attend CBP-sponsored C-TPAT supply chain security training seminars.

Table 2: Relating PPP and B2B key success factors with C-TPAT

PPP key success factors*	Relationship with C-TPAT
Shared vision	
McCutcheon and Stuart (2000)†	Customs-Trade Partnership Against Terrorism (C-TPAT) aligns the goals of private firms with the security vision and requirements of the federal government by prescribing a framework of measures the firm and its supply chain partners must implement
Commitment	
Pettit et al. (2010)† Morgan and Hunt (1994)†	C-TPAT-certified firms and their supply chain partners are regularly audited to ensure continued compliance with and commitment to the program. C-TPAT certification and maintenance is not free, and therefore requires executive commitment to remain certified and gain potential long-term benefits
Open communication and trust	
Leana and Pil (2006)†	A key tenant of C-TPAT is the open exchange of information between private and public entities in the form of certification profiles and security best practices
Willingness to compromise/collaborate	
Faisal et al. (2006)† Morgan and Hunt (1994)†	C-TPAT is a voluntary program bringing together public and private partners who willingly and proactively collaborate to create a critical mass of security throughout the global supply chain
Political support	
Voss et al. (2006)† Kleindorfer and Saad (2005)†	The U.S. Department of Homeland Security (DHS) is the third largest cabinet department in the U.S. Federal Government. C-TPAT is one of the more successful programs within DHS and includes 10,572 members who support its goals as exhibited by their continued participation (U.S. Customs and Border Protection 2013)
Risk awareness	
Lado et al. (1997)†	The federal government shares sensitive threat information with C-TPAT members so that they may reduce the risk of terrorist intrusion. Members are aware that failure to comply with C-TPAT guidelines may lead to loss of expedited border crossing treatment
Clear roles and responsibilities	
Jap (1999)†	C-TPAT clearly delineates the responsibilities of member companies and audits their ongoing compliance to ensure they are fulfilling their roles and responsibilities under the program

Notes: B2B, business to business; PPP, public–private partnership.
*Jacobson and Choi (2008).
†Citations from the relationship marketing, social capital, supply chain, and security literature streams indicating similar key success factors are necessary in B2B relationships.

rity-related public–private and B2B relationships; (2) C-TPAT demonstrates characteristics necessary for PPP success; and (3) similar key success factors characterize PPPs and partnerships between private entities.

C-TPAT as an enabler of relational security performance

The preceding discussion demonstrates that PPPs and private relationships share many of the same key success factors and C-TPAT has incorporated many of these factors in its design. It is therefore logical that the factors engendering success in other PPPs and B2B relationships may also engender success in security-related relationships. Morgan and Hunt (1994) define relationship marketing as, "all marketing activities directed toward establishing, developing, and maintaining successful relational exchanges" and state that, "What should be central to understanding relationship marketing is whatever distinguishes productive, effective relational exchanges from those that are unproductive and ineffective—that is, whatever produces relationship marketing success instead of failure" (p. 22).

Morgan and Hunt's (1994) former statement is modified to introduce the concept of relational security. Relational security is defined as *all activities that establish, cultivate, and maintain successful security exchanges between parties*. We modify Morgan and Hunt's latter statement and propose that to truly understand relational security we must demonstrate those factors that distinguish productive and effective security exchanges between parties from others that are unproductive and ineffective. For C-TPAT to represent an indicator of relational security, it must accomplish two goals. First, the program must help establish, cultivate, and maintain security exchanges between the USG and C-TPAT-certified firms as well as C-TPAT-certified firms and their supply chain partners. Second, certified firms must outperform their noncertified counterparts. This would indicate that C-TPAT distinguishes productive and effective security exchanges from those that are unproductive and ineffective.

HYPOTHESES

The following positions C-TPAT as an indicator of relational security by hypothesizing that C-TPAT is related to success in terms of reduced security breach severity, increased security performance, increased resilience, and improved firm performance.

Breach severity

A severe security breach is conceptualized as one with the potential to significantly impact the affected firm. Not all breaches are created equal. For instance, unauthorized personnel may gain access to a meat processor's facility. If this person gains access to a parking lot, and is then apprehended, the breach would be less severe than if the person gained access to sensitive production machinery or product. As a result, one of C-TPAT's key provisions is the use of risk-based monitoring. Firms are encouraged to monitor their business partners and supply chain activities based upon relative risk. Furthermore, CBP selects C-TPAT participants for validation based on risk, with risk determined by geography, security irregularities, volume and value of imports, and role in the supply chain. These procedures should uncover firms and shipments that pose the greatest risk and cause more severe breaches (U.S. Customs and Border Protection 2004).

Voss et al. (2009b) explore the difference between firms that place a high strategic priority on security and those that do not. Firms that place a high strategic priority on security were characterized by senior management support of security initiatives (e.g., C-TPAT), the belief that security measures are necessary to protect the company's brand or reputation, and the existence of a corporate level strategy to address security concerns. Their findings indicate that firms placing a high strategic priority on security share timely, valid, and actionable security-related information with supply chain partners to improve incident response. This was related to a reduction in supply chain security incidents. Improved response to security incidents also allows firms to neutralize the threat before the breach becomes more severe.

Autry and Bobbitt (2008) describe Supply Chain Security Orientation (SCSO) and detail its outcomes. They propose that firms characterized by SCSO build partnerships with government and other private entities to improve supply chain continuity. This implies SCSO firms are able to reduce the severity of any breaches and ensure operational sustainability. Similarly, Craighead et al. (2007) report that all firms are susceptible to breaches but the ability to detect and respond to abnormal incidents will likely reduce breach severity. This is critical as C-TPAT certification requires firms to share information and prepare for extraordinary events.

Therefore, Hypothesis 1 posits that C-TPAT certification is positively related to reduced breach severity.

H_1: *C-TPAT certification is positively related to reduced breach severity.*

Security performance

We define security performance as the ability of a firm to effectively meet internal and external expectations for delivering products or services without intrusion. Autry and Bobbitt (2008) propose that security improves firms' ability to meet and exceed customer expectations. Voss et al. (2009b) find that firms placing strategic importance on security, which includes extending security efforts beyond the "four walls" and seeking external security validation, experience higher levels of security performance. Closs and McGarrell (2004) advocate forming security relationships in an effort to improve security performance. Prokop (2004) purports that private sector entities must collaborate with the public sector in order to achieve security compliance.

Furia et al. (2011) examine the benefits of C-TPAT certification. They find one benefit is the ability to meet customers' security expectations and 83% of firms in their sample are engaged in contracts requiring C-TPAT certification. Requiring certification indicates these firms expect their supply chain partners to employ proper security procedures. Williams et al. (2009) suggest the USG drives firms to implement supply chain security and this relationship should improve security performance.

