Journal of Transportation Management

Volume 23 | Issue 1 Article 6

4-1-2012

The physical distribution security system: Who is affecting the vulnerability of goods transprtation?

Luca Urciuoli
Cross-Border Research Association, University of Lund, Sweden, luca.urciuoli@gmail.com

THE PHYSICAL DISTRIBUTION SECURITY SYSTEM: WHO IS AFFECTING THE VULNERABILITY OF GOODS TRANSPRTATION?

Luca Urciuoli
Cross-Border Research Association
University of Lund, Sweden

ABSTRACT

The purpose of this study is to explore the vulnerability of physical distribution networks to antagonistic threats. Previous research identifies globalization and Just in Time (JIT) as the main causes of vulnerability. However, cargo crime has always existed, even before the identification of these trends. In this explorative study new factors are brought to light. In particular, it appears that stakeholders' dynamics are influencing the level of security.

INTRODUCTION

The vulnerability of supply chains to antagonistic threats, and more specifically their distribution networks, has become a major concern for managers (Spekman and Davis, 2004; Hintsa, 2011). This concern is supported by available statistics stating that industries are losing significant amounts of money and brand image due to theft, counterfeiting and pilferage of goods stored at terminals or in transport. For instance, statistics recently released by the European Union (EU) Parliament indicate that stolen lorries and goods in the EU add up to some E8.2 billion per year (European Parliament, 2007). In the United States (U.S.) the Federal Bureau of Investigation (FBI) has reported cargo theft in the range of $10-30 billion per year (Anderson, 2007). Counterfeiting is also a major concern for industries costing approximately $176 billion per year (Rodwell, et al., 2007).

The insecurity of supply chains is also of concern to governments. Recent terror events around the world (New York 2001, Madrid 2004 and London 2005) have increased the fear that: 1) products moved in supply chains could be contaminated or substituted with life-hazardous ones, 2) distribution chains could be used to smuggle nuclear weapons or terrorists, and 3) vehicles transporting dangerous goods or weapons for mass destruction could be used as a weapon against sensitive targets (Rice and Spayd, 2005). As a consequence, governments are actively working to secure their borders and inland transportation systems by setting policies and standards that ultimately demand supply chain companies operate under heightened security (Sheffi, 2001).

Previous research points out the importance of risk management approaches to deal with supply chain security (Giunipero and Eltantawy, 2004; Spekman and Davis, 2004). Spekman and Davis (2004) identify six categories of supply chain related risks and illustrate how to classify them. Giunipero and Eltantawy (2004) emphasize the importance of risk management approaches to evaluate end-to-end technology solutions. Some authors have developed supply chain security frameworks and illustrated future research needs (Autry and Bobbitt, 2008; Williams et al., 2008). Autry and Bobbitt (2008) have developed a framework to address how companies approach the mitigation of supply chain security by means of supply chain risk management. Williams et al. (2008) performed a literature review to categorize Supply Chain Security (SCS) factors and to identify a research agenda focusing on intra-organizational activities and quantitative approaches, making explicit the linkage between security and efficiency.

Few researchers have undertaken exploratory studies to discover which stakeholders determine the vulnerability of distribution networks to antagonistic threats. Some authors point out globalization and JIT as the main causes of the increased vulnerability (Crone, 2006; Khemani, 2007). Yet security problems in supply chain operations were known to exist for many years before the adoption of globalization and JIT principles. Other authors emphasize the importance of top management commitment, strategic priority, governmental regulation, security partnerships and willingness to pay as facilitators/inhibitors of security (Autry and Bobbitt, 2008; Voss et al., 2009b). However, none of the known authors has attempted to map a framework that shows which stakeholders affect the security of physical distribution networks. Hence, the suggestion for an additional hypothesis about other reasons that may actually be significant factors affecting the insecurity of physical distribution networks.

The purpose of this study is to perform an explorative inquiry to understand which stakeholders are influencing the security of physical distribution chains and most importantly how. By means of observations and semi-structured interviews, a framework for security in physical distribution networks is outlined and the interaction phenomena and dynamics among actors are determined. Finally, this paper discusses management implications and outlines the importance of further research on the physical distribution security topic.

METHODOLOGY

A qualitative methodology is used in this investigation. This method has been chosen because of the explorative nature of this study and also due to the novelty of the research topic in the transportation management literature, and the consequent lack of research constructs (Denzin and Lincoln, 2000; Autry and Bobbitt, 2008). The methodology consisted of three main phases relating to an approach to the literature review, a data collection plan, and methods of data analysis.

Approach to Literature Review

A literature search was performed within available academic journals to investigate previous security research in the fields of supply chain management, and transportation and logistics management. Keywords used for the search were "*transportation security,*" "*supply chain security,*" "*physical distribution security,*" and "*logistics security.*" Other secondary data from the internet as well as from trade magazines were incorporated into the empirical data collection. A preliminary system framework was developed based on the findings in the academic literature. Four main stakeholders, within and outside the supply chain, were identified: supply chain operators (including goods owners, transport and logistics providers), security solutions providers, criminals, and governments.

Data Collection Plan

Non-participant observations were made during a workshop and a seminar organized in Sweden and allowed for a better understanding of how the security problem is perceived by Swedish actors. The workshop was attended by 67 individuals that were divided into groups and encouraged to discuss the factors influencing the insecurity of distribution networks. The seminar was attended by 42 managers. It was soon apparent that the security system was more complicated than the one hypothesized after the literature review. As a consequence, further actors were added to the framework: including law enforcement agencies, insurance companies, voluntary security certification bodies, and contract legislation bodies.

