University of Central Arkansas
Interlibrary Loan

Torreyson Library
Phone: 501.450.5205
Email: ill@uca.edu
Web: www.uca.edu/library

Electronic Delivery Cover Sheet

Notice: Document Quality

To expedite the delivery of some electronic documents, the UCA Interlibrary Loan (ILL) staff allows electronic deliveries to be sent directly from the lender to you without review from the UCA ILL staff. This process allows for the delivery of documents at any time including times the UCA ILL office is closed. However, the process can also allow for the possibility of incorrect documents, poorly scanned images, missing pages, etc. If you are not satisfied with the quality of your electronically delivered document, please contact the UCA ILL office by phone at 501.450.5205 or email at ill@uca.edu to request a replacement.

Warning Concerning Copyright Restrictions

The copyright law of the United States (Title 17, U.S. Code) governs the making of photocopies or other reproductions of copyrighted material. Under certain conditions specified in the law, libraries and archives are authorized to furnish a photocopy or other reproduction. One of these specified conditions is that the photocopy or reproduction is not to be "used for any purpose other than private study, scholarship, or research." If a user makes a request for, or later uses a photocopy or reproduction for purposes in excess of "fair use," that user may be liable for copyright infringement. Copyright law limits the number of articles photocopied to five from any given periodical published in the previous five calendar years. This institution reserves the right to refuse to accept a copy order if, in its judgment, fulfillment of the order would involve violation of the copyright law.

Journal of Operations Management 29 (2011) 721–736

Contents lists available at ScienceDirect

Journal of Operations Management

journal homepage: www.elsevier.com/locate/jom

Global supply chain design considerations: Mitigating product safety and security risks

Cheri Speier[a,*], Judith M. Whipple[b,1], David J. Closs[c,2], M. Douglas Voss[d,3]

[a] Information Systems, Michigan State University, N215 Eli Broad College of Business, East Lansing, MI 48824, United States
[b] Logistics, Michigan State University, N 325 Eli Broad College of Business, East Lansing, MI 48824, United States
[c] John H. McConnell Professor of Business Administration, Michigan State University, N 370 Eli Broad College of Business, East Lansing, MI 48824, United States
[d] Logistics, University of Central Arkansas, 201 Donaghey Avenue, Conway, AR 72035, United States

ARTICLE INFO

Article history:
Available online 28 June 2011

Keywords:
Supply chain
Risk
Safety

ABSTRACT

Supply chain disruptions pose an increasingly significant risk to supply chains. This research develops a framework to examine the threat of potential disruptions on supply chain processes and focuses on potential mitigation and supply chain design strategies that can be implemented to mitigate this risk. The framework was developed by integrating three theoretical perspectives—normal accident theory, high reliability theory, and situational crime prevention. The research uses a multi-method approach to identify key safety and security initiatives (process management, information sharing, and supply chain partner and service provider relationship management) that can be implemented and the conditions under which each initiative is best suited. The research results illustrate that the depth and breadth of security initiatives depends on top management mindfulness, operational complexity, product risk, and coupling.

1. Introduction

Over the last few years, academics and practitioners alike have increasingly focused on supply chain disruptions and the impact of such disruptions on supply chain design decisions, product safety and security, and financial health (Blackhurst et al., 2005; Craighead et al., 2007; Elkins et al., 2005; Hendricks and Singhal, 2003, 2005; Kleindorfer and Saad, 2005; Rice and Caniato, 2003; Tang, 2006). A great deal of this work has focused on addressing what types of disruptions occur. For example, while supply chain disruptions may result from a variety of unintentional causes such as accidents or natural disasters (Kleindorfer and Saad, 2005), there can also be intentional supply chain disruptions. Intentional disruptions may include theft, contamination/sabotage, or a terrorist attack.

Various examples of unintentional supply chain disruptions exist. Many of these disruptions occur naturally including hurricanes, tornados, floods, and may disrupt a supply chains' transportation infrastructure, supply routes, and/or manufacturing facilities. Unintentional disruptions can also be man-made. An accident (e.g., transportation-oriented, injury) could cause transportation delays or production stoppages or could negatively impact product quality (e.g., contamination). Unintentional contamination events occur with some frequently in the food industry. The Center for Disease Control estimates that on an annual basis, unintentional contamination of food results in 76 million illnesses, 325,000 hospitalizations and 5000 deaths just in the United States (Mead et al., 1999).

Unfortunately, many disruptions have been the result of intentional acts which, like any type of disruption, can range in severity. Theft, for example, can significantly increase a firm's costs, but can also shut down a source of supply as has occurred with increased incidents of piracy on the open seas. There have also been a number of events involving deliberate contamination of product. In 1984, a religious cult intentionally contaminated salad bars in restaurants with a form of salmonella throughout the United States which resulted in 751 cases of illness; the initial attack was designed as a trial for a broader attack that would involve a strain of salmonella causing typhoid fever (World Health Organization, 2008). Increasingly, business entities are an attractive target for intentional sabotage given that 80% of terrorist attacks against U.S. interests over the last thirty years targeted businesses

* Corresponding author. Tel.: +1 517 355 7448.
E-mail addresses: cspeier@bus.msu.edu (C. Speier), whipple@bus.msu.edu (J.M. Whipple), closs@bus.msu.edu (D.J. Closs), voss@bus.msu.edu (M.D. Voss).
[1] Tel.: +1 517 432 6407.
[2] Tel.: +1 517 353 6381; fax: +1 517 432 1112.
[3] Tel.: +1 501 450 3149; fax: +1 501 450 5302.

0272-6963/$ – see front matter © 2011 Elsevier B.V. All rights reserved.
doi:10.1016/j.jom.2011.06.003

(Dobie et al., 2000). The terrorist attacks in the U.S. on September 11, 2001 represent an intentional disruption with catastrophic impact.

Supply chain disruptions, whether intentional or unintentional, have significant negative impact on both short and long-term operations and financial performance (Kleindorfer et al., 2003). Such disruptions have been demonstrated to decrease shareholder value by almost 11% (Hendricks and Singhal, 2003) and firms, on average, experience a 40% decline in stock price following a disruption (Hendricks and Singhal, 2005). Negative consequences associated with supply chain disruptions extend beyond direct financial impacts. Disruptions can also result in an erosion of brand equity, loss of consumer confidence, and may have legal ramifications. Additionally, disruptions that impact product quality can result in product recalls which create the need for costly reverse supply chain activities. Finally, supply chain disruptions may result in the introduction of government regulations (Ravi, 2006). Even with growing evidence regarding the tremendous negative impact of supply chain disruptions, many firms have difficulty fully assessing the potential for a supply chain disruption, and often under-invest in sustainability capabilities to respond to disruptions (Hauser, 2003). Additionally, Chopra and Sodhi (2004) acknowledge that firms often focus on reoccurring, but low impact risks with less focus on high-impact, but less probable risks (e.g., catastrophic intentional events).

Since supply chains are vulnerable to both unintentional and intentional actions, a better understanding of disruption mitigation and supply chain design strategies is critical for both practitioners and researchers. In particular, this research examines supply chain disruptions in three high risk areas-food, pharmaceutical, and hazardous materials – and focuses specifically on supply chain interventions that can improve product safety and security. Qualitative data was collected within all three high risk industry sectors and in-depth empirical data was collected in the food industry. As such, this research uses a multi-method approach to examine types of mitigation and supply chain design strategies that can be implemented within a supply chain and contingencies that impact which strategies are selected. The research offers recommendations to enhance supply chain security.

Following this introduction, this research is organized into five sections. The first section develops a framework examining the role of disruptions on supply chain design. Next, testable hypotheses are developed and results from exploratory and qualitative data analysis are used to illustrate these hypotheses. A quantitative methodological approach is described for testing the hypotheses followed by qualitative insights that offer explanation for the quantitative results. Finally, conclusions and future research directions are provided.

2. Literature review

This section reviews and integrates three research themes resulting in a framework describing the influence of disruptions on supply chains.

2.1. Examining disruptions: impact on supply chain design

Supply chain design decisions have historically focused on "where" to locate facilities (e.g., plants, warehouses) (Greenhut, 1959; Hoover, 1948; Losch, 1954). The primary objective was to minimize the total cost of transportation. With the advent of integrated logistics, integrated manufacturing, and strategic procurement, the perspective broadened to focus on minimizing the total landed cost and included considerations such as material acquisition, production, inventory, and logistics (Bowersox et al., 2006).

Supply chain design objectives have extended beyond cost. The concept of segmental customer service requirements has evolved and suggests that firms need multiple supply chains to meet the unique service requirements of different customer segments while also operating within required cost parameters. The philosophy of this era was not to simply minimize total delivered cost, but, also to understand that design strategies could be created to meet delivery requirements in terms of both time and availability.

More recently, supply chain design objectives have extended even further to include supply chain security, risk, and sustainability dimensions. The security and risk terminologies have been used somewhat interchangeably in supply chain research to date, but the emergent literature is beginning to reveal that these constructs are conceptually different. *Supply chain security* entails the prevention of contamination, damage, or destruction of products and/or supply chain assets, and includes an acknowledgement that these events may occur from intentional and unintentional disruptions (Closs and McGarrell, 2004). Alternatively, *supply chain risk* is defined as the extent to which supply chain outcomes are variable or are susceptible to disruption, and, thus, may be detrimental to a supply chain (Zsidisin et al., 2005). A variety of supply chain risks have been identified including supply disruptions, breakdowns, procurement failures, and forecast inaccuracies (Chopra and Sodhi, 2004; Harland et al., 2003; Johnson, 2001; Spekman and Davis, 2004; Zsidisin, 2003), and, as previously stated, much of the risk management literature has focused on lower-impact, unintentional events. *Supply chain sustainability* refers to a supply chain's ability to operate without interruption due to constraints in facilities, resources, and capacity. Thus, *security* measures are put in place to *protect* the supply chain against potential *risks*, including intentional events. These security measures should defend against such risks and, thus, may prevent (or minimize the negative impact) of these risks from occurring, thereby, increasing supply chain sustainability.

The challenges associated with supply chain safety and security, particularly resulting from intentional acts, are significant. Much of the supply chain is unguarded and only the most visible parts (e.g., individual facilities) are regularly protected. It is estimated that the movement of a single container may involve as many as twenty-five different entities to transport the container from seller to buyer (through customs, inland transportation, international shipping, etc.) (The Economist, 2002). Furthermore, the breadth of supply chain infrastructure makes total protection difficult. The U.S. domestic infrastructure includes roughly 47,000 miles of interstate highways, 99,000 miles of Class I railroad track, 26,000 miles of navigable waterways, 64,000 miles of oil pipeline, 5200 airports, and 9400 commercial waterway facilities (United States Department of Transportation, 2005). Finally, the sheer magnitude of global commerce presents a significant hurdle. Ninety percent of international trade, and almost one-half of U.S. imports, are transported via cargo containers (United States Customs and Border Protection, 2004), and represents almost nine million containers unloaded annually in the United States.