In summary, public sector programs are often used to improve security performance. Hypothesis 2 posits that C-TPAT certification is positively related to higher security performance.

H_2: *C-TPAT certification is positively related to higher security performance.*

Resilience

Resilience is the "ability to react to unexpected disruptions and restore normal supply network operations" (Rice and Caniato 2003, 27). Normal Accident Theory holds that interdependent supply chain partners impact each other's ability to respond, recover, and restore operations following an unexpected event (Perrow 1984; Speier et al. 2011). Top firms value supply chain resiliency. Cisco surveys their top supply chain partners twice per year in an effort to understand their partners' resilience (Bonney 2011). Pfizer requires its prospective supply chain partners to provide detailed information on their resiliency (Ritchey 2011).

Firms must understand their supply chain processes to improve security. Closs et al. (2008) term this understanding, "process management." Firms must map critical nodes and product flows in order to understand a process and its vulnerabilities. Stewart et al. (2009) posit that this will improve resiliency. By assessing node criticality, the firm is better able to preposition supplies or employ redundant processes to speed recovery. This prepositioning can require agreement and cooperation between supply chain partners as well as government agencies. Whipple et al. (2009) find firms facing increased security risk build greater resiliency into their operations and are able to effectively recover from security incidents. Similarly, Voss et al. (2009b) find that firms placing greater emphasis on security initiatives have higher internal and external supply chain resilience. Peleg-Gillai et al. (2006) find that security efforts reduce the time required for problem identification, response, and resolution.

These studies suggest that resilience is a desired outcome of security initiatives. Hypothesis 3 posits that C-TPAT certification is positively related to improved resilience.

H_3: *C-TPAT certification is positively related to improved resilience.*

Firm performance

Firm performance is defined as the firm's ability to meet or beat internal and external performance expectations in terms of pro-

duction cost, quality, and quantity as well as customer satisfaction. Recent research has suggested firm performance benefits resulting from C-TPAT and security initiatives.

Security inspections at border crossings are expensive and delay shipments, which cause transit time uncertainty. Furia et al. (2011) find border delay costs differ by mode with a range of $200–$1,500. These delays increase lead time uncertainty affecting asset utilization, efficiency, and customer satisfaction (Voss et al. 2009b). Shipments from C-TPAT-certified firms are seven times less likely to be inspected (Szakonyi 2013). C-TPAT-certified firms also gain access to expedited inspection procedures that reduce inspection frequency and temporal variability. Furthermore, some security measures (e.g., RFID and smart seals) improve asset visibility, simultaneously increasing supply chain security and decreasing costs (Lee and Whang 2003; Lee and Wolf 2003). Additional research has specifically addressed cost savings for C-TPAT-certified firms. Eggers (2004) reports that participating in government security initiatives resulted in a cost savings of $378–$462 per container imported into the United States. Hasbro's C-TPAT certification reduced inbound inspection delays yielding over $500,000 in annual cost savings (Gonzalez 2004). These studies suggest that C-TPAT-certified firms achieve higher performance through reduced costs and other ancillary benefits (Sheu et al. 2006; Furia et al. 2011).

Autry and Bobbitt (2008) posit that security practices improve quality. Voss et al. (2009a) posit that security and quality are both strategic supplier attributes and may be complementary. Security inspections occurring during the manufacturing and logistics processes would likely uncover quality issues. For instance, a security inspection designed to uncover food product contamination may also uncover discolored product or faulty packaging. Finally, other performance improvements may also be realized. Security programs often require increased information sharing and supply chain visibility. This improves efficiency and effectiveness by lowering inventories, improving productivity by reducing delays, increasing fill-rates, and meeting production and shipping goals (Sarathy 2006).

C-TPAT certification may also lead to increased market opportunities. Voss et al. (2009a) find that under certain conditions purchasing agents are willing to trade off price and delivery reliability in return for security. This indicates that some firms may be more satisfied with secure suppliers. Peleg-Gillai et al. (2006) find that security efforts engendered higher customer satisfaction in the form of reduced customer attrition. Sheu et al. (2006) discover firms have increased customer satisfaction performance as a result of C-TPAT certification.

Autry and Bobbitt (2008) propose that firms may even gain a competitive advantage from security by avoiding the effects of a successful terrorist event after it occurs and, more proactively, by preventing competitors from drawing contrasts between their own security measures. C-TPAT and security may yield other marketing benefits as well (Murphy 2008). Firms may use voluntary certifications as part of a marketing program designed to attract and retain new business (Arora and Gangopadhayay 1995).

Alternatively, some particularly sensitive supply chain customers are using C-TPAT compliance as a supplier choice criterion (Szakonyi 2013). As a result, C-TPAT-certified firms may gain a competitive advantage and take business from noncertified competitors. Therefore, Hypothesis 4 posits that C-TPAT certification is positively related to higher firm performance.

H_4: *C-TPAT certification is positively related to higher firm performance.*

METHOD

This study utilized a survey methodology with data gathered through an online research panel provider (Zoomerang). Online panels have become increasingly popular in various disciplines including marketing (e.g., Hoffman et al. 2010; Kees et al. 2010; Oliver and Rosen 2010; Shang et al. 2010; Soster et al. 2010; Beitelspacher et al. 2011; Chernev et al. 2011; Palmeira and Thomas 2011; Bearden and Haws 2012) and supply chain management (e.g., Autry et al. 2008, 2010; Jack et al. 2010; Richey et al. 2010; Grawe et al. 2011; Zelbst et al. 2012). Prior research indicates that online panels yield data similar to more traditional data collection methods (Dennis 2001; Pollard 2002). Moreover, research has indicated that data collected via research panels may actually be superior. Braunsberger et al. (2007) find online panel data to be more reliable than that collected through other means.

Supply chain researchers have recently been called upon to carefully choose appropriate samples (Knemeyer and Naylor 2011; Thomas 2011). This research employs the sampling procedures of other supply chain researchers who have utilized panels (e.g., Autry et al. 2010). First, respondents were asked questions regarding current employment status and their role within their firm. Only individuals who currently worked within a role requiring sufficient supply chain knowledge were allowed to continue in the survey. Given the nature of the research, respondents in executive and managerial roles with relatively large amounts of responsibility and knowledge of the firm were targeted.

Respondents were also asked about their specific job titles. Responses from titles such as CEO, VP, Director, Owner, and Manager were sought. Persons whose job titles indicate a lack of sufficient subject matter knowledge were eliminated from the sample. Finally, the survey also included multiple "trap" questions based on previous online panel research recommendations (Maronick 2009). If respondents failed the traps, their responses were eliminated.