Thereafter, to enhance the comprehension of the roles of these actors in the Physical Distribution Security System (PDSS) and their reciprocal interactions, a total of 16 interviews were conducted, four unstructured and 12 semi-

TABLE 1
DEMOGRAPHIC CHARACTERISTICS OF RESPONDENTS

	Industry	Position
Respondent 1	Electronics Manufacturer	Security manager
Respondent 2	Transportation	Lawyer
Respondent 3	Road Carrier	Security Manager
Respondent 4	Logistics Service Provider	Global Security Manager
Respondent 5	Food Products	Security Manager
Respondent 6	Pharmaceutical	Security Manager
Respondent 7	Cash Transportation	Security Manager
Respondent 8	Law Enforcement Agency	Police inspector
Respondent 9	Security Certification	International Sales Manager
Respondent 10	Logistics Service Providers	Regional Security Manager
Respondent 11	Security Solution Provider	Commercial Director
Respondent 12	Road Carrier	CEO
Respondent 13	Security Solution Provider	CEO
Respondent 14	Shipping company	Senior Director
Respondent 15	Shipping Company	Corporate Security Manager
Respondent 16	Insurance Company	Claims Manager

structured. The respondents to be interviewed were chosen from a convenience sample of individuals joining a Scandinavian research project dealing with transportation security. Table 1 shows the demographic characteristics of the sample interviewed.

The interviews were completely unstructured in the beginning of the research to gain a better understanding of key topics and add the widest range of possible information. These interviews were meant to let the respondents freely discuss the main causes of the vulnerability of physical distribution networks to antagonistic threats. Once these topics became more defined, semi-structured interviews with more pointed questions were used. The scheme used for the semi-structured interviews is provided in Appendix A. After eight interviews it was clear that the factors highlighted by the respondents corresponded with those identified during the observation sessions. Hence, four more interviews were carried out to ensure saturation of the data before discontinuing data collection (Glaser and Strauss, 1967; Easterby-Smith et al., 1991).

Methods of Data Analysis

Using content analysis, themes and constructs were derived from the interviews and merged with those found in the literature search. To enhance validity of the findings, the following quality criteria were considered during the data collection and analysis: credibility, dependability, transferability and confirmability (Guba and Lincoln, 1989; Lambert et al. 2004; Autry and Bobbitt, 2008). Credibility concerns how the personal constructs of the respondents match the researchers' perceptions. The observations made at the workshop were compared with the results obtained by a consulting firm that was responsible for documenting the workshop. In addition, since recording of interviews was not allowed, the answers provided during the interviews were verbally repeated to the respondents to confirm the interpretation provided by the researcher.

Dependability refers to the temporal stability of the data. The data collection was initiated with unstructured interviews and improved with the development of a semi-structured questionnaire. To enhance the stability of the data, only the

responses from the semi-structured interviews were used in the analysis. Transferability is the ability to apply the results to other contexts. The interviews were performed with managers belonging to a wide set of organizations within and outside Sweden. Likewise, the seminar and workshop where observations were performed included representatives from diverse logistics companies in Sweden. Finally, confirmability is the extent to which the findings reflect the data collected. This was ensured by keeping notes of the data collected at the observations and during the interviews.

LITERATURE REVIEW

The literature scanned in peer-reviewed logistics, transportation and supply chain management journals and conference proceedings is reported in this section by highlighting the main stakeholders that influence the security of distribution networks: 1) supply chain, logistics and transport operators, 2) security solutions providers, 3) criminals, and 4) governments.

Supply Chain, Logistics and Transport Operators

The influence of supply chain, logistics and transport operators is identified by previous research exploring the following factors: globalization and JIT trends, security partnerships, risk sharing among transport purchasers and sellers, and willingness to pay. Globalization and JIT trends are exposing supply chains to higher risks. Moving products within and to foreign countries where companies lack knowledge of local culture, authorities and legislation makes it difficult to protect cargo (Crone 2006; Khemani 2007; Sheffi, 2001). Crone (2006) compares today's globalization strategies to the classic story of the Trojan War where the Trojans "failed to see the risks of what appeared to be a benefit." Just in Time (JIT) trends tighten supply chains in a way that increases the consequences of disruptions and thereby increasing the risks of security incidents in distribution networks (Khemani, 2007). According to an analysis performed by Wilson (2005), JIT manufacturing and deliveries, and streamlined order fulfilment techniques, can reduce in-transit and on-hold inventories but can also severely increase the magnitude of disruptions.

In Autry and Bobbitt (2008) as well as in Voss et al. (2009b) the importance of security related partnerships covering contractual agreements and risk and reward sharing among actors is emphasized. The authors maintain that encouraging collaboration among supply chain members and specifying security requirements in contractual agreements may improve the security of distribution chain assets and operations. In addition, risk sharing and rewards are also fundamental practices to stimulate stakeholders into taking their share of responsibility and working actively with security.