Beyond the size and scope of the infrastructure, there are significant costs associated with protecting the supply chain. The cost of supply chain defense and security is anticipated to exceed US$ 151 billion annually (Russell and Saldanha, 2003). Further, Sheffi (2001) posits that supply chains will incur cost and service penalties because of conflicts between security and business goals. For example, a firm within a supply chain may have to trade- off between a higher priced supplier with a proven quality record and a lower priced supplier that may offer a lesser quality product. Supply chains may be redesigned to apply more resilient

transportation capabilities (e.g., use of air freight to reduce variability associated with delivery lead-times, outsourcing to firms in more stable countries of origin, or considering alternative ports of entry to avoid port congestion) to enable more sustainable delivery. Additionally, additional inventory may be carried at different sources within the supply chain to buffer against potential disruptions.

2.2. Normal accident and high reliability theory: implications for security

Normal accident theory (NAT) and high reliability theory (HRT) provide a backdrop from which to examine supply chain disruptions and the factors, including supply chain design, which can mitigate such disruptions. Both NAT and HRT have developed robust research streams across business, healthcare, sociology, and other academic disciplines (Sagan, 1993; Weick, 2004; Wolf, 2001, 2005). While these theories have not been widely employed to frame supply chain research, their focus on normal accidents and organizational reliability provide a meaningful lens from which to examine supply chain disruptions. NAT and HRT will be briefly described and then the complementary aspects of each will be discussed to frame the theoretical lens implemented in this research.

Normal accident theory (NAT) was developed from an in-depth analysis of the Three Mile Island nuclear plant disaster and suggests that accidents are inevitable, and therefore normal, when two conditions exist-tight coupling and complex interactions (Perrow, 1984, 1999). Tight coupling occurs when supply chains have components (e.g., participating firms, processes, such as just-in-time deliveries) that are highly interdependent. Tight coupling also involves very little, if any, process slack or buffering of product/people/etc. Thus, when processes, components, and organizations are tightly coupled, the potential for an incident increases while the time available for recovery from that incident diminishes (Perrow, 1994; Rijpma, 2003). Similarly, a supply chain with loose coupling typically has excess slack, buffering, and time designed into activities, potentially facilitating faster recovery or possibly no negative impact should a disruption occur (Perrow, 1984).

An organization experiences complex interactions within its supply chain when underlying processes involve unanticipated and/or unfamiliar events, where such events are not clearly visible, and when the impact of events on underlying processes cannot be immediately nor fully comprehended (Perrow, 1994). These interactions between normal processes and events may make it difficult to easily access information about products and processes, and may create unintended consequences because of the difficulty associated with isolating activities to a single process or organization (Perrow, 1994). While NAT (and HRT) discuss complexity as the complexity of interactions, the label supply chain complexity is used in subsequent sections of this paper. Thus, supply chain complexity will focus on the inherent complexity in a focal firm's marketplace as it sells goods and services from local (least complex) to global (more complex) marketplace.

NAT can be expanded to the realm of supply chain disruptions – not only are unintentional "accidents" inevitable, but also, intentional events may prove inevitable (e.g., theft). Tight coupling, which occurs via interdependence and synchronization among supply chain members, potentially affords an opportunity for greater damage from an intentional event. Given the previous discussion regarding the number of handoffs and the vast complexity of the global supply chain network, complex interactions certainly exist within many supply chains as well.

In a similar way *high reliability theory* (HRT) focuses on the processes that a firm can implement to ensure continued organizational reliability and reduce or even eliminate the possibility of accidents (Roberts, 1990a,b). Much of the research in this stream has focused on specific organizations in accident-prone/hazardous industries (defined as those that are tightly coupled and having complex interactions) to identify specific organizational practices that increase reliability. Thus, HRT research has focused on organizations in industries that could experience a significant failure with dramatic consequences, but had not – in other words, the organization has proven itself to be highly reliability despite its high risk environment. Examples of such entities include nuclear power plants, aircraft carriers, and air traffic control. This is not meant to suggest that these entities are not error or incident free. Rather, what makes high reliability organizations different is that they have a tremendous capacity to respond to such incidents in a way that is not disabling, and, then, to learn from and restructure their procedures to mitigate similar future incidents and avoid dramatic failures (Weick and Sutcliffe, 2001). For example, McFadden et al. (2009) used HRT to examine patient safety in hospitals and found leadership commitment and a safety culture positively impacted safety initiatives and safety outcomes. The importance of leadership commitment to and visibility around key security initiatives is a key theme to acknowledge here and will be brought up again in subsequent sections. We have labeled the role of leaders in creating a culture around security as one of mindfulness-creating visible awareness about the importance of securing the supply chain.

HRT also has implications for intentional events as illustrated by changes in the airline industry since September 11th and other airline terrorist incidents. Policy changes regarding carry-on restrictions serve as an example of a joint attempt by the airline industry and the federal government to put into place an immediate response to reduce the potential of terrorist activities and to make such a response a standard check-in process in an effort to prevent further attacks. Other examples that highlight the HRT theory include information technology and information security systems. As computer "hackers" become more savvy and design/transmit more elaborate viruses or other disruptive actions, computer software programs must also respond by preventing intentional actions that would compromise personal information. From an HRT perspective, the reliability of a supply chain can be enhanced to better protect against disruptions – whether such disruptions are intentional or unintentional. As an example of HRT applied to unintentional events, firms have developed contingency plans for alternative production facilities and/or delivery routes in response to natural disasters and/or may hold more inventory as buffer stock (e.g., during hurricane season).

While NAT and HRT have spawned broad research streams and examined different facets of "accidents" there is a growing body of literature describing the complementary nature of these theories (LaPorte, 1994a,b; Rijpma, 1997). These researchers describe the intersection of NAT and HRT as a focus on the protection mechanisms that firms and (from our perspective supply chains) can put in place to best respond to organizational and (supply chain) disruption. This complementary view stems from both theories focusing on accident prevention—NAT from a system design and risk mitigation perspective and HRT from an integration of organizational practice perspective. As such, the intersection between theories has traction for supply chain disruption research by extending NAT beyond "normal" accidents to include intentional incidents while using the ideas of HRT incorporating learning from disruptions into the continuous supply chain design improvement process (Rijpma, 1997).

Additionally, HRT posits that specific supply chains are at particular risk for disruption and, thus, have a greater impetus in developing a high degree of organizational reliability. This complementary perspective is consistent with recent supply chain literature describing the need for both a secure and a resilient supply chain because prevention of disruptions may not always be possible (Sheffi and Rice, 2005). Table 1 compares elements of NAT

Table 1
Normal accident and high reliability theory.

	Normal accident theory	High reliability theory
General premise	Accidents are normal and will occur although steps can be taken to minimize occurrence (Perrow, 1984)	Accidents are preventable (Roberts, 1990a, 1990b).
Conceptual framing	Theory on the causation (complex interactions and coupling) of specific types of accidents (Rijpma, 1997)	Identifies organizational strategies to reduce potential problems and promote organizational reliability (Weick, 1987)
Nature of research	Primarily industry or specific incident focus with emphasis on restructuring high risks environments (Tenner, 1997)	Focus on organizational practices and culture that promote reliability (Roberts, 1990a, 1990b)
Perspectives on tight coupling	Failures can escalate out of control before intervention can occur (Perrow, 1994; Rijpma, 2003).	Tight coupling can be mitigated using different strategies (LaPorte and Consolini, 1991): Time pressure → redundancy Insufficient slack → bargaining and negotiation, system flexibility
Perspectives on complex interactions	*Increased complexity among systems creates the potential for an independent event to interact in ways that can not be foreseen by designers or understood by operators (Perrow, 1994)*	Complexity can be mitigated using different strategies (Weick and Sutcliffe, 2001) Technological complexity → continuous training, responsibility and accountability, and decentralized decision making Interaction complexity → training and socialization; informal networks for solving problems; redundancy; empowerment of employees to intervene in situation Information Source Complexity → use of direct information sources

and HRT in order to describe characteristics associated with supply chain reliability.

2.3. Integrating crime prevention and the disaster management process with NAT/HRT

To more fully shape the NAT/HRT perspective, this research also integrates the notion of situational crime prevention from the criminal justice literature. This is an important perspective as it provides a lens to more fully understand intentional acts of disruption. Situational crime prevention provides an important backdrop to more fully understand intentional threats and to help a supply chain identify corresponding security and protection approaches. Situational crime prevention builds upon routine activity theory (Cohen and Felson, 1979) which argues that the motivation for crime (economic or psychological benefits) is largely invariant but what does vary are criminal opportunities, generated through the intersection of motivated offenders and vulnerable targets accessible in specific locations.

Situational crime prevention builds upon these principles and generates a simple, but powerful formula: crime is the product of the confluence in space and time of motivated offenders, vulnerable victims or targets, and the absence of effective guardians. Prevention seeks to make criminal acts less attractive or feasible for offenders by manipulating some combination of offender motivation, vulnerability of targets, and presence of effective guardians (Clarke, 1995, 1997). Applied in the context of a number of public and private settings, situational crime prevention interventions have been shown to consistently prevent crime (Eck and Weisburd, 1995; Felson and Clarke, 1997; Clarke, 1997). As such, whether an intentional event is inevitable (NAT) or preventable (HRT) is not the core issue. Situational crime prevention assumes that, given sufficient motivation, criminal attempts are inevitable without proper protection mechanisms in place.

In the context of situational crime prevention, prevention from intentional action requires that attention be given to at least one of the three possible prevention levers: the likely offender (e.g., terrorist); a suitable target (a specific object-product or container that can be attacked, transportation network, manufacturing facility); and/or a physical location where the attack can occur (Felson and Clarke, 1998). Thus, an intentional action can only occur when there is a highly motivated offender, a suitable target at an available location, and/or an absent or insufficient guardian. Guardianship includes routine precautions that individuals and supply chains take to safeguard employees, products, capital investments, and business processes from intentional acts. As potential offenders, targets, and locations become salient, supply chains can implement specific actions in an effort to mitigate or prevent an intentional disruption.