Pilot study

A pilot study was conducted with the same panel provider (Zoomerang). The pilot study generated 33 usable responses. Principal components analysis (PCA) was used to assess item and construct unidimensionality, reliability, and validity. All measures performed as expected and no alterations were made to the survey.

Main study

The sample was then expanded and 852 responses were collected. Respondents were excluded who lacked appropriate expertise, failed trap questions, or did not complete the survey yielding 338 usable responses. Individual and firmographic data

are presented in Table 3. C-TPAT membership was assessed by asking informants if their firm was C-TPAT certified (0 = not certified; 1 = certified). Of the 338 respondents, 81 identified their firms as C-TPAT certified and 257 had not achieved or sought certification.

Outcome measures

The items for each of the outcome measures are found in the Appendix. All items used a 7-point semantic differential response scale with varying anchors. Breach severity is defined as the extent to which firms have reduced the impact of security failures. Two newly created items were used to measure breach severity and assess respondents' level of agreement that a severe security breach has occurred. BS_1 asked respondents to indicate their level of agreement as to whether their firm has suffered a severe security breach. BS_2 asked respondents to consider the breaches they have experienced and indicate the severity of these incidents.

Resiliency is defined as the "ability to react to unexpected disruption and restore normal supply network operations" (Rice and Caniato 2003, 27). Measures include items from previous studies (e.g., Williams et al. 2009b) and new items derived from discussions with knowledgeable academics and practitioners engaged in supply chain risk research and practice.

Security performance is defined as the ability of a firm to effectively meet internal and external expectations for delivering products and/or services without unauthorized intrusion. Items to measure security performance were adopted from Voss et al. (2009a).

Table 3: Sample description

Respondent title	Number	%
CEO/President/GM	73	23.9
VP/AVP/EVP	14	4.6
Director/Assistant Director/Dept. Head	50	16.4
Manager/Assistant Manager	168	55.1
Supply chain position		
Manufacturer	112	37.2
Carrier	24	8.0
Wholesaler/Distributor	45	15.0
Freight forwarder	13	4.3
Third-party logistics provider	21	7.0
Warehouser	21	7.0
Retailer	65	21.6
Revenue		
$1–$999,999	49	17.4
$1,000,000–$9,999,999	76	27.0
$10,000,000–$49,999,999	66	23.5
$50,000,000–$99,999,999	47	16.7
Greater than $1B	43	15.3
Employees		
1–99	104	29.9
100–499	71	20.4
500–4,999	73	21.5
Greater than 5,000	91	26.8

Firm performance is the firm's ability to meet or beat internal and external performance expectations in terms of production cost, quality, and quantity as well as customer satisfaction. Respondents were asked to indicate how well their firm has met internal performance targets across various items. Next, respondents were asked to evaluate the same performance items against their direct competition. This type of measurement is consistent with prior strategy research (e.g., Chattopadhyay et al. 2001).

RESULTS

Psychometric assessment

Several steps were taken in order to evaluate construct unidimensionality, reliability, and validity. First, unidimensionality was assessed using a PCA as suggested by Netemeyer et al. (2003). Unidimensionality was demonstrated in each instance when all items only loaded highly on the construct of interest.

Next, scale reliability was assessed using Cronbach's alpha. Alpha values are presented in Table 4 and ranged from .849 to .940 (Nunnally and Bernstein 1994). Last, construct validity was assessed in two ways. First, PCA with Varimax Rotation was used to assess discriminant and convergent validity. As shown in Table 4, all items loaded on their expected component and failed to significantly load on unassociated components.

Second, average variance extracted (AVE) was also used to assess convergent and discriminant validity (Fornell and Larcker 1981). As shown in Table 5, AVE is greater than .50 and greater than the shared variance for each construct.

Table 4: Factor structure and reliability

BS_1				.904
BS_2				.909
R_1	.692			
R_2	.786			
R_3	.779			
R_4	.752			
R_5	.730			
R_6	.794			
R_7	.824			
R_8	.728			
R_9	.728			
SP_1			.779	
SP_2			.755	
SP_3			.704	
SP_4			.722	
$Perf_1$		.547		
$Perf_2$		.710		
$Perf_3$		.637		
$Perf_4$		.679		
$Perf_5$		.629		
$Perf_6$		.708		
$Perf_7$		.737		
$Perf_8$		.731		
Cronbach's alpha	.940	.903	.893	.849

Note: All factor loadings of less than .40 were suppressed for readability.

Table 5: Average variance extracted and shared variance

	Breach severity	Resilience	Security performance	Firm performance
AVE	.553	.696	.61	.579
Shared variance				
Breach severity	n/a			
Resilience	.016	n/a		
Security performance	.063	.445	n/a	
Firm performance	.044	.448	.518	n/a

Note: AVE, average variance extracted.

Table 6: Results of MANCOVA multivariate tests

Effect	Value	F	Hypothesis df	Error df	*p*-value	Partial eta squared	Observed power
Firm size	.952	4.160	4	332	.003	.048	.919
C-TPAT	.952	4.219	4	332	.002	.048	.923

Note: C-TPAT, Customs-Trade Partnership Against Terrorism; MANCOVA, multivariate analysis of covariance.

Analysis

Multivariate analysis of covariance (MANCOVA) was utilized to assess significant differences by C-TPAT certification. Four dependent variables were assessed: breach severity, resilience, security performance, and firm performance. Firm size was added as a control variable. Larger firms may exhibit improved security performance as they have "more to lose" than their smaller counterparts. Additionally, larger firms may possess greater resources, which influence performance levels. Finally, larger firms may have better overall performance that could be attributable to factors other than C-TPAT certification. Firm size was measured by the number of employees at the respondent's firm.

Table 6 presents the multivariate MANCOVA results. The overall model was statistically significant: (F [df = 4, 332] = 4.219, $P = .002$; Wilk's Lambda = .952; partial eta squared = .048, observed power = .923). The control variable was also significant (F [df = 4, 332] = 4.160, $P = .003$; Wilk's Lambda = .952; partial eta squared = .048, observed power = .919) and the confounding effects of firm size were eliminated from the model.

Next, the outcome variables were analyzed individually using the tests of between-subject effects. Table 7 presents the mean scores for all constructs by C-TPAT certification status. Three significant differences were found between the two groups.

Hypothesis testing

H_1 posits that C-TPAT certification is positively related to reduced breach severity. Results indicate no significant difference in the severity of security breaches between C-TPAT-certified firms ($mean_{certified} = 2.49$) and noncertified firms ($mean_{noncertified} = 2.40$; $P = .884$). H_1 is not supported.