Only one article explored an issue concerning owners' willingness to pay for goods as an inhibitor of physical distribution security (Voss et al., 2009a). According to the authors supply chain firms are not always willing to pay for firms offering advanced security transportation. By means of a survey sent to manufacturing industries in the food sector, the authors demonstrate the positive relationship between concern over security incidents and preferences for advanced security as well as willingness to trade off price for advanced security. The findings show that price, and delivery reliability, is more important than security when contracting suppliers. Hence, security is not a top priority when selecting distribution carriers.

Security Solutions Providers

The importance and the fundamental role of security solution providers to the insecurity of physical distribution are emphasized by several authors. Downey (2004) encourages industry

leaders to identify research and technology resources that can minimize the threats along distribution chains. According to the author, technology can fight the "*asymmetrical threat posed by terrorists,*" which consists of enemies seeking supply chains' weak points instead of trying "*to overcome them by using superior force.*" Sheffi et al. (2003) propose technological solutions for preventive and recovery operations to be implemented in three areas: physical security, information security and freight security. Autry and Bobbitt (2008) point out the importance of security-dedicated communication and technology, i.e. the implementation of GPS monitoring, RFID and similar technologies to monitor and enhance security in supply chains.

Another issue found in previous research is the impact of security solutions on the efficiency of supply chains. Some authors believe that the introduction of security in physical distribution may bring higher efficiency, but others don't. Sheffi (2001) states that security enhancement can also bring "collateral benefits" such as trade facilitation, asset visibility and tracking, faster standard development, etc. Other authors assert that in some cases security measures conflict with the concepts of lean logistics. According to Powanga (2006), basic logistics performance indicators can be expressed as revenues (order fulfilment), operating costs (in transit inventory, transportation, insurance premiums, buffer stock carrying costs), fixed costs (facilities, capital utilization) and working capital (buffer stock levels). Likewise, Mazeradi and Ekwall (2009) show, by means of a survey, how the implementation of the ISPS-code may increase paperwork and slow down processes in port terminals.

Criminals

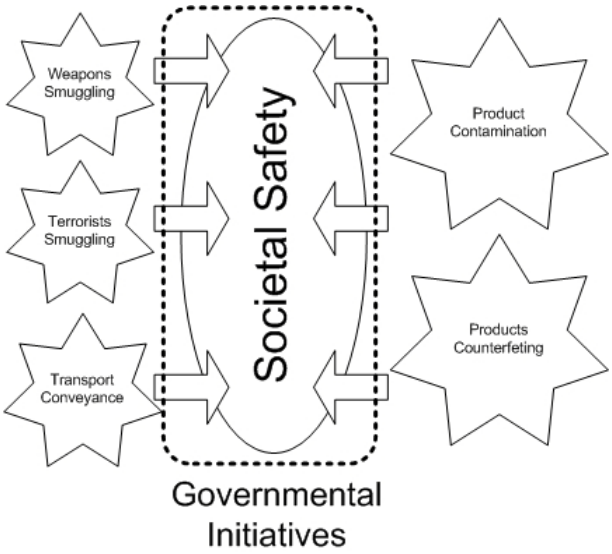
The behaviour of criminal groups targeting physical distribution is also a factor that may discourage the enhancement of security. Ekwall (2009) affirms that diverse typologies of crime may be related to attacks against physical distribution: situational crime, professional crime and crime displacement effects. Situational crime is determined by a rational choice made by weighing diverse factors such as effort, potential payoff, risk of apprehension and punishment, and individual needs. A variation of situational crime is the professional theft that is based on methodical plans and takes advantage of high-tech methods to defeat protection measures (Ekwall, 2009; Ekwall and Lumsden, 2007). Ekwall (2009), according to the principles of the routine activity theory, identifies three elements characterizing cargo theft: a perpetrator, a supply chain (the criminals' target) and the lack of protective measures. Insufficient protection in one of the links of a distribution chain will determine a weak point and the consequent attack (crime displacement effect). Hence, the low protection of distribution chains makes them attractive to criminals. At the same time, the opportunistic behaviour of criminals may discourage operators from protecting their assets.

Governments

Governments are mainly afraid of the terror threats hidden in the vulnerability of supply chains. These hidden threats include the smuggling of weapons or terrorists, contamination or counterfeiting of products and usage of transport conveyances as weapons. Therefore diverse initiatives have been started by governments around the world to prevent catastrophic consequences for society. See Figure 1:

The first security enhancements were implemented in the air sector a few months after the attacks in New York. The sea sector followed almost immediately when a standard framework for the identification and assessment of vulnerabilities in sea transportation and port facilities was included in the International Ship and Port Facility Security Code (ISPS) (Katarelos and Alexopoulos, 2007; Bichou, 2004).

FIGURE 1
THREATS TO SOCIETAL SAFETY



The involvement of governments is mentioned in Sheffi (2001) as well as in Sheffi et al. (2003). According to these authors, the upcoming security regulations for C-TPAT (Customs-Trade Partnership Against Terrorism), the AEO (Authorized Economic Operator) and the ISPS code could force many distribution firms to enhance their security levels.

DATA ANALYSIS

In this section the findings from the literature review are combined with the empirical data collected from observations and interviews. Combining the literature review and the observations, some of the following stakeholders emerged as key players in security. The first section which follows deals with findings from the observations specifically. The second section deals with findings that came directly from interviews of the actors.