The Disaster Management Process (Helferich and Cook, 2003) can be overlapped with the situation crime prevention theory to develop a framework of supply chain security as shown in Fig. 1. Organizations that are able to appropriately prevent, detect,

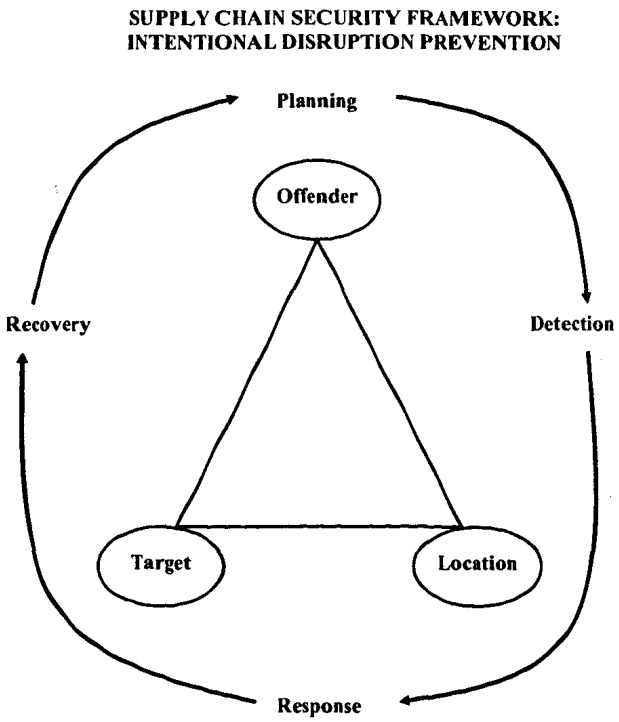

Fig. 1. Supply chain security framework: intentional disruption prevention.

respond and recover from a security incident occurring anywhere within the supply chain have created a resiliency (potentially through supply chain design capabilities) to ensure sustainable supply chains (Christopher and Peck, 2004; Sheffi, 2005). The disaster management process consists of four stages (planning, detection, response and recovery) and documents the actions a supply chain should undertake before, during, and after a security incident (Helferich and Cook, 2003). *Planning* represents the supply chain's efforts to formulate actions in anticipation of an incident. *Detection* is the supply chain's ability to recognize an incident. While some incidents are easy to detect (e.g., a container seal broken), others are not (e.g., contamination of food with a biological agent that goes undetected). The real challenge of detection is to ascertain that an incident has occurred prior to it doing any harm. The *response* stage begins as soon as the incident is detected and reflects short-term responses including mobilizing equipment to respond to the emergency, removing people from danger, providing for those affected by the incident, and bringing necessary services and systems back on-line. *Recovery* involves the long-term efforts necessary to get the supply chain started again and often places the most strain on involved parties.

Note that the disaster management process, while applied in Fig. 1 to intentional disruptions, can also be applied to unintentional disruptions. In other words, supply chains could plan around potential natural disasters (e.g., hurricanes) by creating contingencies (e.g., when hurricanes of a certain magnitude are detected, product is re-routed through buyer/seller distribution centers, or port of entry) as an appropriate response to the potential disaster after which normal recovery plans resume.

2.4. Qualitative analysis to conceptualize hypotheses and evaluate theoretical foundations

Given the focus of this paper was to extend the research on safety and security, a multi-methodological approach was taken. The first stage of research was to employ an inductive method using a grounded theory approach to examine the aforementioned theoretical foundations in order to assess the potential validity of the theoretical lens. Grounded theory approaches focus on the systematic gathering and analysis of data to derive theory (Strauss and Corbin, 1998) and have been widely used in marketing and supply chain research (Gebhardt et al., 2006; Giunipero et al., 2006; Malshe and Sohi, 2009; Mellos and Flint, 2009).

A grounded theory approach to studying a phenomenon is designed to build theory directly from data collected from the field (e.g., interviews, document analysis, etc.). While there are some divergent views on how to best implement grounded theory approaches (Glaser, 2001; Strauss and Corbin, 1998), the implementation of a strong data coding mechanism to help researchers develop their interpretations is an important component to the methodological process (Strauss and Corbin, 1998). The grounded theory research methodology is often applied when a research phenomenon is in a relatively early stage of development and/or to address a complex issue with significant variation in making sense of the phenomenon (Glaser and Strauss, 1967; Strauss, 1987).

Once key themes emerged from the qualitative analysis, the research team developed a survey instrument to collect data from a broader array of firms where this data could be assessed using empirical methods. While both the qualitative and quantitative approaches offer strengths and weaknesses in examining a phenomenon, we believe that using both approaches to examine safety and security issues in supply chain design is particularly important given the relative nascent research focused in this area.

2.5. Data collection

Setting: data were collected from large and small firms in the food, pharmaceutical, and hazardous materials industries. These industries and the associated supply chains were selected based on expectations that there would be significant differences in the potential for disruptions, the impact of such disruptions, and the visible application of disaster management processes.

Methods: The grounded theory approach encourages the use of multiple sources of data –interviews, observation, documents, etc. to capture a breadth of issues and to understand these issues in context (Glaser, 2001). The research relied primarily on personal interviews- given the emerging nature of supply chain security research, little empirical work has been conducted (in comparison to other longer-standing supply chain phenomena) and much of the research in supply chain security has been descriptive (Voss et al., 2009). As such, the interviews were implemented to help guide the development of measures and constructs for quantitative analysis. In addition, organizational documents and websites were collected and examined to triangulate commentary provided by interview respondents.

Members of the research team typically scheduled a site visit to speak with multiple firm respondents–although some interviews were conducted via telephone. In addition, supply chain partners (suppliers, customers, and supply chain service providers) were identified and data was gathered from a sampling of these partners. Participating firms were asked to provide access to their highest ranking executive/manager responsible for security, quality, and/or supply chain management. In some firms, multiple managers were interviewed as each of these functional areas might be under different manager's responsibility, while in other firms (particularly smaller firms), one individual might have oversight across all three functional areas. Finally, interviews were conducted sequentially by industry. Interviews were initiated with those in the food industry, followed by the pharmaceutical, and finally, hazardous materials industries.

Using the techniques prescribed by Eisenhardt (1989) and Yin (1994), qualitative data was collected. A interview guide with open-ended questions was developed and pre-tested with academic reviewers (by drawing from the literature in supply chain management and criminal justice disciplines as well as the NAT and HRT theories) and with industry practitioners from each industry familiar with supply chain security issues. The interview guide was semi-structured, but allowed for the researchers to explore new issues raised during the interview process. Two or more research team members participated in every interview. Each research team member transcribed notes taken during the interviews and these notes were discussed after the interviews by the research team in order to clarify any issues or questions as well as to identify emerging themes. Interviews were conducted with 75 managers across 25 different firms.

Coding: In order to reduce the potential for categorization bias, we did not develop a priori supply chain design dimensions but instead, reviewed and coded the supply chain security initiatives described by respondents. Multiple research team members culled through the interview note transcripts looking for key themes associated with the research framework. Four research team members were involved in the coding process and each team member identified key themes that were discussed at each interview site. Two researchers independently identified themes associated with each interview site. Once themes had been developed for each interview site, members of the research team examined the themes first individually and then as a group to determine which theme labels were similar and focusing on a similar concept and which labels were very different from one another and focusing on very different concepts. Based on the independent and team process, four

key themes emerged across industries from the qualitative analysis relating to supply chain disruption mitigation and design and these four themes serve as the focus on this research: supply chain security process management, security information sharing, supply chain partner security management, and supply chain service provider security management.

The results of this coding were validated by presenting the constructs to 10 executives responsible for security at eight firms. These presentations resulted in a more precise sculpting of the activities underlying each concept. Each construct is discussed below.

2.5.1. Supply chain security process management

Supply chain security process management assesses the degree to which security provisions have been integrated into processes to detect, prevent, respond, and recover from a security incident that may occur anywhere within the supply chain (e.g. flow of product, services, or information). This construct emerged from interview discussions highlighting various strategies that firms had adopted to create integrated supply chain processes in an effort to improve security as well as to better respond should an incident occur. For example, one food industry firm discussed the decision to move from a large, decentralized transportation process (across multiple divisions) into a centralized transportation network to ensure all carriers and service providers adhered to the firm's expectations regarding protection.

Participating firms often discussed the development of cross functional process maps or flowcharts to understand supply chain product and information flows and to identify potential security risks. Process management also included the use of simulated incidents to test the integrity of procedures and processes. Many of the participating firms discussed monthly or quarterly mock events that they and their supply chain partners participated in to simulate recalls, contaminations, and information hackers. Simulated incidents included table-top exercises designed to test the effectiveness of a supply chains security capabilities.

2.5.2. Supply chain security information sharing

Supply chain security information sharing focuses on the degree to which supply chain partners share accurate information in a timely fashion to address security-related incidents. Information systems provide a first defense mechanism by which to understand trends in product contamination, missing shipments, and the root causes of these occurrences. The flow of information across a supply chain network provides increased visibility between supply chain partners to help discover and recover from incidents and can result in critical supply chain design initiatives (Blackhurst et al., 2005). As indicated by Zhou and Benton (2007) "information sharing is a means to capture supply chain dynamics and thus reduce uncertainty in external and internal environments" (p. 1363). Consistent with the NAT and HRT frameworks, tight coupling and complex interdependencies between supply chain partners should result in greater sharing of information between partners, in part, to provide an early warning about possible exceptions and problems.

Information systems also play a critical role in gathering information that can be subsequently shared with suppliers, customers, service providers, and government agencies to identify potential problems or to create recovery actions. One of the participants discussed the development of a corporate level contact list to be used in the event of contamination or other major disruption. This contact list includes executives, division chiefs, corporate affairs personnel, and suppliers. The list also includes backup suppliers and carriers that may be called upon if primary partners are not available.

2.5.3. Supply chain partner security management

Supply chain partner security management characterizes the procedures to monitor and assess the degree to which the supply chain partner is making appropriate investments to mitigate security risk. Sheffi (2001) posits collaboration with external partners is necessary to ensure that security procedures are communicated and followed. Collaboration between firms has been cited as a unique, critical factor in any comprehensive security program (Dobie et al., 2000; Rinehart et al., 2004; Varkonyl, 2004; Wolfe, 2001). Supply chain partners' capabilities need to be verified from a security standpoint as partners who lack sufficient security capabilities might be replaced. In addition, as the overall level of supply disruption risk increases, buyers are more likely to select alternative suppliers better able to protect product throughout the supply chain hand-offs (Ellis et al., 2010).

Interview respondents from multiple food and pharmaceutical producers discussed the increased importance of having a trusting relationship with suppliers. Key respondents indicated that their firms rely heavily on their supplier's protection initiatives to guarantee a secure product supply. In addition, multiple firms talked about a significant reduction or even elimination of spot buying to ensure greater control over product quality and reduced possibility of contamination. Further, one firm discussed the decision not to source any product internationally due to the perceived increased risk of contamination or loss of control over the product during shipment. Finally, some firms spent time training suppliers regarding the potential for product contamination, particularly where suppliers might include small family-run farms. These training efforts included both education regarding security issues as well as training in how suppliers could best protect themselves and their products. Additionally, participants discussed more extensive certification and audit programs for suppliers to ensure that the expected codes of behavior were followed. External integration with key suppliers and customers had the greatest influence on a firm's supply chain agility which represents one potential disruption mechanism (Braunscheidel and Suresh, 2009).