H_2 posits that C-TPAT certification is positively related to higher security performance. Results indicate that C-TPAT-certified firms outperform noncertified firms in overall security performance ($mean_{certified} = 5.82$, $mean_{noncertified} = 5.39$; $P = .000$), meeting security expectations of customers ($mean_{certified} = 6.00$, $mean_{noncertified} = 5.58$; $P = .002$), responding to security incidents ($mean_{certified} = 5.89$, $mean_{noncertified} = 5.54$; $P = .016$), reducing security incidents over time ($mean_{certified} = 5.80$, $mean_{noncertified} = 5.29$; $P = .001$), and detecting security incidents before they become an issue ($mean_{certified} = 5.62$, $mean_{noncertified} = 5.06$; $P = .000$). H_2 is supported.

H_3 posits that C-TPAT certification is positively related to improved resilience.

Results indicate C-TPAT-certified firms exhibit significantly greater overall resilience ($mean_{certified} = 5.31$, $mean_{noncertified} = 4.80$; $P = .000$), ability to quickly return to normal operations ($mean_{certified} = 5.42$, $mean_{noncertified} = 4.98$; $P = .009$), preparation for major unexpected supply chain disruptions ($mean_{certified} = 5.45$, $mean_{noncertified} = 4.75$; $P = .000$), ability to conduct supply chain operations in the event of security breach ($mean_{certified} = 5.08$, $mean_{noncertified} = 4.50$; $P = .001$), provision of resources for responding to breaches ($mean_{certified} = 5.54$, $mean_{noncertified} = 4.91$; $P = .000$), and preparation for recovering from supply chain breaches ($mean_{certified} = 5.37$, $mean_{noncertified} = 4.86$; $P = .003$). H_3 is supported.

H_4 posits that C-TPAT certification is positively related to higher security performance. Results indicate C-TPAT-certified firms exhibit significantly higher overall firm performance ($mean_{certified} = 5.46$, $mean_{noncertified} = 5.10$; $P = .001$). C-TPAT-certified firms exhibited a significantly greater ability to beat internal performance in terms of production cost ($mean_{certified} = 5.01$, $mean_{noncertified} = 4.56$; $P = .003$), product quality ($mean_{certified} = 5.61$, $mean_{noncertified} = 5.20$; $P = .007$), and productivity ($mean_{certified} = 5.45$, $mean_{noncertified} = 4.91$; $P = .000$). C-TPAT-certified firms exhibited significantly higher performance relative to competitors in terms of product quality ($mean_{certified} = 5.62$, $mean_{noncertified} = 5.29$; $P = .021$) and productivity ($mean_{certified} = 5.50$, $mean_{noncertified} = 4.97$; $P = .001$). Results suggest C-TPAT has a more pronounced relationship with the ability to meet internal targets than outpace competition. H_4 is supported.

Table 7: Results from tests of between-subject effects

			Mean scores	
		p-Value	C-TPAT (n = 81)	Non-C-TPAT (n = 257)
	Breach severity	.884	2.49	2.40
BS_1†	We have suffered a serious supply chain breach.	.491	2.37	2.24
BS_2‡	When thinking about security breaches in the supply chain, we have suffered…	.781	2.53	2.58
	Security performance	.000*	5.82	5.39
SP_1†	Our firm effectively meets the security expectations of our customers.	.002*	6.00	5.58
SP_2†	Our firm is able to effectively respond to security incidents that occur.	.016*	5.89	5.54
SP_3†	Our firm has been successful in reducing the number of security incidents over time.	.001*	5.80	5.29
SP_4†	Our firm is able to effectively detect security incidents before they become an issue.	.000*	5.62	5.06
	Resilience	.000*	5.31	4.80
R_1†	We would quickly bounce back from a serious breach to our supply chain.	.103	5.12	4.83
R_2†	If a serious supply chain breach were to happen, we would return to normal operations in short order.	.009*	5.42	4.98
R_3†	We are prepared for major unexpected supply chain disruptions.	.000*	5.45	4.75
R_4†	We would not have problems with supply chain operations in the event of a significant supply chain breach.	.001*	5.08	4.50
R_5†	A serious breach in our supply chain would have little effect on our long-term supply chain operations.	.104	4.87	4.57
R_6†	We provide resources to create contingency plans for responding to supply chain breaches.	.000*	5.54	4.91
R_7†	We are well prepared for recovering from major supply chain breaches.	.003*	5.37	4.86
R_8†	We have detailed processes for resuming supply chain operations in the event of a breach.	.000*	5.53	4.81
R_9†	We have a formal mechanism for identifying potential responses to emerging supply chain breaches.	.000*	5.53	4.76
	Firm performance	.001*	5.46	5.10
$Perf_1$§	In terms of the cost of producing our products and/or services, we are…	.003*	5.01	4.56
$Perf_2$¶	In terms of the cost of producing our products and/or services, we are…	.062	5.04	4.76
$Perf_3$§	In terms of the quality of our products and/or services, we are…	.007*	5.61	5.20
$Perf_4$¶	In terms of the quality of our products and/or services, we are…	.021*	5.62	5.29
$Perf_5$§	In terms of the quantity produced per employee, we are….	.000*	5.45	4.91
$Perf_6$¶	In terms of the quantity produced per employee, we are….	.001*	5.50	4.97
$Perf_7$§	In terms of customer satisfaction, we are…	.398	5.61	5.48
$Perf_8$¶	In terms of customer satisfaction, we are…	.214	5.66	5.47

Notes: *Indicates significant difference at $p < .05$.
†1 = Strongly disagree; 7 = Strongly agree.
‡1 = No breach at all; 7 = Very serious breach.
§1 = Well below target; 7 = Well above target.
¶1 = Far behind competition; 7 = Far above competition.

IMPLICATIONS

Managerial implications

Prior research suggests that the role of management is to develop strategies that improve organizational performance (Hunt and Morgan 1997). Our results suggest that a strategy to improve security via C-TPAT certification is associated with superior performance. C-TPAT-certified firms significantly outperform their non-C-TPAT counterparts with regard to security performance, resilience, and firm performance.

Executives can use this information to make informed decisions regarding the pursuit of C-TPAT certification. Any security effort comes at a cost. Obtaining and maintaining certification requires resources. The cost–benefit question of security is one that many firms struggle to answer. This research provides some

clarity as firms seek to justify C-TPAT certification and may aid efforts to gain buy-in for C-TPAT implementation. Results indicate that positive outcomes are associated when C-TPAT certification is achieved.

We found that private sector participants gain by implementing a PPP-based security program. Specifically, C-TPAT-certified firms more effectively meet the security expectations of their customers, are better at detecting security issues, and are more resilient when security issues do occur.

C-TPAT is related to resilience. C-TPAT helps firms prepare for security issues and certified firms are more readily prepared to respond to security incidents. A main component of C-TPAT is encouraging the creation and maintenance of contingency plans internally and externally among supply chain partners. C-TPAT forces companies to develop responses to security incidents, which may allow them to more quickly resume operations.