Observations

The observations were carried out on the occasion of two events. First, a workshop organized by a Swedish Law Enforcement Agency. And secondly, at a seminar organized by one of the main Scandinavian insurance companies. During these events, issues related to the increasing attacks against distribution networks were discussed and possible solutions were elaborated on. Following are some of the findings that emerged by organizational type. These organizations include several new ones that were brought to light during the workshops and these include law enforcement agencies, voluntary certification organizations, insurance companies, and contract legislation bodies.

Supply Chain, Logistics and Transport Operators
The central role of supply chain, logistics and transport operators is confirmed by the high attendance of representatives at the workshops. However, only the construct related to the "willingness to pay for security" of transport buyers was discussed. The rest of the constructs generated during the literature review were not directly mentioned in the workshops.

Security Solutions Providers
During the workshops the importance of security solutions to protect cargo during transit was highlighted by the participants; however no detailed discussion was undertaken on the topic. On the contrary, secondary data present extensive discussions on this issue. Most of the literature found concerned the "*collateral*

benefits" brought by security investments such as trade facilitation, asset visibility and tracking, faster standard development, etc. (Rice and Spayd, 2005). The same concept of "*collateral benefits*" is discussed by Peleg-Gillai et al. (2006) and Closs and McGarrell (2004). Willys and Ortiz (2004) emphasize that efficiency and security in supply chain transportation are closely interrelated. Since higher security may reduce customs delays so may the higher transparency of information of goods flows reduce shipping costs and time. The same literature acknowledges the difficulty in reliably evaluating security investments. According to Rice and Spayd (2005) return on investments are difficult to estimate because of the complexities in evaluating how well a security solution can prevent a problem from occurring, how frequently this would happen, and how cost savings will be determined.

Government Authorities

The role of governments is mentioned by many authors in previous literature (Closs and McGarrell, 2004; Abbott et al., 2003; Sheffi et al., 2003; Rice and Spayd, 2005; Willys and Ortiz, 2004). All the authors are convinced that authority regulations may disrupt transportation flows due to Customs' delays; even though security will be enhanced. In addition, some authors also point out that the absence of business cases, solid ROIs and clear guidelines from governments, is frightening many operators and may result in declining interest towards the enhancement of distribution security (Lee, 2004; Rice and Spayd, 2005). However, the role of governments was not mentioned in any of the workshops.

Law Enforcement Agencies

The role of law enforcement agencies in preventing attacks, as well as in supporting operators efforts in recovering their shipments, was mentioned in both workshops. During the events, representatives from law enforcement organizations encouraged transportation companies to report cargo theft and improve collaboration with law enforcement. Law enforcement agencies were also criticized by the participants since they don't often prioritize cargo theft among their activities nor do they properly prosecute cargo criminals. The issue concerning the low prosecution of criminals has also been found in articles published in trade journals (Badolato, 2000; Anderson, 2007).

Voluntary Certification Organizations

Many participants to the workshop mentioned the existence of TAPA EMEA (Transported Asset Protection Association) - an organization supporting transportation buyers and sellers with recommendations and guidelines to secure transportation assets (TAPA EMEA, 2008). Participants believed that the implementation of routines and specific technologies suggested by the organization may enhance physical distribution security. Other secondary data mention the International Standards Organization (ISO) certification as a means to enhance supply chain security. The ISO proposes best practices and minimum requirements for supply chain management, recommends technologies (i.e. mechanical locks or electronic seals), and establishes communication standards for radio frequency based security solutions (Liard, 2007; ISO, 2008).

Insurance Companies

The role of insurers concerns the coverage of the risks related to loss or damage of the goods during a transportation assignment. All the mentioned parties involved in goods transportation, including consignors and consignees, LSPs and transport carriers, have the opportunity to buy property or liability insurance, according to what is stated in the contract. Likewise, stakeholders have the option of retaining part of these risks so as to pay lower premiums.

The role of the insurance companies is confirmed in both the events where observations were performed. The data collected actually indicate that many operators blame insurance companies for increased security problems. Managers were expecting not only financial solutions but also practical support in choosing security measures and defining security levels in transport operations. Another finding from the workshops is that if security requirements are not specified in contracts, operators with a risk-seeking attitude can trade off the costs for insurance premiums and excesses with the costs of implementing security solutions.

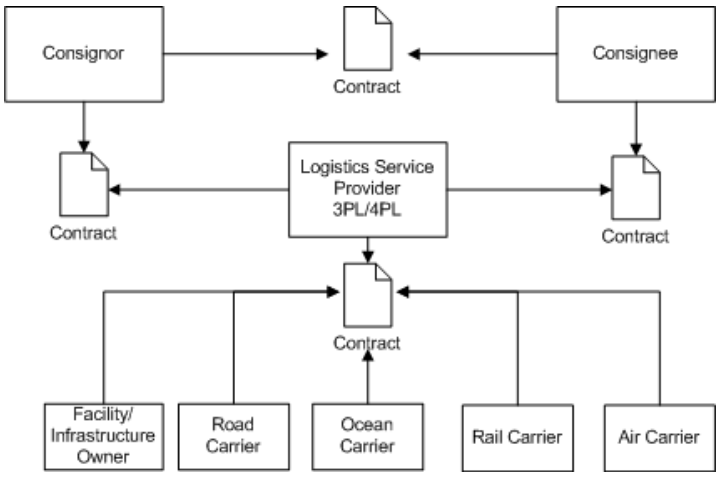
Other secondary data used for the analysis and related to insurance companies concern mostly the procedures to sub-contract carriers, transfer risks as well as current regulations to define cargo liabilities (Stöth, 2004; ICC, 2008; NSAB, 2000).