2.5.4. Supply chain service provider security management

Finally, supply chain service provider security management assesses the same procedures for service providers as discussed for supply chain partners. Multiple respondent companies discussed their efforts with transportation carriers to increase driver awareness of security threats (e.g., risks when stopping at a truck stop, cargo security, etc.). Similarly, multiple firms require that service providers screen drivers to decrease the risk of hiring a driver who may intend to do harm through product contamination, hijacking, or using a vehicle or cargo for malicious purposes. These expectations also extend to other transportation modes and full-service providers (e.g., third party providers that offer both transportation and warehousing). In one example, truck drivers had to report previous product transported before the firm would release product to be tendered by the carrier – in this case, if the previous product hauled could potentially contaminate the firm's products, the carrier was not authorized to take the load.

3. Hypothesis development

Given the integration of three theoretical foundations used to guide this research, the hypotheses developed attempt to synthesize key factors of importance across the theoretical perspectives proposed. The researchers identified four key factors that represent potential considerations from each theoretical perspective that may impact a firm's security efforts, including: (1) Product Risk; (2) Supply Chain Complexity; (3) Coupling; and (4) Mindfulness. Each factor is described below and is related to the four themes

or elements identified in the qualitative results as key disruption mitigation and design strategies.

3.1. Product risk

Certain types of products are likely to be perceived as risky – either due to the nature of the product or supply chain and/or the potential for unintentional or intentional disruptions. Specifically, food products that have been identified as high risk include perishable (i.e., not processed) agriculture products, meat and dairy (Casagrande, 2000; RAND, 2003) as they are more susceptible to damage/spoilage (Moncke, 2004). There are a number of reasons that perishable products, in general, and food/dairy/agriculture pose such significant risk. First, livestock and agriculture production typically occurs across highly unsecured distributed geographies and as such, provide an accessible target to potential offenders. Second, the holding, processing, and distribution of livestock is highly concentrated facilitating very fast and broad-based spread of any contaminant. Third, there are far many more lethal and contagious biological agents that can attack plants and animals than humans. These biological agents are often not harmful to humans and accessible, making it relatively easy for a willing offender to obtain and apply against an accessible target (Moncke, 2004).

Further, the food industry is believed to be a particularly salient target of intentional sabotage because ingestion of contaminated product has the potential to cause widespread injury or death (World Health Organization, 2008). In order to reduce the attractiveness of a target, highly specific preventative measures need to be applied to eliminate or reduce the damage that can occur (Clarke, 1997). Such preventative measures could include enhanced process management (e.g., processes to prevent, detect, response and recover from an incident). For example, firms in the food industry are likely to use of Hazard Analysis and Critical Control Point (HACCP), a food safety process adopted by the USDA.[4] Information sharing regarding potential threat levels or suspicious incidents would be important for firms in a more risky position. This information sharing should extend beyond the four walls of the firm to include supply chain partners and service providers. Therefore, we hypothesize:

H1. Firms that have higher risk products have increased _____ than those firms with less risky products.

a. supply chain security process management
b. supply chain security information sharing
c. supply chain partner security management
d. supply chain service provider management

3.2. Supply chain complexity

Firms managing more complex supply chain interactions have an increased risk of experiencing a supply chain disruption and are more likely to make investments to manage or even reduce the supply chain complexity where warranted (Perrow, 1984). Such firms are more likely to invest into supply chain security process management, for example, in order to better prevent, detect, respond, and recover from any incidents. Further, such firms can manage some of the supply chain complexity in supply chain hand-offs by increasing the information sharing to increase overall supply chain visibility. Firms that have greater levels of supply chain complexity are more likely to aggressively manage their supply chain and service partner initiatives regarding security. Firms with significant supply chain complexity will strive to reduce complexity by holding partners more accountable for their security efforts. As part of the interviews, many firms discussed having more detailed audit procedures for suppliers and service providers in an effort to increase standardization of operations. Therefore, we hypothesize:

H2. Firms with greater supply chain complexity have increased _____ than those firms with less supply chain complexity.

a. supply chain security process management
b. supply chain security information sharing
c. supply chain partner security management
d. supply chain service provider management

Firms that face high levels of risk need to be cognizant of greater security needs for the supply chain. This greater risk compounds the supply chain complexity factors for supply chain design. For example, in the chemical industry, certain products may be more attractive to terrorists due to their explosive or hazardous qualities (e.g., high product risk). Given the vast movement of such products across potentially accessible areas (e.g., open rail yards), the level of product risk is compounded by the supply chain complexity. Therefore, we hypothesize:

H3. Across firms with greater supply chain complexity, those firms that have risky products have increased _____ to reduce the product risk level.

a. supply chain security process management
b. supply chain security information sharing
c. supply chain partner security management
d. supply chain service provider management

3.3. Coupling

Firms that have tighter coupling relationships have an increased risk of experiencing a supply chain disruption and are more likely to make investments to manage or even loosen the relationships where warranted. Such firms are more likely than those with more loosely coupled relationships to invest into supply chain security process management to better prevent, detect, respond, and recover from any incidents. Further, such firms can manage some of the tighter coupling by increased information sharing to enhance overall supply chain visibility. This is particularly true with respect to tracking technologies, such as RFID and GPS. Firms that have tighter coupling relationships are more likely to aggressively manage their supply chain and service partner initiatives regarding security. As the security of any supply chain is only as strong as the weakest link (Sheffi, 2001), firms with tight coupling relationships will strive to manage the potential negative impact of tight coupling by holding partners and service providers more accountable for their security efforts. Therefore, we hypothesize:

H4. Firms with more tightly coupled partnerships have increased _____ than those with more loosely coupled partnerships.

a. supply chain security process management
b. supply chain security information sharing
c. supply chain partner security management
d. supply chain service provider management

3.4. Mindfulness

While many firms are compelled by government, industry or competitor standards to make investments in security, other firms are more aggressive about building a more visible security culture within the firm. Creating more visible awareness is an attribute of

[4] For additional information on HACCP, see http://www.cfsan.fda.gov/~lrd/haccp.html.

high reliability organizations and has been referred to as "mindfulness" (Weick and Sutcliffe, 2001). Highly mindful organizations are able to identify changing circumstances and when such circumstances necessitate an organizational response to more strongly position the firm (in general) to avoid disruption. Similarly to the way in which McFadden et al. (2009) found leadership commitment and a safety culture positively impacted safety initiatives and safety outcomes in hospitals, this research hypothesizes that mindfulness will positively impact the development of a secure and resilient supply chain.

Executive commitment to security and fostering a security culture is hypothesized as a necessary condition for implementing an effective security environment. Top management needs to encourage frank discussions regarding the importance of security, both for the safety of stakeholders and to maintain the value of the firm's brand. Top management must be visible in their commitment and dedication to implementing security initiatives. As an example from the exploratory interviews, some firms have created a "chief security officer" position or a cross-functional corporate security committee to provide additional structure for security initiatives. Interestingly, annual security audit reports, used by some participating firms, also include a focus on information technology security threats, executives foster a culture among personnel that places security among their top priorities. A culture that empowers front-line employees to demonstrate a security mindset is also key (Sheffi and Rice, 2005).

Organizational mindfulness focusing on security is difficult to assess directly, but can be observed based on the manner in which the firm signals the importance of security (e.g., having a chief security officer). Firms that consider supply chain security to be a strategic priority perceive greater levels of security initiatives and higher security performance (Voss et al., 2009). Similarly, firms that look beyond the threat of terrorism as a potential for a supply chain disruption and think about the potential impact on the firm's brand/reputation are more likely to create a more mindful security culture (EyeforTransport, 2004). Specifically, mindful firms are more likely to recognize that product contamination, for example, may damage customer perceptions of their brand (Aberdeen Research Group, 2004). As such, more mindful firms are more likely to make supply chain design investments in order to enhance security efforts than firms that have not made supply chain security a more visible aspect of their business. Therefore, we hypothesize:

H5. More mindful firms have increased _____ than those that are less mindful.

a. supply chain security process management
b. supply chain security information sharing
c. supply chain partner security management
d. supply chain service provider management

4. Research method

A quantitative methodology was developed as the second element of the multi-method approach taken in this research. A quantitative survey was designed to more fully investigate the security actions taken by firm and the resulting response to possible disruption threats. The survey instrument measured the four thematic construct areas (e.g., process management, information sharing, partner security management, and service provider management) as well as assessed the level of risk, supply chain complexity, coupling and mindfulness. The survey was pre-tested in an iterative fashion by administering it to qualified supply chain and criminal justice academicians as well as a number of food industry managers and others familiar with security efforts. Modifications were made to the survey following each pretest round until researchers determined that questions were clear and achieved the original survey goal.

The quantitative survey data was collected from a targeted industry – the food industry – whereby the sample included food manufacturers drawn from mailing lists of supply chain and security managers (and higher) working at food manufacturers. An executive vice president at a very visible food firm wrote a cover letter inviting respondents to participate in the study. Respondents ranged from presidents, vice-presidents, directors, managers and supervisors with 58% of the respondents indicating that they were their firm's president/vice-president or director. Seventy percent of the respondents indicated that they had 15 years or more of work experience in the food industry. A total of 1373 potential respondents were asked to complete the survey. Respondents were given the option of completing the survey on-line or in hard copy format. If respondents elected to complete the hard copy format, responses were either faxed or mailed back to researchers in a pre-paid envelope. A total of 239 surveys were returned for an overall response rate of 17%; 40 surveys were deemed unusable due to missing data or unrealistic responses rendering a final sample size of 199 ($n = 199$) with a usable response rate of 14%. Non-response bias was assessed by comparing demographic characteristics of early and late respondents; χ^2 difference tests indicated no significant differences between the groups (Armstrong and Overton, 1977).

Several steps were utilized to purify construct measures, assess convergent validity, and assess discriminate validity as prescribed by Anderson and Gerbing (1988). First, item to total correlations were examined. Items with low correlations as they relate to the *a priori* hypothesized scales were deleted. Exploratory factor analysis with varimax rotation was used to assess internal and discriminant factor validity. As noted in Table 2, each item loaded highly on the expected factor (all loadings greater than .6) and all cross-factor loadings were less than .3. Second, Cronbach's alpha was examined for each item within a construct and the reliabilities exceeded the recommended 0.70 cut-off (Nunnally, 1978).