C-TPAT is related to firm performance. There are many factors that may cause firms to ignore issues of security altogether. These factors include the cost of security measures and firms' perception that they are low-risk (Williams et al. 2008). Results provide evidence that C-TPAT-certified firms enjoy higher performance than non-C-TPAT firms. Results indicate that C-TPAT-certified firms are significantly better at surpassing internal cost targets than their noncertified counterparts. Furthermore, C-TPAT firms are better able to meet internal performance targets and outperform the competition on quality and output per employee.

Results also hold potential implications for USG efforts to promote C-TPAT certification. Specifically, if C-TPAT-certified firms exhibit higher levels of performance, this information can be used to induce greater private sector participation. Mutually sharing risk and reward is key in any relationship. In this PPP, the government receives higher levels of security and protection from security threats. Private sector partners can experience improved performance along the measures presented heretofore.

Theoretical implications

This research proposes TCA as a theoretical basis to explain why a PPP was chosen as the preferred governance mechanism to achieve broad security implementation. The dynamic nature of the global supply chain and tendency of firms to save upfront costs by shirking security obligations would tend to suggest a hierarchical governance structure is in order and the USG should insource the security function. However, reality dictates it is financially infeasible and legally impossible to insource security of a system the size of the global supply chain. This necessitates the use of market-based principles where firms are certified based on their security processes (instead of measurable outcomes) and the extent to which they encourage supply chain partners to employ similar processes. The end result is a hybrid relational governance mechanism wherein the USG and industry collaborate for the betterment of all.

This research suggests that B2B relationships and PPPs share many of the same key success factors. For many firms, participating in a PPP may appear challenging or even unnecessary. However, the notion of relational security suggests that participating in a well-designed PPP is much like investing in an inter-firm relationship. Moreover, participating in a PPP like C-TPAT may indeed bring supply chain partners closer together as they will be forced to collaborate and share information in order to earn certification.

This research introduces relational security and illustrates C-TPAT's role as one indicator of relational security. C-TPAT establishes, cultivates, and maintains security exchanges between public and private parties. Results indicate these relationships are *successful*. C-TPAT's success was demonstrated through improved security, resilience, and firm performance. Without success, relational security does not exist. Demonstrated success is necessary to justify the resources necessary for relational security program maintenance to counter ongoing threats.

Relational security can be viewed within the context of normal accident theory (Perrow 1984), high reliability theory (Roberts 1990), and situational crime prevention (Cohen and Felson 1979) as presented in this study or discussed in Speier et al. (2011). Normal accident theory posits that disruptions are normal—and therefore inevitable—in complex supply chains under conditions of tight coupling. Tight coupling occurs when supply chain relationships are characterized by dependency. Conversely, high reliability theory seeks to explain why risky contexts, which should face frequent disruptions (i.e., carrier flight decks), are remarkably reliable. A key tenant of high reliability theory is that disruptions can be nearly eliminated through proper mitigation efforts and the creation of a safety culture is one such effort. Situational crime prevention is based on routine activity theory and argues that crime is the product of a motivated offender (e.g., terrorist or disgruntled employee), a vulnerable target (e.g., a shipment in transit), and an absent or insufficient guardian (e.g., a lack of security measures protecting the target). When these three factors are present at the same time and location, then a security event is likely to occur.

Firms are often engaged in complex global supply chains and dependent (i.e., tightly coupled) on their international partners. These international relationships are inherently risky and require relational security activities to mitigate security threats. Relational security highlights the need to share sensitive security information with supply chain partners. The firm must ingrain a security (i.e., safety) culture before they recognize the need to share this information. The information shared should partially focus on the identification of likely offenders, vulnerable targets, and potential locations where a security event could occur. Likely relational security partners include suppliers, customers, carriers, terminal/port operators, and government entities among others (Closs and McGarrell 2004). Forming close relational security ties with these parties will help create a supply chain-wide security culture, protect the benefits associated with dependency, and institute capable guardians to protect vulnerable targets against motivated offenders.

CONCLUSIONS

Limitations and future research

This research is limited by the use of survey methodology. Results indicate respondents' perceptions and may not reflect actual, quantifiable security performance. In addition, causal relationships were not hypothesized. Future research should seek to understand if C-TPAT directly influences outcomes such as secu-

rity performance, resilience, customer satisfaction, and firm performance. Also, additional research should specifically address how security programs, like C-TPAT, influence business purchasing decisions. Are industrial buyers willing to pay premiums to utilize C-TPAT-certified suppliers? If the answer is yes, then security programs like C-TPAT may certainly have a large role in industrial marketing initiatives.

Future research should further investigate relational security. This research should examine the antecedents of PPP and interfirm relational closeness including trust, commitment, communication, and opportunistic behavior. One particularly interesting investigation would involve the role of trust as it affects the extent to which firms monitor their suppliers' security measures. Theoretically, purchasing firms that trust their suppliers would feel less compelled to regularly engage in expensive monitoring activities. However, close relationships characterized by trust are expensive in terms of the amount of time and effort necessary for their formation and maintenance. Purchasing firms would theoretically only maintain such relationships with their most important suppliers of their most important products. If these suppliers, or their products, are of such importance, then the purchasing firm may actually monitor the supplier even more closely to prevent supply disruptions. Future research may also examine the antecedents of relational security exchanges between companies and their employees as well as employees and their coworkers.

Another promising line of relational security research would investigate factors that distinguish productive and effective security exchanges from those that are unproductive and ineffective. Distinguishing factors likely include trust, shared vision, executive commitment, communication, technology, and culture. The key PPP and B2B success factors presented in Table 2 may serve as a starting point.

It has been said that the role of government is to perform those functions that society is unable or unwilling to perform on its own. However, governments may lack the knowledge or authority to unilaterally accomplish certain goals without the participation of private entities. Given the scale and scope of the international supply chain, government efforts to increase security require a PPP, such as C-TPAT. Our research demonstrates that C-TPAT-certified firms outperform their noncertified counterparts in several important areas. To the extent that this comparative performance difference induces firms to gain or retain C-TPAT certification, and security risk is reduced, society as a whole benefits from more secure commerce.