Contract Legislation Bodies

Participation in the workshops also unveiled the importance of contract legislation in the definition of security requirements in distribution operations. According to secondary literature, the relationships among actors involved in a shipment are regulated by specific laws. While transportation disputes are stated in international conventions and rules (i.e. CIM, CMR conventions), logistics matters concerning such operations as inventory management, labelling or packaging are not put under any convention and are primarily determined by industrial organizations or private agreements (i.e. Incoterms 2000 and NSAB 2000). As has already been mentioned, different agreements have to be executed to move the goods from the consignor to the consignee. See Figure 2 below. These can be performed in verbal or written form (Stöth, 2004).

Existing regulations like Incoterms or NSAB 2000 focus on the transfer of risks among actors and indicate Combiterms as a means to split costs among players. In addition, in case of loss these agreements oblige the reimbursement of the goods invoice value plus 10% for indirect costs (ICC, 2008; NSAB, 2000). In these agreements, nothing is specified about security requirements for transportation assignments and how related costs should be split among actors.

FIGURE 2
CONTRACTUAL RELATIONSHIPS



(Adapted from STÖTH, 2004, pp. 22)

The findings from the observations also reveal that it is crucial to specify security requirements in the contracts between transport buyers and sellers. However, the legislation bodies, today, don't provide any support for this and operators perceive this process as complicated and resource and time demanding. As a consequence, often verbal agreements are preferred by companies.

Interviews of Organizations

The interviews highlighted the following stakeholders as influencing the security of physical distribution networks: 1) law enforcement agencies, 2) supply chain, logistics and transport operators, 3) criminals, 4) contract legislation bodies and 5) other authorities.

Law Enforcement Agencies

The interviews confirmed the relevance of law enforcement agencies in the discussion concerning physical distribution security. According to three of the respondents, the problem faced today is that the amount of theft claims received from transport operators is not high enough to justify an increase of resources to combat criminals. At the same time, transport operators are afraid to show their brands in theft statistics. In addition, they feel that this is only an administrative cost that will rarely lead to cargo recovery.

"Transport operators are afraid to show their brand names in theft statistics and therefore they don't announce the problem to the police that in its turn doesn't have the real picture of the situation".

"Operators are not claiming enough, thus we cannot allocate resources adequately."

"Our company has a good cooperation with the national law enforcement agency. However we know that many thefts are not reported by other companies. This makes it hard to combat cargo theft."

Two respondents also said that to reduce the increase in cargo theft experienced during recent years, Swedish law enforcement agencies must develop programs to increase awareness about the cargo security problem.

"The activities organized by the law enforcement agency have contributed to increase awareness of the cargo theft problem"

"Thanks to the workshops we have had the possibility to come closer to the law enforcement agency and strengthen collaboration"

Finally another problem mentioned in the interviews was that existing laws to prosecute criminals are not strong enough to discourage thieves from taking chances in assaulting cargo moving in distribution networks. As a consequence, it is not only difficult to capture thieves but also to keep them in custody.

"Criminals attack according to a trade-off between risks and revenues. The situation today is that supply chains are easy and profitable targets. At the same time prosecution is not severe enough to discourage perpetrators."

"Once criminals are captured, we can keep them in custody for a limited amount of time. So they are back in business after only few months."

"Prosecution should be more severe to discourage criminals attacking our supply chains."

Supply Chain, Logistics and Transport Operators

The role of supply chain actors, including logistics and transport providers, is also outlined in the interviews. The complexity necessary to develop and formalize agreements among all the actors, especially with the physical carriers (road, rail, sea, and air carriers), or between them (a carrier contracting another carrier) is also discussed in the interviews. Transportation carriers are companies owning fleets of vehicles including vessels, airplanes, trucks, and in some cases even trains (companies are usually state owned). Often, within the road sector, the transport carrier can even be the driver and his vehicle. Therefore the complexity and administrative burden experienced, concerning laws, regulations and standard contracts, makes informal verbal agreements more congenial.

"It happens that some carriers mention and stress the complexity of the contracts or standard agreements. Large industries or LSPs can handle them but often small-medium transport carriers can prefer verbal agreements"

"According to our experience the standard agreements are perceived as too complex and it has happened that carriers prefer verbal agreements"

"We know that in some cases carriers are engaged with verbal agreements"

"As an insurance association we have had cases in which transportation carriers had been engaged with verbal agreements"

Four managers mentioned the difficulties encountered in raising their prices to enhance security. In two of the interviews, the respondents highlighted the fact that goods owners requesting higher security must be willing to pay for it.

"Security costs have to be internalized into our freight rates. Thus it is difficult for us to remain competitive on the marketplace"

"Some customers are willing to pay for extra costs related to security. Thus we increase our prices. In some cases we also perform a negotiation process with the transport carriers to define how security costs, direct and indirect, have to be split"

The interviews also bring to light the influence of insurance companies. According to one of the interviewed professionals, some Scandinavian insurers appear to exert pressure on their customers, denying premium discounts to those retaining risks by purchasing or implementing security measures.

"We have a dialogue with only one insurance company and they are not willing to give us premium reductions. This is nonsensical..."

Two respondents declared that insurances' "excesses" are too high and therefore operators prefer to pay the consequences of a loss themselves instead of investing in security.