Specific supply chain-level and product-level information were used to develop the four independent variables of: product risk, supply chain complexity, coupling, and mindfulness. Product risk was measured using the following binary scheme: (high risk: products that could be easily contaminated (e.g., meats/poultry/fish/produce); low risk: products that were considered less perishable and more shelf stable (e.g., canned goods) (RAND, 2003)

Supply chain complexity was measured using a 4-level categorical variable describing the supply chain complexity of the firm's marketplace-local, regional, national, or global. As Sheffi (2001) suggests, global relationships present added security difficulties as focal firms are less able to monitor their partners and protect against theft, contamination, or insertion of unauthorized counterfeit cargo. Hendricks et al. (2009) illustrated that firms with geographical diversification had greater negative stock market impact as a result of a disruption than firms with less geographical diversification as greater diversification leads to more deleterious effects throughout the supply chain.

Coupling was measured using a 4-level categorical variable focusing on the need for synchronization between a buyer and supplier. Firms managing the synchronization associated with just – in-time deliveries when participating in a global supply chain would exhibit very strong coupling while firms managing a local supply base would require less buyer/supplier coupling. Consistent with supply chain complexity, prior research demonstrates that firms with more supply chain slack (e.g., firms with less demanding just-in-time/global sourcing requirements) had less negative stock market impact when a disruption occurred while firms with less supply chain slack (e.g., firms with more demanding global just-in-time sourcing requirements) had greater negative stock

Table 2
Dependent variable factor analysis and reliabilities.

Construct items	Factor loading	λ
Supply chain security process management		.918
Our firm has processes in place to prevent a contamination/security event in our supply chain	.849	
Our firm has processes in place to detect a contamination/security event in our supply chain	.830	
Our firm has processes in place to respond to a contamination/security event in our supply chain	.875	
Our firm has processes in place to recover from a contamination/security event in our supply chain	.775	
Supply chain security information sharing		.846
Our firm's information systems could provide the following information within 24 h for each food item transported within the past year:	.760	
•The name of the immediate previous source and immediate subsequent recipient		
•The origin and destination points		
•The date the shipment was received and released		
•The number of packages in the shipment		
•Description of freight		
•Route and transfer points through which the shipment moved		
Our firm's information systems provide our supply chain partners with timely information they need to respond to contamination/security incidents	.778	
Our firm's information systems provide our supply chain partners with valid information they need to respond to contamination/security incidents	.781	
Our supply chain partners can provide us the actionable information we need to respond to contamination/security incidents	.777	
Supply chain partner security management		.890
Our firm has defined consequences for supply chain partners who fail to comply with supply chain security procedures	.775	
Our firm uses security audits to determine if relationships should be maintained with suppliers	.891	
Our firm uses security audits to determine if relationships should be maintained with customers	.843	
Our firm audits the security procedures of contract manufacturers	.798	
Supply chain service provider security management		.792
Our firm verifies that service providers perform security background checks on their employees	.770	
Our firm collaborates with service providers to improve their security programs	.697	
Our firm verifies that service providers monitor transportation assets	.604	

market impact when a disruption occurred (Hendricks et al., 2009). As such, we measured the coupling based on the degree to which a firm needed to manage just-in-time deliveries across a more distributed supply base breadth: local, regional, national or global.

Finally, mindfulness was measured using three items that served as an indicator of the firm's interest in positioning security as a strategic priority: (1) Our firm's senior management views supply chain security as necessary for protecting our brand or reputation; (2) Our firm has a senior management position focusing on security; and (3) Our firm's senior management views supply chain security as a competitive advantage. These three items represent the willingness (or lack thereof) of a firm to create a security and safety-oriented culture. All three items were measured using a 5-point Likert scale. The items were averaged (per the factor analysis results) and then the average scores were divided into quartiles to categorize the variable.

5. Results

The survey data was analyzed using MANOVA. MANOVA is an appropriate test to implement when the data consists of multiple correlated dependent variables and yet it is desirable to run a single, overall statistical test to minimize the potential for overstating significant relationships. A correlation analysis (Table 3) confirmed that the dependent variables in the sample were all significantly correlated with one another and as such, the MANOVA results are presented in Tables 4–7 and Figs. 2–4.

Table 4 provides the overall MANOVA results demonstrating that all of the main effects are significant (product risk: (F (4, 185) = 4.26, $p < .003$); supply chain complexity: (F (12, 185) = 2.52, $p < .003$); mindfulness: (F (12, 185) = 2.81, $p < .001$)) or approaching significance (coupling: (F(12, 185) = 1.66, $p < .065$)). In addition, there were three 2 way interactions that were significant: (product risk × supply chain complexity: (F (36, 185) = 2.09, $p < .017$));

Table 3
Dependent variable correlation matrix.

	Process management	Information sharing	SC partner security management	SC service provider management
Process management	1	.397**	.214**	.569**
Information sharing		1	.448**	.439**
SC partner security management			1	.404**
SC service provider management				1

** p-value < .01.

Table 4
Hypothesis testing M ANOVA results (reporting of complete model).

Independent variable	df	F	p value
Intercept	(4, 185)	1143.32	.000
Product risk (H1)	(4, 185)	4.26	.003
SC complexity (H2)	(12, 185)	2.52	.003
Product risk × complexity (H3)	(36,185)	2.09	.017
Coupling (H4)	(12, 185)	1.66	.065
Mindfulness (H5)	(12, 185)	2.81	.001
Product risk × coupling	(36, 185)	2.87	.001
Product risk × mindfulness	(36, 185)	1.41	.158
SC complexity × coupling	(36, 185)	.783	.800
SC complexity × mindfulness	(36, 185)	1.35	.086
Coupling × mindfulness	(36, 185)	1.60	.016

MANOVA generates four related yet unique tests to determine the significance of the *F*-statistic (Pillai's Trace, Wilks' Lambda, Hotelling's Trace, and Roy's Largest Root). Pillai's Trace is the most conservative of the four tests and as such, we report the significance of the F-test based on Pillai's Trace to minimize Type I error. All three-way and four-way interactions were tested as part of a holistic model and were all insignificant.

product risk × coupling: (F (36, 185) = 2.87, $p < .001$); and coupling × mindfulness: (F (36, 185) = 1.60, $p < .016$). None of the 3 or 4 way interactions were significant.

Hypothesis 1 suggests that firms with high risk products are more likely to invest in supply chain design investments. The MANOVA results indicate that higher risk firms invest more heavily in process management (F (1, 185) = 13.81, $p < .001$) and information sharing (F (1, 185) = 5.06, $p < .026$) than those firms with less risky products (process management means: 4.22 as compared to 3.45; information sharing means: 4.39 as compared to 3.80). Supply chain partner security management is not significantly different across high and low risk products (F (1, 185) = .008, $p < .929$) nor is service provider management (F (1, 185) = .759, $p < .385$). Therefore, Hypotheses H1a and H1b are supported and H1c and H1d are not supported.

Hypothesis 2 suggests that firms having greater supply chain supply chain complexity are more likely to invest in supply chain design investments than firms facing less supply chain complexity. The MANOVA results indicate that high supply chain complexity firms invest more heavily in process management (F (3, 185) = 2.92, $p < .037$), information sharing (F (3, 185) = 4.00, $p < .009$), supply chain partner security management (F (3, 185) = 2.81, $p < .042$), and service provider management (F (3, 185) = 2.82, $p < .042$) than firms having less supply chain complexity. As noted in Table 6: *process management*: high supply chain complexity firms have significantly greater process management activities (4.24) than moderate or low supply chain complexity firms (means: 3.77, 3.53, 3.41); *information sharing*: high supply chain complexity firms have significantly greater information sharing activities (4.40) than moderate or low supply chain complexity firms (means: 4.15, 3.93, 3.41); and low supply chain complexity firms have less information sharing activities than moderate firms; *supply chain security partner management*: high supply chain complexity firms have significantly greater supply chain security partner management

Table 5
Between subjects effects for significant main and 2 way interaction effects.

Independent variable df	Process management	F	p value
Product risk (H1)	Process management	13.81	.000**
(1,185)	Information sharing	5.06	.026*
	SC partner security management	.008	.929
	SC service provider management	.759	.385
Supply chain complexity (H2)	Process management	2.92	.037*
(3,185)	Information sharing	4.00	.009**
	SC partner security management	2.81	.042*
	SC service provider management	2.82	.042*
Product risk × supply chain complexity (H3)	Process management	7.28	.032*
(3,185)	Information sharing	2.46	.031*
	SC partner security management	.122	.947
	SC service provider management	2.66	.050*
Coupling (H4)	Process Management	1.37	.255
(3,185)	Information sharing	1.05	.372
	SC partner security management	2.74	.046*
	SC service provider management	3.07	.030*
Mindfulness (H5)	Process management	5.06	.002**
(3,185)	Information sharing	3.08	.030*
	SC partner security management	5.10	.003**
	SC service provider management	4.78	.003**
Product risk × coupling	Process management	7.28	.000**
(3,185)	Information sharing	2.46	.065
	SC partner security management	1.57	.200
	SC service provider management	2.55	.059
Coupling × mindfulness	Process management	2.60	.009**
(9,185)	Information sharing	.26	.985
	SC partner security management	1.71	.092
	SC service provider management	1.86	.064

* $p < .05$.
** $p < .01$.

Table 6
MANOVA results for main effects means and standard deviations.

Independent variable	Condition	Process management mean (s.d.)	Information sharing mean (s.d.)	Supply chain partner security mean (s.d.)	Service provider management mean (s.d.)
Product risk (H1)	Low	3.45 (.08) (2)	3.80 (.10) (2)	2.28 (.10)	2.71 (.10)
	High	4.22 (.11)	4.39 (.13)	2.39 (.13)	2.93 (.13)
Supply chain complexity (H2)	1	3.41 (.20) (4)	3.41 (.23) (2,3,4)	2.36 (.23) (3,4)	2.19 (.24) (4)
	2	3.53 (.14) (4)	3.93 (.17) (4)	2.31 (.27) (4)	2.98 (.17) (4)
	3	3.77 (.12) (4)	4.15 (.14) (4)	2.00 (.14) (4)	2.62 (.14) (4)
	4	4.24 (.11)	4.40 (.13)	2.70 (.13)	3.13 (.14)
Coupling (H4)	1	3.72 (.17)	4.11 (.20)	2.42 (.20) (2)	2.86 (.21) (2)
	2	3.48 (.16)	4.02 (.18)	1.76 (.19) (3,4)	2.16 (.19) (3,4)
	3	3.92 (.12)	3.93 (.13)	2.27 (.14) (4)	2.85 (.14) (4)
	4	3.89 (.12)	4.19 (.14)	2.77 (.14)	3.15 (.14)
Mindfulness (H5)	1	3.36 (.13) (2,3,4)	3.64 (.16) (2,3,4)	1.58 (.16) (2,3.4)	1.92 (.16) (2,3,4)
	2	3.72 (.13) (4)	4.14 (.15) (4)	2.32 (.15) (4)	2.77 (.15) (4)
	3	3.76 (.13) (4)	4.07 (.15) (4)	2.66 (.15) (4)	3.03 (.16) (4)
	4	4.4 (.16)	4.44 (.18)	2.89 (.19)	3.67 (.19)

Table 7
MANOVA results for supply chain complexity × risk interaction.