APPENDIX

Table A1: Measurement Items

Variable	Item	Scale	Adapted from
BS_1	We have suffered a serious supply chain breach.	1-Strongly disagree; 7-Strongly agree	NEW
BS_2	When thinking about security breaches in the supply chain, we have suffered…	1-No breach at all; 7-Very serious breach	NEW
SP_1	Our firm effectively meets the security expectations of our customers.	1-Strongly disagree; 7-Strongly agree	NEW
SP_2	Our firm is able to effectively respond to security incidents that occur.	1-Strongly disagree; 7-Strongly agree	Voss et al. (2009b)
SP_3	Our firm has been successful in reducing the number of security incidents over time.	1-Strongly disagree; 7-Strongly agree	Voss et al. (2009b)
SP_4	Our firm is able to effectively detect security incidents before they become an issue.	1-Strongly disagree; 7-Strongly agree	Voss et al. (2009b)
R_1	We would quickly bounce back from a serious breach to our supply chain.	1-Strongly disagree; 7-Strongly agree	Williams et al. (2009b)
R_2	If a serious supply chain breach were to happen, we would return to normal operations in short order.	1-Strongly disagree; 7-Strongly agree	Williams et al. (2009b)
R_3	We are prepared for major unexpected supply chain disruptions.	1-Strongly disagree; 7-Strongly agree	Williams et al. (2009b)
R_4	We would not have problems with supply chain operations in the event of a significant supply chain breach.	1-Strongly disagree; 7-Strongly agree	Williams et al. (2009b)

Continued.

Table A1: Measurement Items (Continued)

Variable	Item	Scale	Adapted from
R_5	A serious breach in our supply chain would have little effect on our long-term supply chain operations.	1-Strongly disagree; 7-Strongly agree	Williams et al. (2009b)
R_6	We provide resources to create contingency plans for responding to supply chain breaches.	1-Strongly disagree; 7-Strongly agree	NEW
R_7	We are well prepared for recovering from major supply chain breaches.	1-Strongly disagree; 7-Strongly agree	NEW
R_8	We have detailed processes for resuming supply chain operations in the event of a breach.	1-Strongly disagree; 7-Strongly agree	NEW
R_9	We have a formal mechanism for identifying potential responses to emerging supply chain breaches.	1-Strongly disagree; 7-Strongly agree	NEW
In terms of…			
$Perf_1$	…the cost of producing our products and/or services, we are…	1-Well below target; 7-Well above target	Chattopadhyay et al. (2001)
$Perf_2$	…the cost of producing our products and/or services, we are…	1-Far behind competition; 7-Far above competition	Chattopadhyay et al. (2001)
$Perf_3$	…the quality of our products and/or services, we are…	1-Well below target; 7-Well above target	Chattopadhyay et al. (2001)
$Perf_4$	…the quality of our products and/or services, we are…	1-Far behind competition; 7-Far above competition	Chattopadhyay et al. (2001)
$Perf_5$	…the quantity produced per employee, we are….	1-Well below target; 7-Well above target	Chattopadhyay et al. (2001)
$Perf_6$	…the quantity produced per employee, we are….	1-Far behind competition; 7-Far above competition	Chattopadhyay et al. (2001)
$Perf_7$	…customer satisfaction, we are…	1-Well below target; 7-Well above target	Chattopadhyay et al. (2001)
$Perf_8$	…customer satisfaction, we are…	1-Far behind competition; 7-Far above competition	Chattopadhyay et al. (2001)

REFERENCES

Anderson, E. 1985. "The Salesperson as Outside Agent or Employee: A Transaction Cost Analysis." *Marketing Science* 4(Summer):234–54.

Arora, S., and Gangopadhayay, S. 1995. "Toward a Theoretical Model of Voluntary Overcompliance." *Journal of Economic Behavior and Organization* 28(3):289–309.

Autry, C.W., and Bobbitt, L.M. 2008. "Supply Chain Security Orientation: Conceptual Development and a Proposed Framework." *International Journal of Logistics Management* 19(1):42–64.

Autry, C.W., Grawe, S.J., Daugherty, P.J., and Richey, R.G. 2010. "The Effects of Technological Turbulence and Breadth on Supply Chain Technology Acceptance and Adoption." *Journal of Operations Management* 28(6):522–36.

Autry, C.W., Skinner, L.R., and Lamb, C.W. 2008. "Interorganizational Citizenship Behaviors: An Empirical Study." *Journal of Business Logistics* 29(2):53–74.

Bakir, N.O. 2008. "A Decision Tree Model for Evaluating Countermeasures to Secure Cargo at United States Southwestern Ports of Entry." *Decision Analysis* 5(4):230–48.

Bearden, W.O., and Haws, K.L. 2012. "How Low Spending Control Harms Consumers." *Academy of Marketing Science Journal* 40(1):181–93.

Beitelspacher, L.S., Richey, R.G., and Reynolds, K.E. 2011. "Exploring a New Perspective on Service Efficiency: Service Culture in Retail Organizations." *The Journal of Services Marketing* 25(3):215–28.

Bonney, J. 2011. "Cisco's Agnostic Resiliency." *Journal of Commerce* February 21:15.

Bowersox, D.J., Closs, D.J., and Stank, T.P. 1999. *21st Century Logistics: Making Supply Chain Integration a Reality*. Oak Brook, IL: Council of Supply Chain Management Professionals.

Braunsberger, K., Wybenga, H., and Gates, R. 2007. "A Comparison of Reliability Between Telephone and Web-Based Surveys." *Journal of Business Research* 60(7):758–64.

Chattopadhyay, P., Glick, W.H., and Huber, G.P. 2001. "Organizational Actions in Response to Threats and Opportunities." *The Academy of Management Journal* 44 (5):937–55.

Chernev, A., Hamilton, R., and Gal, D. 2011. "Competing for Consumer Identity: Limits to Self-Expression and the Perils of Lifestyle Branding." *Journal of Marketing* 75(3):66–82.

Christopher, M., and Lee, H. 2004. "Mitigating Supply Chain Risk Through Improved Confidence." *International Journal of Physical Distribution and Logistics Management* 35 (4):388–96.

Closs, D.J., and McGarrell, E.F. 2004. "Enhancing Security Throughout the Supply Chain." IBM Center for the Business of Government, http://www.businessofgovernment.org/report/enhancing-security-throughout-supply-chain, 1–52.

Closs, D.J., Speier, C., Whipple, J.M., and Voss, M.D. 2008. "Supply Chain Security: A Framework for Protecting Your Supply Chain." *Logistics Management* 47(9):45–6.

Coase, R.H. 1937. "The Nature of the Firm." *Economica* 4:386–405.

Cohen, L.E., and Felson, M. 1979. "Social Change and Crime Rate Trends: A Routine Activity Approach." *American Sociological Review* 44:588–605.

Craighead, C.W., Blackhurst, J., Rungtusanatham, M.J., and Handfield, R.B. 2007. "The Severity of Supply Chain Disruptions: Design Characteristics and Mitigation Capabilities." *Decision Sciences* 38(1):131–56.

Dennis, J.M. 2001. "Are Internet Panels Creating Professional Respondents?" *Marketing Research* 13(2):34–38.

Dwyer, R.F., Schurr, P.H., and Oh, S. 1987. "Developing Buyer-Seller Relationships." *Journal of Marketing* 52(April):21–34.