"We know that if the loss is lower than the insurance excesses than we prefer to pay it ourselves"

"We have insurances and also our transport carriers do. However we know that companies prefer to pay the losses themselves, since the excesses are too high."

Finally when it comes to application of premium discounts, opinions diverge. Two respondents state that they encounter difficulties in agreeing on discounts. Conversely, three respondents declared that it is possible to have discounts, although in some cases these are too low and affect only the excesses.

Security Solutions Providers

All the interviewed managers agree on the central role of security solutions in the protection of distribution chains. Best practices and technical systems may strongly decrease cargo attacks. Three of the interviewed professionals underlined the importance of using security solutions to combat criminals attacking distribution chains.

"We work intensively with detection sensors to be installed at our facilities and protect them against various threats. These sensors include motion detection or perimeter alarms to be installed at main doors or windows."

"We put a great emphasis on security technologies, and when it comes to the protection of our facilities we want to be a step ahead our competitors"

"Our terminals are highly secured although it is often difficult to have the security budget approved by top management"

Three respondents stated that some security solutions are too expensive.

"We make assessments of technologies 'on offer.' However most of these systems cannot guarantee 100% security and cost too much money. You can imagine the financial implications to implement these systems on a fleet of a hundred vessels"

"As a security manager I get a limited budget to spend on security. Thus it is difficult to buy more advanced technologies"

"… only those companies that have access to money and resources can properly deal with the problem"

Criminals

The perception of the criminals' opportunistic behaviour is also emphasized in previous research. Insufficient protection in one of the links of a supply chain will determine a weak point and the consequent attack (crime displacement effect). Four respondents confirmed this line of reasoning:

"Criminals search for weak points and attack in specific places where they know trucks stop."

"Criminals attack according to a trade-off between risks and revenues. The situation today is that supply chains are easy and profitable targets."

"Security solutions may become ineffective after a while. Criminals learn quickly how to deceive the installed equipment"

"It is very important to set up the best practices very quick. However the situation is very dynamic. This means that if somebody is implementing some practice or measure to avoid attacks than also the criminals will modify their behaviours to overcome the resolutions."

It can be argued that the increased threats and attacks against distribution networks should stimulate companies to increase their security levels: first of all to stop the losses due to theft, and secondly to comply with upcoming mandatory requirements meant to stop terrorists. However, as one respondent commented, this is not happening:

"Statistics show increasing attacks against freight transportation. Nevertheless, for reasons I can't understand, operators don't consider this as a problem and are not seeking adequate protection".

Contract Legislation Bodies

The role of contract legislation is also mentioned in the interviews. All the respondents agree that the specification of security requirements in contracts may enhance security even though it requires both a deep understanding of physical security and achieving an agreement among parties. Only one respondent mentions that contract agreements may be useless, since it is difficult to verify if a carrier is truly following the security measures specified in the contract. As this manager commented, "we request our carriers to install specific security measures, but we don't really know if they follow them or not."

Authority

Many of the interviewed respondents have knowledge of the authority regulations. Seven managers mentioned that they know the AEO, ISPS or C-TPAT initiatives, but only two of them declared that the AEO initiative can influence their security investments.

"We are participating to the AEO initiative set up by the European Commission and are working to gain compliance."

"Yes, we are working to meet the AEO requirements since it is our desire to secure our operations. In addition, it is important to gain compliance to simplify customs inspections and avoid transport delays."

CONCLUSION

The findings from this explorative study show diverse factors that may be responsible for the vulnerability of supply chains and more specifically of their physical distribution systems. Previous research identifies globalization and JIT as the main causes. However, by combining these findings with data collected from secondary sources, observations, and a total of 16 interviews (4 unstructured and 12 semi-structured) performed with key actors in the transport security area, the identification of eight players and their interactions into an integrated Physical Distribution Security System can be outlined. This constitutes an environment in which other stakeholders and reasons are brought to light as significant factors.

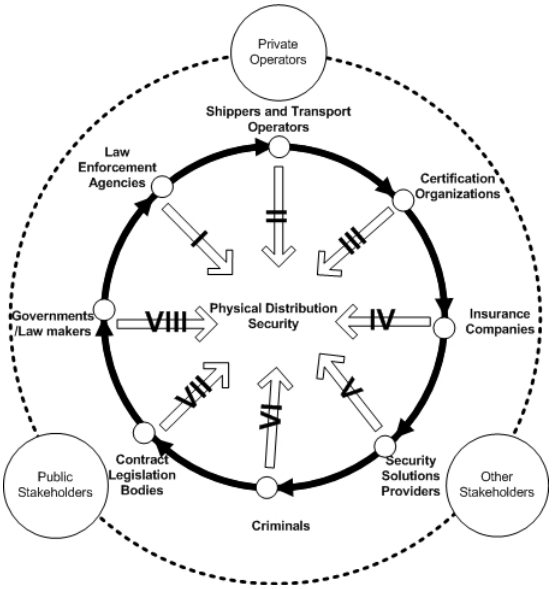
The Physical Distribution Security System is illustrated in Figure 3 below, where each actor is depicted with a Roman Numeral and arrows show the interdependency among the actors and the physical distribution security. Summing up,

the initiatives organized by the first actor (Actor I in the figure), the law enforcement agency, may positively stimulate the development and implementation of cooperative solutions to increase security. However, the behaviours of some distribution operators that don't announce the theft assaults make it difficult for the agency to allocate enough resources to combat cargo crime. At the same time, existing criminal laws are not able to properly prosecute cargo crime, which may discourage some companies to denounce cargo crime. The second actor (Actor II, supply chain, logistics and transport operators) experiences difficulties in defining security partnerships. Existing standard legislative commitments are too complex and at the same time don't support the definition of security requirements. This study confirms that the willingness to pay for secured freight transportation is still too low and the low marginal revenues that are typical of the transportation market make it difficult to afford security investments.