Independent variable	Condition	Low risk mean (s.d.)	High risk mean (s.d.)
Complexity × risk level (H3b)	Process management		
	1	2.45 (.26)	−0.29
	2	3.17 (.18)	−0.24
	3	3.45 (.13)	−0.21
	4	4.17 (.15)	4.32(.18)
	Information sharing		
	1	2.52 (.30)	−0.34
	2	3.69 (.21)	−0.28
	3	3.87 (.15)	−-0.25
	4	4.37 (.17)	4.44 (.21)
	Supply chain partner security		
	1	2.26 (.30)	2.43 (.34)
	2	2.06 (.21)	2.73 (.28)
	3	2.12 (.16)	1.84 (.25)
	4	2.73 (.17)	2.66 (.21)
	Service provider management		
	1	2.08 (.31)	2.27 (.35)
	2	3.04 (.22)	2.87 (.29)
	3	2.40 (.16)	2.93 (.25)
	4	2.94 (.17)	3.34 (.22)

activities (2.70) than moderate or low supply chain complexity firms (means: 2.00, 2.31, 2.36); and *service provider management*: high supply chain complexity firms have significantly greater service provider management activities (3.13) than moderate or low supply chain complexity firms (means: 2.62, 2.98, 2.19). Therefore, Hypotheses H2a, H2b, H2c, and H2d are supported.

Hypothesis 3 predicts an interaction effect between the product risk and supply chain supply chain complexity such that firms with both high risk products and greater supply chain complexity are more likely to invest in supply chain design investments than firms with less risky products and/or less supply chain complexity in their supply chain. The MANOVA results indicate that the interaction is significant for process management (F (3,

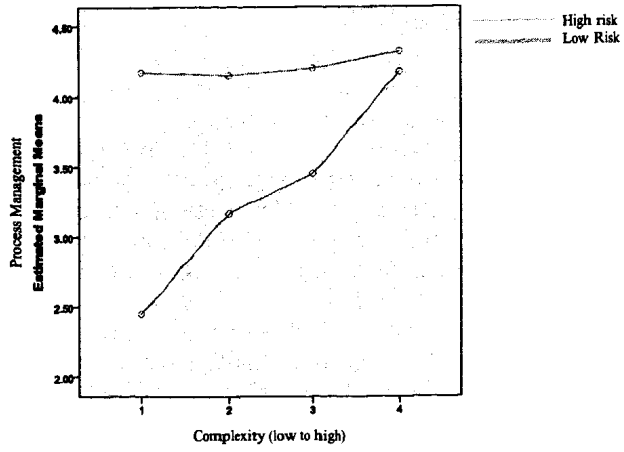

Fig. 2. Complexity by risk level interaction for process management process management.

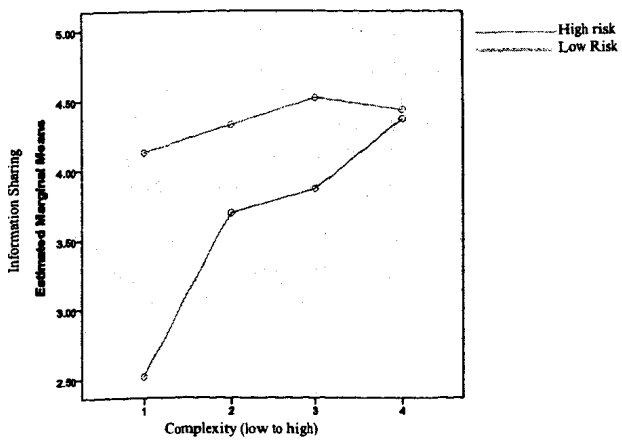

Fig. 3. Complexity by product risk level interaction for information sharing.

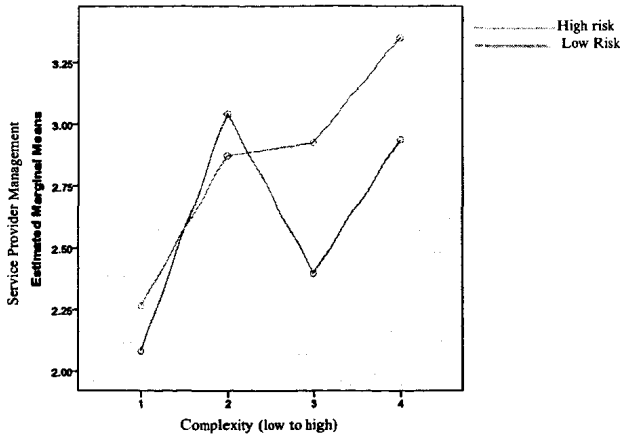

Fig. 4. Complexity by product risk level interaction for service provider management.

185) = 7.28, $p < .032$), information sharing ($F(3, 185) = 2.46$, $p < .031$) and service provider management ($F(3, 185) = .2.66$, $p < .05$) but not for supply chain partner security management ($F(3, 185) = .122$, $p < .947$). For process management and information sharing, firms with higher risk products invest in greater process management and information sharing activities for all levels of supply chain complexity. However, firms with lower risk products only invest in process management and information sharing activities at high levels of supply chain complexity. Therefore, Hypotheses H3a, H3b, and H3d are supported and H3c is not supported. The interactions means are reported in Table 7 and are illustrated in Figs. 2–4.

Hypothesis 4 suggests that tightly coupled firms are more likely to invest in supply chain design investments than firms with loose coupling. The overall MANOVA test result was approaching significance ($F(9, 185) = 1.66$, $p < .065$) and the results indicate that more tightly coupled firms invest more heavily in supply chain partner security management ($F(3, 185) = 2.74$, $p < .046$) and service provider management ($F(3, 185) = 3.07$, $p < .030$) than those firms with loose coupling. Neither information sharing ($F(3, 185) = 1.05$, $p < .372$) nor process management is significant ($F(3, 185) = 1.37$, $p < .255$). As noted in Table 6: *supply chain security partner management*: more tightly coupled firms have significantly greater supply chain security partner management activities (2.77) than more moderately coupled firms (means: 2.27, 1.76) but are not significantly different than loosely coupled firms (2.42); and *service provider management*: more tightly coupled firms have significantly greater supply chain security partner management activities (3.15) than more moderately coupled firms (means: 2.85, 2.16) but are not significantly different than loosely coupled firms (2.86). Given that the overall MANOVA test statistic is only approaching significance and two of the underlying dependent variable tests are significant, none of the H4 hypotheses are supported.

Hypothesis 5 suggests that more mindful firms are more likely to invest in supply chain design investments than firms that are less mindful. The MANOVA results indicate that more mindful firms invest more heavily in all four supply chain design activities: (1) Process management ($F(3, 186) = 5.06$, $p < .002$); (2) Information sharing ($F(3, 186) = 3.08$, $p < .030$); (3) Supply chain partner security management ($F(3, 186) = 5.10$, $p < .003$); and (4) Service provider management ($F(3, 186) = 4.78$, $p < .003$). As noted in Table 6: *process management*: high mindfulness firms have significantly greater process management activities (4.40) than moderate or low mindfulness firms (means: 3.76, 3.72, 3.36) and low mindfulness firms have significantly less process management activity than moderate firms; *information sharing*: high mindfulness firms have significantly greater information sharing activities (4.44) than moderate or low supply chain complexity firms (means: 4.07, 4.14, 3.64); and low mindfulness firms have less information sharing activities than moderate firms; *supply chain security partner management*: high mindfulness firms have significantly greater supply chain security partner management activities (2.89) than moderate or low supply chain complexity firms (means: 2.66, 2.32, 1.58); and low mindfulness firms have less supply chain security partner management activities than moderate firms; and *service provider management*: high mindfulness firms have significantly greater service provider management activities (3.67) than moderate or low supply chain complexity firms (means: 3.03, 2.77, 1.92); and low mindfulness firms have less service provider management activities than moderate firms. Therefore, Hypotheses H5a, H5b, H5c, and H5d were all supported.

6. Discussion and conclusions

The results have important implications for security management and are highlighted in Table 8. First, supply chains manufacturing and transporting more high risk products are more likely to invest in process management and information sharing supply chain design initiatives. Similarly, greater inherent supply chain complexity results in greater investments into the supply chain design initiatives of process management, information sharing, supply chain partner security management, and service provider management. Further, there is a strong interaction effect between the product risk level and supply chain complexity resulting in increased supply chain design investments into process management, information sharing, and service provider management. Supply chains having tighter coupling are more likely to invest in supply chain partner and service provider management initiatives. Finally, firms having leaders with greater mindfulness associated with security and risk are more likely to invest in process management, information sharing, and partner and service provider management initiatives.

A major factor driving supply chain design security initiatives is mindfulness. Firms with mindful executives have implemented a broader range of design initiatives to enhance their security. A second factor driving supply chain design security initiatives is supply chain complexity. Firms participating in highly complex supply chains have incorporated information sharing as well as initiatives with supply chain partners and service providers to enhance their security. A third factor driving supply chain re-design are products that are high risk. Firms with such products are refining operating processes and increasing information sharing to reduce their risk. However, these firms are not implementing initiatives with partners or service providers. This could suggest these firms have designed their supply chain to minimize the role of partners and service providers. Alternatively, the lower means for supply chain and service partner management may indicate that firms are trying to get their own house in order before reaching out to partners across the supply chain (Kleindorfer and Saad, 2005). The final driver is tight coupling which results in redesign initiatives with supply chain partner and service providers. It is critical that tightly coupled firms integrate their security efforts with the supply chain partners. In summary, the depth and breadth of a firm's security initiatives depends on top management mindfulness, supply chain complexity, product risk, and coupling in decreasing order of interaction.

From a theoretical perspective, the results support the use of Natural Accident and High Reliability Theories as a useful lens from which to understand supply chain design issues. Specifically, the tenets of supply chain complexity and coupling-the critical dimensions of both NAT and HRT–highlight the difficulty of responding to intentional and unintentional security disruptions given the synchronization of supply chain partners and breadth/interactions

Table 8
Summary of significant main and interaction effects.