Eggers, W.D. 2004. "Prospering in the Secure Economy." A Deloitte Research Study, Deloitte Touche Tohmatsu, New York, NY, www.deloitte.com

Faisal, M.N., Banwet, D.K., and Shankar, R. 2006. "Supply Chain Risk Mitigation: Modeling the Enablers." *Business Process Management Journal* 12(4):535–52.

Fornell, C., and Larcker, D.F. 1981. "Evaluating Structural Equation Models With Unobservable Variables and Measurement Error." *Journal of Marketing Research* 18(1):39–50.

Furia, P., Rexrode, D., Il-Kim, Y., Lee, J., Ellis, J., and Guterbock, T.M. 2011. "Customs-Trade Partnership Against Terrorism: 2011 Costs and Savings Survey." University of Virginia Center for Survey Research, www.cbp.gov, 1–39.

Gonzalez, A. 2004. "Linking Supply Chain Security With Sarbanes-Oxley and the Bottom Line." ARC Advisory Group White Paper, www.ctl.ca

Grawe, S.J., Daugherty, P.J., and Roath, A.S. 2011. "Knowledge Synthesis and Innovative Logistics Processes." *Journal of Business Logistics* 32(1):69–80.

Heide, J.B. 1994. "Interorganizational Governance in Marketing Channels." *Journal of Marketing* 58(1):71–85.

Hendricks, K.B., and Singhal, V.R. 2005. "An Empirical Analysis of the Effect of Supply Chain Disruptions on Long-Run Stock Price Performance and Equity Risk of the Firm." *Production and Operations Management* 14(1):35–52.

Hodge, G.A., and Greve, C. 2007. "Public Private Partnerships: An International Performance Review." *Public Administration Review* 67(3):545–58.

Hoffman, D.L., Praveen, K.K., and Novak, T.P. 2010. "The 'Right' Consumers for Better Concepts: Identifying Consumers High in Emergent Nature to Develop New Product Concepts." *Journal of Marketing Research* 47(5):854–65.

Hunt, S.D., and Morgan, R.M. 1997. "Resource-Advantage Theory: A Snake Swallowing Its Tail or a General Theory of Competition?" *Journal of Marketing* 61(4):74–82.

Jack, E.P., Powers, T.L., and Skinner, L. 2010. "Reverse Logistics Capabilities: Antecedents and Cost Savings." *International Journal of Physical Distribution and Logistics Management* 40(3):228–46.

Jacobson, C., and Choi, S.O. 2008. "Success Factors: Public Works and Public Private Partnerships." *International Journal of Public Sector Management* 21(6):637–57.

Jap, S.M. 1999. "Pie-Expansion Efforts: Collaboration Processes in Buyer-Supplier Relationships." *Journal of Marketing Research* 36(4):461–75.

Kees, J., Burton, S., Andrews, J.C., and Kozup, J. 2010. "Understanding How Graphic Pictorial Warnings Work on Cigarette Packaging." *Journal of Public Policy and Marketing* 29(2):265–76.

Kleindorfer, P.R., and Saad, G.H. 2005. "Managing Disruption Risks in Supply Chains." *Production and Operations Management* 14(1):53–68.

Knemeyer, A.M., and Naylor, R.W. 2011. "Using Behavioral Experiments to Expand Our Horizons and Deepen Our Understanding of Logistics and Supply Chain Decision Making." *Journal of Business Logistics* 32(4):296–302.

Lado, A., Boyd, N.G., and Hanlon, S.C. 1997. "Competition Cooperation and the Search for Economic Rents: A Syncretic Model." *Academy of Management Review* 22(1):110–41.

Leana, C.R., and Pil, F.K. 2006. "Social Capital and Organizational Performance: Evidence From Urban Public Schools." *Organization Science* 17(3):353–416.

Lee, H.L., and Whang, S. 2003. "*Higher Supply Chain Security With Lower Cost: Lessons from Total Quality Management*." Research paper No. 1824, Stanford University, Stanford CA, October.

Lee, H.L., and Wolf, M. 2003. "Supply Chain Security Without Tears." *Supply Chain Management Review* 7(1):12–20.

Maronick, T.J. 2009. "The Role of the Internet in Survey Research: Guidelines for Researchers and Experts." *Journal of Global Business and Technology* 5(18):18–31.

McCutcheon, D., and Stuart, F.I. 2000. "Issues in the Choice of Supplier Alliance Partners." *Journal of Operations Management* 18(3):279–301.

Morgan, R.M., and Hunt, S.D. 1994. "The Commitment-Trust Theory of Relationship Marketing." *Journal of Marketing* 58 (3):20–38.

Murphy, S. 2008. "Stepping Up Security: An Interview With James Williams." *Supply Chain Management Review* 12(8):8.

NCPPP: National Center for Public-Private Partnerships. 2008. "Public-Private Partnerships Defined." www.ncppp.org/howpart/index.shtml#define

Netemeyer, R.G., Bearden, W.O., and Sharma, S. 2003. *Scaling Procedures: Issues and Applications*. Thousand Oaks, CA: Sage Publications.

Nunnally, J.C., and Bernstein, I.H. 1994. *Psychometric Theory*. 3rd ed. New York: McGraw-Hill.

Oliver, J.D., and Rosen, D.E. 2010. "Applying the Environmental Propensity Framework: A Segmented Approach to Hybrid Electric Vehicle Marketing Strategies." *Journal of Marketing Theory and Practice* 18(4):377–93.

Palmeira, M., and Thomas, D. 2011. "Two-Tier Store Brands: The Benefic Impact of a Value Brand on Perceptions of a Premium Brand." *Journal of Retailing* 87(4):540–48.

Peleg-Gillai, B., Bhat, G., and Sept, L. 2006. "Innovators in Supply Chain Security: Better Security Drives Business Value." Stanford University and The Manufacturing Institute, 1–34.

Perrow, C. 1984. *Normal Accidents: Living With High-Risk Technologies*. New York: Basic Books.

Pettit, T.J., Fiksel, J., and Croxton, K.L. 2010. "Ensuring Supply Chain Resilience: Development of a Conceptual Framework." *Journal of Business Logistics* 31(1):1–21.

Pollard, W.E. 2002. "Use of Consumer Panel Survey Data for Public Health Communication Planning: An Evaluation of Survey Results." *American Statistical Association 2002 Proceedings of the Section on Health Policy Statistics* 2720–24.

Prokop, D. 2004. "Smart and Safe Borders: The Logistics of Inbound Cargo Security." *International Journal of Logistics Management* 15(2):65–75.

Rice, J.B., and Caniato, F. 2003. "Building a Secure and Resilient Supply Network." *Supply Chain Management Review* 7(5):22–30.