The certification organizations (Actor III, i.e. TAPA EMEA or ISO28000) represent an incentive for distributors to raise their security level and gain access to a network of secure operators. In addition, standards, recommendations, and best practices can support shippers and transport operators in securing their assets and operations. The insurance companies, (Actor IV), seem to have both a negative and positive effect on the security of physical distribution. The negative impact is that it may happen that risk-seeking companies may trade-off insurance premiums and excesses with the implementation of security solutions. Nevertheless, insurance companies may stimulate the enhancement of security by offering premium discounts to distribution operators.

The providers of security solutions are also encountering difficulties (Actor V). While the development of security technologies and services offer the possibility to automate or outsource the processes for enhancing security in a cost effective manner, companies perceive costs as too high. At the same time, absence of business cases and operational standards results in most security solutions being viewed as not mature enough to be fully implemented in physical distribution. The behaviour of

FIGURE 3
THE PHYSICAL DISTRIBUTION SECURITY SYSTEM (PDSS)



criminals may also discourage the enhancement of security (Actor VI). As long as there are weak links or nodes in a distribution chain, attacks will not decrease but will only move from the protected spots. Contract legislation bodies (Actor VII) are today used to define transport assignments as well as cargo liabilities among all the involved stakeholders. However, these don't provide any support for agreed upon security requirements to be adopted. At the same time, it is not possible to verify that physical carriers follow what is stated in the contract. Finally, governments also have a significant role in the enhancement of security in physical distribution (Actor VIII). Many believe that regulations may stimulate operators; however there is still confusion and uncertainty about the costs and related requirements of the authority certifications. Thus many companies are waiting.

Implications, Future Research and Limitations

This manuscript reveals practical implications for managers as well as the necessity to conduct further research. The practical implication of this investigation is to use the framework in Figure 3 to stimulate stakeholders to identify initiatives that could bring mutual benefits and higher security to all the actors identified in the PDSS. The main recommendation is to accomplish this objective by promoting collaboration opportunities that may introduce new driving forces, remove the existing barriers or perhaps turn the barriers into driving forces.

Future research should be oriented to performing more descriptive studies based on empirical data to confirm the hypotheses found in this paper. Is it true, as previous investigations point out, that insecurity in supply chains is merely caused by such factors as globalization and JIT? Or may other inter-organizational relationships complicate the implementation of security measures as well as discourage distribution operators? In terms of limitations, the main data used for the analysis is collected by means of qualitative techniques and is based on a restricted number of interviews. Therefore subjectivity of interpretations as well as limited generalizability of the findings is acknowledged.

Once the factors explaining the vulnerability of supply chains to antagonistic attacks have been clearly identified, normative research should be performed to understand how the stakeholders' goals may be aligned and, thereby, supply chain security improved. Enhancing security within a supply chain requires the involvement of multiple stakeholders that need to agree on a specific degree of protection and thereby specify security requirements in supply or transportation contracts. This process today presents many difficulties for practitioners, and the research challenges concern the development of standard agreements in which security requirements are specified, achievement of consensus, sharing of responsibilities, internalization of security costs as well as risk and cost sharing among stakeholders. Another important aspect is the standardization and harmonization of security across supply chains. As many authors state, "*a supply chain is as secure as the weakest of its links.*" Therefore it is essential that stakeholders speak the same security language and strive to align the protection level of all the nodes and links of a supply chain network. Especially from a technological viewpoint, a standardization process of security technologies has to be initiated.

REFERENCES

Abbott, G., Rosalind, T., and Brandt, L. (2003), "Commercium Interrupts: Supply Chain Responses to Disaster," *Acquisition Policy*, Fort McNair, Washington, D.C. 20319-5062.

Anderson, B. (2007), "Securing the Supply Chain – Prevent Cargo Theft," *Security*, 44(5): 56-58.

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

Badolato, E.V. (2000), "Smart Moves Against Cargo Theft," *Security Management*, 44(7): 110-115.

Bichou, K. (2004), "The ISPS Code and the Cost of Port Compliance: An Initial Logisitcs and Supply Chain Framework for Port Security Assessment and Management," *Maritime Economics and Logistics*, 6: 322-348.

Closs, D.J., and McGarrell, E.F. (2004), "Enhancing Security Throughout the Supply Chain," IBM Center for the Business of Government, *Special Report Series*, April 2004.

Crone, M. (2006), "Are Global Supply Chain too Risky? A Practitioner's Perspective," *Supply Chain Management Review*, 10(4): 28-35.

Denzin, N.K., and Lincoln, Y.S. (2000), *Handbook of Qualitative Research*, Sage Publications, Thousands Oaks, US.

Downey, M.L. (2004), "The Challenge of Transportation Security," *Supply Chain Management Review*, 8(2): 9-10.