Supply chain factors influencing security efforts	Supply chain disruption design themes			
	Process management	Information sharing	SC partner security management	Server provider management
Risk level	M	M		
Supply chain complexity	M	M	M	M
Risk level × supply chain complexity	I	I		I
Coupling			M	M
Mindfulness	M	M	M	M
Coupling × mindful	I			
Risk level × coupling	I			

M = significant main effect; I = significant interaction effect.

associated with supply chain partners supporting more global marketplaces. In addition, the situational crime prevention lens highlights the importance of understanding the potential offender, location, and target. In this research, the testing of hypotheses focused on the notion of target by examining the inherent risk (e.g., attractiveness of the target) associated with different food products. The results also demonstrate the validity of this lens.

We believe that the integration of these theoretical perspectives provides tremendous direction for future research. First, a more sophisticated examination of supply chain complexity and coupling should be examined in order to more fully understand which supply chain structures and interactions lead to more tight coupling and greater complexity and the degree to which these structures/interactions can be supported with the supply chain design initiatives examined in this research. As such, future research should focus on more fully understanding who participates in a supply chain beyond 1st tier suppliers and customers – many recent recalls and/or product contaminations highlighted that the problem occurred prior to the 1st tiered supplier (e.g., lead paint in toys, melamine in milk at farm level, etc.). More fully understanding the breadth/depth of the supply chain network involves a more in-depth examination of cohesion.

Similarly, we explored aspects of the situational crime prevention framework by examining a specific facet of the target. Future research should examine additional target facets including the level of target facility protection, differences in supply chain security design initiatives among different high risk products, differences in supply chain security design initiatives among very different types of high risk products (e.g., food vs. hazardous materials). In addition, future research should examine aspects of the location and the offender to more fully understand supply chain security design initiatives. Location, in particular, would appear to be of critical interest for supply chain researchers. Specifically, how do supply chain network design (i.e., which countries, what transportation methods, what border crossings, etc.) issues influence the types of supply chain security design initiatives that are implemented.

Finally, the supply chain research design initiatives examined in this research were a product of qualitative interviews conducted with firms within the food, pharmaceutical, and hazardous materials industries. Future research should more fully test the boundary conditions of the integrated theory—does it apply only to firms that manufacture/distribute these products or does it apply more broadly to other industries? In addition, future research should evaluate and examine other supply chain design initiatives that would apply in these and other industries.

In addition to the theoretical implications associated with this research, there are a number of practical implications. First, from an information sharing perspective, firms alter their supply chain design by requiring greater visibility of information between partners or consider changing partners to those that are able to meet their information needs when higher risk products are involved. Similarly, greater supply chain complexity and more mindful organizations also make greater investments into information sharing to improve supply chain security. Thus, greater visibility of information between partners or changing partners to those that are able to meet information needs become critical supply chain design choices.

Initiating or maintaining a partnership based on the ability to effectively share information between partners is not particularly new. The compatibility of information systems between firms has been a factor in merger and acquisition decisions. Similarly, vendor-specific enterprise resource planning systems have become almost a standard within some industries to facilitate information sharing between suppliers and customers. Many firms are investing in information systems capabilities that facilitate information sharing and our results have implications for information systems vendors. Most suppliers have a multitude of customers who are likely to be using different information systems platforms. As these customers demand more real-time information, the supplier may have difficulty sending data that can be easily integrated into the customers' information system. Suppliers may be faced with investing in significant customization of existing systems or even the duplication of some systems to ensure that critical customers can obtain the information they need. Information systems vendors have an opportunity to develop middleware and other platform independent tools that allow suppliers to more easily send data to customers regardless of their software platform.

Given the nascent amount of empirical research focusing on supply chain security assessments, this research serves as a first step in develop constructs concerning security design initiatives and hypotheses examining conditions that make these initiatives more important. However, this research also focused on determining the relevancy and boundary conditions of the research findings. In the first phase (qualitative data collection across industries) of the research, we saw significant consistency in the supply chain design issues implemented across industries. To more fully understand industry boundary conditions, we added a third research phase which served as a validation tool to determine if the quantitative results gathered in the food industry could be seen in an alternate high risk industry-hazardous materials. The next section describes the final stage of this research – validating the empirical model based on food industry initiative using qualitative data from the hazardous materials industry.

6.1. *Qualitative validation*

The research validation process focused on the selection of a particular firm whereby both NAT and HRT applied as well as firm that was concerned with both unintentional and intentional supply chain disruptions. As such, Dow Chemical was selected to provide corroborating evidence that validates and supports the empirical results of this research. Insights into how Dow Chemical manages its supply chain provides the opportunity to share best practices to further improve the understanding and applicability of these

results examined in this paper Specifically, the following section reviews four supply chain design investment areas that highlight aspects of product risk level, supply chain complexity, coupling and mindfulness – and the corresponding approaches taken in process management, information sharing, partner security management and service provider management to enhance supply chain security.

Dow Chemical is a large multinational company shipping bulk product using multiple surface and ocean transportation modes. Dow Chemical indicates that less than 1% of its shipments are rated "highly hazmat," the company has invested significant time and effort to re-evaluate supply chain design in light of security concerns. The firm has identified four drivers of a sustainable supply chain: (1) supply chain design; (2) supply chain visibility; (3) shipping container design; and (4) enhanced collaboration.

With respect to supply chain design, Dow Chemical has focused on redesigning supply chain flows to reduce the number of shipments and/or the distance the containers travel for highly hazardous materials. As such, Dow Chemical is looking at ways to *reduce the supply chain complexity* inherent in its current operations. This has been accomplished through multiple mechanisms including converting to less hazardous materials by using alternative sources of supply (*product risk, supply chain partner security management*) or by converting the highly hazardous material to a less hazardous derivative prior to shipment (*product risk, process management*). Specifically, Dow has worked with suppliers to integrate processes resulting in the combining of chemicals at the customer's production sites to reduce the level of hazardous material shipped. Therefore, supply chain design has been achieved by reducing supply chain complexity by focusing on process and supply chain partner security management and reducing inherent product risk.

In addition, Dow has made supply chain and service provider partner changes and adjustments. For example, Dow has evaluated customer demands to determine whether it would be too risky to ship highly hazardous product desired by the customer (*product risk*). Across the chemical industry, a recent report suggests that the amount of hazardous material produced or transported has been reduced such that 38 million residents in the United States are no longer at risk (Orum, 2006).

With respect to supply chain visibility and *information sharing*, Dow's goal is to know the real-time location and lading conditions of every HazMat railcar and door-to-door tracking of every intermodal container. This type of visibility facilitates rapid communication and response to potential risks and incident information (*supply chain security partner and service provider management*). To this end, Dow is working to install global positioning system (GPS) capabilities where most needed. To date, this effort has not only increased visibility, but it has also improved delivery response time to customers, reduced inventory levels, improved fleet utilization, and more quickly identified in-transit problems which enabled recovery plans to be put in place quicker. As such, these changes provide a mechanism for addressing the tight *coupling* inherent across the supply chain.

Dow Chemical has played a leading effort in shipping container design. Dow is the largest bulk shipper in North America and its fleet of 26,000 railcars is the second largest in the world (Reese, 2007) and therefore has significant cause for concern regarding railcar security. Dow has worked to reduce the ability for a railcar to be tempered with and to improve the safety of a railcar should a derailment occur (e.g., example of *process management and service provider management*).

The final prong of Dow's supply chain sustainability strategy focuses on enhanced collaboration with third party service providers, carriers, and local communities to enhance emergence preparedness should an incident occur (*supply chain partner and service provider management*). Dow reaches out to local emergence responders along transportation routes where hazardous materials travel to train responders on how to handle different chemicals. Dow is also activity in industry groups as a method for improving industry standards and processes.

These supply chain re-design efforts would not be possible without top management support. Dow has created a security-concerned culture that encourages innovation and network optimization to ensure it focuses on continuous improvement opportunities (e.g., *mindfulness*).

6.2. Conclusion

Creating and monitoring a global supply chain design to support product safety and security is an increasingly difficult proposition. The supply chain complexity of industry supply chains (e.g., product movements, information flow, etc.) coupled with product risk levels require firms to much more proactively and aggressively assess risk and implement appropriate supply chain design capabilities. Part of that proactive stance means firms must become more mindful of the need for a safer and secure supply chain recognizing the inter-relatedness and interdependencies that naturally exist within a supply chain network.

This research effort has provided a multi-method approach to examine a relatively new phenomenon and to contribute to the literature in a meaningful way. This research moves beyond descriptive and conceptual efforts to develop and test safety and security constructs. Future research focused on product safety and security can further test and investigate specific initiatives firms put in place to better prevent, detect, respond and recover from a potential disruptions. In particular, it would be useful to test the relationships proposed in this research in industries that are not as "disruption-prone" to investigate the implications to the results given the research has a foundation in HRT. Additionally, this research does not examine the supply chain design initiatives from a cost perspective. Yet, many of these initiatives may result in significant cost increases (e.g., new facilities, learning curve adjustment time with new partner, etc.). Future research could more fully examine how firms assess risk from a financial perspective and manage the potential threat/risk/cost trade-offs.

Acknowledgements

This research was supported by the U.S. Department of Homeland Security (Grant number N-00014-04-1-0659), through a grant awarded to the National Center for Food Protection and Defense at the University of Minnesota. Any opinions, findings, conclusions, or recommendations expressed in this publication are those of the author(s) and do not represent the policy or position of the Department of Homeland Security.

References

Aberdeen Group, 2004. How supply chain leaders protect their brands: A benchmark report on regulatory compliance and product safety mandates for food, pharmaceuticals, consumer products, and medical services (September).

Anderson, J.C., Gerbing, D.W., 1988. Structural equation modeling in practice: a review and recommended two-step approach. Psychological Bulletin 103 (3), 411–423.

Armstrong, J.S., Overton, T.S., 1977. Estimating nonresponse bias in mail surveys. Journal of Marketing Research 16 (August), 396–402.

Blackhurst, J., Craighead, C.W., Elkins, D., Handfield, R.B., 2005. An empirically derived agenda of critical research issues for managing supply-chain disruptions. International Journal of Production Research 43 (19), 4067–4081.

Bowersox, D.J., Closs, D.J., Cooper, M.B., 2006. Supply Chain Logistics Management, second ed. McGraw-Hill Publishing, New York.