Richey, R.J., Jr., Tokman, M., and Dalela, V. 2010. "Examining Collaborative Supply Chain Service Technologies: A Study of Intensity, Relationships, and Resources." *Journal of the Academy of Marketing Sciences* 38(1):71–89.

Rindfleisch, A., and Heide, J.B. 1997. "Transaction Cost Analysis: Past, Present, and Future Applications." *Journal of Marketing* 61(4):30–54.

Ritchey, D. 2011. "Leading With Resiliency During a Natural Disaster." *Security Magazine* 48(3):46–52.

Roberts, K.H. 1990. "Some Characteristics of One Type of High Reliability Organization." *Organization Science* 1(2):160–76.

Russell, D.M., and 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.

Shang, J., Basil, D.Z., and Wymer, W. 2010. "Using Social Marketing to Enhance Hotel Reuse Programs." *Journal of Business Research* 63(2):166–72.

Sheffi, Y. 2001. "Supply Chain Management Under the Threat of International Terrorism." *International Journal of Logistics Management* 12(2):1–11.

Sheu, C., Lee, L., and Niehoff, B. 2006. "A Voluntary Logistics Security Program and International Supply Chain Partnership." *Supply Chain Management: An International Journal* 11(4):363–74.

Soster, R.L., Monga, A., and Bearden, W.O. 2010. "Tracking Costs of Time and Money: How Accounting Periods Affect Mental Accounting." *Journal of Consumer Research* 37 (4):712–21.

Speier, C., Whipple, J.M., Closs, D.J., and Voss, M.D. 2011. "Global Supply Chain Design Considerations: Mitigating Product Safety and Security Risks." *Journal of Operations Management* 29(7/8):721–36.

Stewart, G., Kolluru, R., and Smith, M. 2009. "Leveraging Public Private Partnerships to Improve Community Resilience in Times of Disaster." *International Journal of Physical Distribution and Logistics Management* 39(5):343–64.

Szakonyi, M. 2013. "Custom's C-TPAT Goal: Show 'Em the Money." *Journal of Commerce* January 21:18.

Thomas, R. 2011. "When Student Samples Make Sense in Logistics Research." *Journal of Business Logistics* 32(3):287–90.

U.S. Customs and Border Protection. 2004. "Securing the Global Supply Chain: Customs-Trade Partnership Against Terrorism Strategic Plan." www.cbp.gov, 1–38.

U.S. Customs and Border Protection. 2013. "C-TPAT Program Achievements." http://www.cbp.gov/xp/cgov/trade/cargo_security/ctpat/ctpat_news_reports/

Van Ham, H., and Koppenjan, J. 2001. "Building Public-Private Partnerships: Assessing and Managing Risks in Port Development." *Public Management Review* 4(1):593–616.

Voss, M.D., Closs, D.J., Calantone, R.J., Helferich, O.K., and Speier, C. 2009a. "The Role of Security in the Food Supplier Selection Decision." *Journal of Business Logistics* 30(1):127–55.

Voss, M.D., Page, T.J., Keller, S.B., and Ozment, J. 2006. "Determining Important Carrier Attributes: A Fresh Perspective Using the Theory of Reasoned Action." *Transportation Journal* 45(3):7–19.

Voss, M.D., Whipple, J.M., and Closs, D.J. 2009b. "The Role of Strategic Security: Internal and External Security Measures With Security Performance Implications." *Transportation Journal* 48(2):5–23.

Wathne, K.H., and Heide, J.B. 2000. "Opportunism in Interfirm Relationships: Forms, Outcomes, and Solutions." *Journal of Marketing* 64(4):36–51.

Wettenhall, R. 2003. "The Rhetoric and Reality of Public-Private Partnerships." *Public Organization Review* 3(1):77–107.

Whipple, J.M., Voss, M.D., and Closs, D.J. 2009. "Supply Chain Security Practices in the Food Industry: Do Firms Operating Globally and Domestically Differ." *International Journal of Physical Distribution and Logistics Management* 39(7):574–94.

Williams, Z., Lueg, J.E., and LeMay, S.A. 2008. "Supply Chain Security: An Overview and Research Agenda." *International Journal of Logistics Management* 19(2):254–81.

Williams, Z., Lueg, J.E., Taylor, R.D., and Cook, R.L. 2009a. "Why All the Changes? An Institutional Theory Approach to Exploring the Drivers of Supply Chain Security." *International Journal of Physical Distribution and Logistics Management* 39(7):595–618.

Williams, Z., Ponder, N., and Autry, C.W. 2009b. "Supply Chain Security Culture: Measure Development and Validation." *International Journal of Logistics Management* 20(2):243–60.

Williamson, O. 1985. *The Economic Institutions of Capitalism*. New York: Free Press.

Zelbst, P.J., Green, K.W., Sower, V.E., and Reyes, P.M. 2012. "Impact of RFID on Manufacturing Effectiveness and Efficiency." *International Journal of Operations and Production Management* 32(3):329–50.

Zsidisin, G.A. 2003. "A Grounded Definition of Supply Risk." *Journal of Purchasing and Supply Management* 9(5–6):217–24.

Zsidisin, G.A., and Ellram, L.M. 2003. "An Agency Theory Investigation of Supply Risk Management." *The Journal of Supply Chain Management: A Global Review of Purchasing and Supply* 39(3):15–27.

SHORT BIOGRAPHIES

M. Douglas "Doug" Voss (PhD Michigan State University) is an Associate Professor of Logistics and Supply Chain Management at the University of Central Arkansas and Director of the Center for Logistics Education, Advancement, and Research (CLEAR). Doug received his PhD in logistics. He also has an MS and BS in Transportation and Logistics Management from the University of Arkansas. Before beginning his position at the University of Central Arkansas, Doug served as a post-doctoral research associate at Michigan State University and also worked in the motor carrier industry. His research has appeared in numerous publications and received best paper awards from the *Journal of Operations Management*, Midwest Decision Sciences Institute, and CSCMP's Educator's Conference.

Zachary Williams (PhD Mississippi State University) is Associate Professor of Marketing and Logistics and a Jerry and Felicia Campbell Endowed Professor for Research at Central Michigan University. He received his PhD in marketing, with focus on supply chain management. His doctoral research on supply chain security was recognized with awards from the Institute for Supply Management and the Supply Chain Management Research Center in the Sam Walton College of Business at the University of Arkansas. His research interests are focused on three areas: supply chain security and disaster response; customer satisfaction and segmentation with logistics services; and the growth and development of logistics professionals. His research on these areas has lead to a breadth of academic publications, including top journals such as: *Journal of Business Logistics, International Journal of Logistics Management,* and *International Journal of Physical Distribution and Logistics Management,* among others.