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

Casagrande, R., 2000. Biological terrorism targeted at agriculture: the threat to US national security. The Nonproliferation Review, Fall-Winter, 92–105.
Chopra, S., Sodhi, M.S., 2004. Managing risk to avoid supply chain breakdown. Sloan Management Review 46 (1), 53–62.
Christopher, M., Peck, H., 2004. Building the resilient supply chain. The International Journal of Logistics Management 15 (2), 1–13.
Clarke, R.V., 1997. Situational Crime Prevention: Successful Case Studies. Harrow and Heston, New York.
Clarke, R.V., 1995. In: Tonry, M., Farrington, D. (Eds.), Situational Crime Prevention. In Building a Safer Society. University of Chicago Press, Chicago, pp. 91–150.
Closs, D.J., McGarrell, E.F., 2004. Enhancing security throughout the supply chain. IBM Center for the Business of Government. www.businessofgovernment.org (accessed March 2, 2006).
Cohen, L.E., 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.M., Handfield, R.B., 2007. The severity of supply chain disruptions: design characteristics and mitigation capabilities. Decision Sciences 28 (1), 131–156.
Dobie, K., Glisson, L.M., Grant, J., 2000. Terrorism and the global supply chain: where are your weak links? Journal of Transportation Management 12 (1), 57–66.
Eck, J.E., Weisburd, D., 1995. Crime and Place. Criminal Justice Press, Monsey, NY.
Eisenhardt, K.M., 1989. Building theories from case study research. Academy of Management Review 14 (4), 532–550.
Elkins, D., Handfield, R.B., Blackhurst, J., Craighead, C.W., 2005. 18 ways to guard against disruption. Supply Chain Management Review 9 (1), 46–53.
Ellis, S.C., Henry, R.M., Shockley, J., 2010. Buyer perceptions of supply disruption risk: a behavioral view and empirical assessment. Journal of Operations Management 28 (1), 34–46.
EyeforTransport Global Research, 2004. North American Supply Chain Security—An Analysis of EyeforTransport's Recent Survey (July).
Felson, M., Clarke, R.V., 1998. Opportunity Makes the Thief. Police Research Series Paper 98, Policing and Reducing Crime Unit, Research Development and Statistics Directorate. Home Office, London.
Felson, M., Clarke, R.V., 1997. Business and Crime Prevention. Criminal Justice Press, Monsey, NY.
Gebhardt, G.F., Caprenter, G.S., Sherry Jr., J.F., 2006. Creating a market orientation: a longitudinal, multiform, grounded analysis of cultural transformation. Journal of Marketing 70 (4), 37–55.
Giunipero, L., Handfield, R.B., Eltantawy, R., 2006. Supply management's evolution: key skill sets for the supply manager of the future. International Journal of Operations and Production Management 26 (7), 822–844.
Glaser, B., Strauss, A., 1967. Discovery of Grounded Theory. Aldine, Chicago, IL.
Glaser, B.G., 2001. The Grounded Theory Perspective: Conceptualization Contrasted with Description. Sociology Press, p. 11.
Greenhut, M., 1959. Plant Location in Theory and Practice. University of North Carolina Press, Chapel Hill, NC.
Harland, C., Brenchley, R., Walker, H., 2003. Risk in supply networks. Journal of Purchasing & Supply Management 9 (2), 51–62.
Hauser, L.M., 2003. Risk-adjusted supply chain management. Supply Chain Management Review 7 (6), 64–71.
Helferich, O.K., Cook, R.L., 2003. Securing the Supply Chain. Council of Logistics Management, Oak Brook, IL.
Hendricks, K.B., Singhal, V.R., 2003. The effect of supply chain glitches on shareholder wealth. Journal of Operations Management 21 (5), 501–522.
Hendricks, K.B., Singhal, V.R., 2005. 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.
Hendricks, K.B, Singhal, V.R., Zhang, R., 2009. The effect of supply chain slack, diversification, and vertical relatedness on the stock market reaction to supply chain disruptions. Journal of Operations Management 27 (3), 233–246.
Hoover, E., 1948. The Location of Economic Activity. McGraw-Hill, New York.
Johnson, M.E., 2001. Learning from toys: lessons in managing supply chain risk from the toy industry. California Management Review 43 (3), 106–124.
Kleindorfer, P.R., Belke, J.C., Elliot, M.R., Lee, K., Lowe, R.A., Feldman, H., 2003. Accident epidemiology and the U.S. chemical industry: accident history and worst-case data from RMP*Info. Risk Analysis 23 (5), 865–881.
Kleindorfer, P.R., Saad, G.H., 2005. Managing disruption risks in supply chains. Production and Operations Management 14 (1), 53–68.
LaPorte, T.R, 1994a. A strawman speaks up: comments on the limits of safety. Journal of Contingencies and Crisis Management 2 (4), 207–211.
LaPorte, T.R., Consolini, P.M., 1991. Working in practice but not in theory: theoretical challenges of 'high reliability organizations'. Journal of Public Administration Research and Theory 1 (1), 19–47.
LaPorte, T.R., 1994b. A rejoinder to Perrow. Journal of Contingencies and Crisis Management 2 (4), 221–227.
Losch, A., 1954. The Economics of Location. Yale University Press, New Haven.
Malshe, A., Sohi, R.S., 2009. What makes strategy making across the sales-marketing interface more successful? Journal of the Academy of Marketing Science 37, 400–421.
McFadden, K., Henagan, S.C., Gowen III, C.R., 2009. The patient safety chain: transformational leadership's effect on patient safety culture, initiatives, and outcomes. Journal of Operations Management 27 (5), 390–404.
Mead, P., Slutsker, L., Dietz, V., 1999. Food-related illness and death in the United States. Emerging Infectious Diseases 5 (5 (September-October)), 840–842.
Mellos, J., Flint, D.J., 2009. A refined view of grounded theory and its application to logistics research. Journal of Business Logistics 30 (1), 107–127.
Moncke, J., 2004. Agroterrorism: Threats and preparedness. CRS Report for Congress. http://www.fas.org/irp/crs/RL32521.pdf.
Nunnally, J., 1978. Psychometric Theory. McGraw Hill, New York.
Orum, P., 2006. Preventing toxic terrorism: How some chemical facilities are removing danger to American communities, report commissioned by the Center for American Progress, http://www.crtk.org/library_files/ChemicalSurvey.pdf.
Perrow, C., 1984. Normal Accidents: Living with High-risk Technologies. Basic Books, New York.
Perrow, C., 1999. Organizing to reduce the vulnerabilities of complexity. Journal of Contingencies and Crisis Management 7 (3), 150–155.
Perrow, C., 1994. The limits of safety: the enhancement of a theory of accidents. Journal of Contingencies and Crisis Management 2 (4), 212–220.
Rand Report, 2003. National Defense Research Institute. Agroterrorism: What is the threat and what can be done about it? http://rand.org/pubs/research_briefs/RB7565/RB7565.pdf.
Ravi, S., 2006. Security and the global supply chain. Transportation Journal 45 (4), 28–51.
Reese, A., 2007. Disaster proofing the supply chain. Supply and Demand Chain Executive 8 (3), 42–47.
Rice, J.B, Caniato, F., 2003. Building a secure and resilient supply network. Supply Chain Management Review 7 (5), 22–30.
Rijpma, J.A., 1997. Complexity, tight coupling and reliability: connecting normal accidents theory and high reliability theory. Journal of Contingencies and Crisis Management 5 (1), 15–23.
Rijpma, J.A, 2003. From deadlock to dead end: the normal accidents – high reliability debate revisited. Journal of Contingencies and Crisis Management 11 (1), 37–45.
Roberts, K.H., 1990a. Some characteristics of one type of high reliability organization. Organization Science 1 (2), 160–176.
Roberts, K.H., 1990b. Managing high reliability organizations. California Management Review 32 (4), 101–113.
Rinehart, L.M., Myers, M.B., Eckert, J.A., 2004. Supplier relationships: the impact on security. Supply Chain Management Review 8 (6), 52–59.
Russell, D.M., Saldanha, J.P., 2003. Five tenets of security-aware logistics and supply chain operations. Transportation Journal 42 (4), 44–54.
Sagan, S.D., 1993. The Limits of Safety: Organizations, Accidents and Nuclear Weapons. Princeton University Press, Princeton, NJ.
Sheffi, Y., Rice Jr., J.B., 2005. A supply chain view of the resilient enterprise. MIT Sloan Management Review 47 (1), 41–48.
Sheffi, Y., 2001. Supply chain management under the threat of international terrorism. International Journal of Logistics Management 12 (2), 1–11.
Sheffi, Y., 2005. The Resilient Enterprise. MIT Press: Cambridge, MA Southwest Airlines company website. Retrieved June 20, 2006 from http://www.southwest.com.
Spekman, R.E., Davis, E.W., 2004. Risky business: expanding the discussion on risk and the extended enterprise. International Journal of Physical Distribution and Logistics Management 34 (5), 414–433.
Strauss, A., 1987. Qualitative Analysis for Social Scientists. Cambridge University Press, Cambridge, England.
Strauss, A., Corbin, A., 1998. Basics of Qualitative Research: Techniques and Procedures for Developing Grounded Theory. Sage Publications, Thousand Oaks, CA.
Tang, C., 2006. Robust strategies for mitigating supply chain disruptions. International Journal of Logistics: Research & Applications 9 (1), 33–45.
Tenner, E., 1997. Why Things Bite Back: Technology and the Revenge of Unintended Consequences. Alfred A. Knopf, New York.
The Economist, 2002. Special report: When trade and security class—Container trade, 363(8267), April 6, 59–62.
United States Customs and Border Protection, 2004. CSI in Brief. http://www.cbp.gov/xp/cgov/border_security/international_activities/csi/csi_in_brief.xml (accessed January 8, 2007).
United States Department of Transportation Bureau of Transportation Statistics, 2005. Pocket Guide to Transportation. http://www.bts.gov/publications/pocketguide_to_transportation/2005/pdf/entire.pdf (accessed January 23, 2005).
Varkonyl, I., 2004. Breaking down silos in supply chain security. Journal of Commerce 8 (2), 1.
Voss, M.D., Whipple, J.M., Closs, D.J., 2009. The role of strategic security: Internal and external security measures with security performance implications. Transportation Journal 48 (2), 5–23.
Weick, K.E., 1987. Organization culture as a source of high reliability. California Management Review 29, 112–127.
Weick, K.E., 2004. Normal accident theory as frame, link, and provocation. Organization and Environment 17 (1), 27–31.
Weick, K.E, Sutcliffe, K.M., 2001. Managing the Unexpected—Assuring High Performance in an Age of Complexity. Jossey-Bass, San Francisco, CA, USA, pp. 10–17.
Wolf, F., 2001. Operationalizing and testing normal accidents in petrochemical plants and refineries. Production and Operations Management 10 (3), 292–305.
Wolf, F., 2005. Resource availability, commitment and environmental reliability & safety: a study of petroleum refineries. Journal of Contingencies and Crisis Management 13 (1), 2–11.