Ekwall, D. (2009), "The Displacement Effects in Cargo Theft," *International Journal of Physical Distribution and Logistics Management*, 39(1): 47–62.

Ekwall, D., and Lumsden, K., (2007), "Differences In Stakeholder Opinion Regarding Antagonistic Gateways within the Transport Network, *Nofoma Proceedings*, Reykjavik, 2007.

Easterby-Smith, M., Thorpe, R., Lowe, A. (1991), *Management Research: An Introduction*, SAGE Series in Management Research, First Edition.

European Parliament (2007), "Organised Theft of Commercial Vehicles and their Loads in the European Union, Directorate General for Internal Policies of the Union," [On-line] Available: http://www.nea.nl/index.cfm/16,829,c,html/829/Theft%20of%20commercial%20vehicles_EN%20(3).pdf. Accessed: 08/06/06.

Giunipero, L.C., and Eltantawy, R.A. (2004), "Securing the Upstream Supply Chain: A Risk Management Approach," *International Journal of Physical Distribution and Logistics Management*, 34(9): 698-713.

Glaser, B.G., and Strauss, A.L., (1967), *The Discovery of Grounded Theory: Strategies for Qualitative Research*, Aldine Transaction, New York.

Guba, E., and Lincoln, Y. (1989), *Fourth Generation Evaluation*, Sage Publications, Thousand Oaks, CA.

Hintsa, J. (2011), *Post-2001 Supply Chain Security – Impacts on the Private Sector,* Doctoral Thesis Dissertation, Lausanne, Switzerland.

ICC (2008), Incoterms, "ICC - International Chamber of Commerce, International World Organization", [On-line]. Available: http://www.iccwbo.org/incoterms/id3045/index.html. Accessed: 15/03/08.

ISO (2008), "International Organization for Standardization (ISO) – International Standards for Business", Governments and Society, [On-line]. Available: http://www.iso.org/iso/home.htm. Accessed: 11/04/08.

Katarelos, E.D., and Alexopoulos, A.B. (2007), "The Master's Role in Relation to the Safety of the Port, Particularly Under the Concept of the ISM and the ISPS Codes", paper presented at *International Symposium on Maritime Safety, Security and Environmental Protection*, 20th September 2007, Athens (Greece).

Khemani, K. (2007), "Bringing Rigor to Risk Management,"*Supply Chain Management Review*, 11 (2): 67.

Lambert, D.M., Knemeyer, A.M., and Gardner, J.T. (2004), "Supply Chain Partnerships: Model, Validation and Implementation," *Journal of Business Logistics*, 25(2): 21-42.

Lee, Hau L. (2004), "Supply Chain Security – Are You ready?," *Stanford Global Supply Chain Management Forum,* 3rd September 2004.

Liard, M. (2007), "Cargo Container Security Tracking - RFID", *Cellular and Satellite Communications for Supply Chain Management and National Security*, ABI Research.

Mazeradi, A. and Ekwall, D. (2009), "Impacts of the ISPS Code on Port Activities – A Case Study on Swedish Ports," *World Review of Intermodal Transportation Research*, 2(4): 326-342.

NSAB (1998), "NSAB 2000 - General Conditions of the Nordic Association of Freight Forwarders," [On-line]. Available: http://www.nordicfreight.org/nsabsve.pdf. Accessed: 01/06/08.

Peleg-Gillai, B., Bhat, G., and Sept, L. (2006), Innovators in Supply Chain Security - Better Security Drives Business Value, *Stanford University - The Manufacturing Institute*, The Manufacturing Innovation Series.

Powanga, L. (2006), "A Business Perspective of US International Seaborne Security Measures: Impact on Importers," *Journal of Global Business*.

Rice, J.B., and Spayd, P.W. (2005), *Investing in Supply Chain Security: Collateral Benefits*, IBM Center for Business of Government.

Rodwell, S., Van, E.P., Reid, A., and Walendowski, J. (2007), "Study: Effects of Counterfeiting on EU SMEs and a Review of Various Public and Private IPR Enforcement Initiatives and Resources," [On-line]. Available: http://ec.europa.eu/enterprise/enterprise_policy/industry/doc / Counterfeiting_Main%20Report_Final.pdf. Accessed: 31/08/07.

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

Sheffi, Y., Rice, J.B., Fleck, J.M., and Caniato, F. (2003), "Supply Chain Response to Global Terrorism: A Situation Scan," paper presented at EurOMA-POMS Conference, 17th June 2003, Como (Italy).

Spekman, R.E., and 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.

Stöth, G. (2004), *Transport- och Logistikrätt*, Industrilitteratur, Lidingö, 2004.

TAPA EMEA (2008), "TAPA EMEA Transported Asset Protection Association," [On-line]. Available: http://www.tapaemea.com/public/. Accessed: 01/02/08.

Voss, M.D., Closs, D.J., Calantone, R.J., and Helferich, O.K., (2009a), "The Role of Security in the Food Supplier Selection Decision," *Journal of Business Logistics*, 30(1): 127 – 155.

Voss, M.D., Whipple, J.M. and Closs, D.J., (2009b), "The Role of Strategic Security: Internal and External Security Measures with Security Performance Implications," *Transportation Journal*, 48(2): 5 -24.

Williams, Z., Lueg, J.E., LeMay, S.A. (2008), "Supply Chain Security: An Overview and Research Agenda," *The International Journal of Logistics Management*, 19(2): 254–281.

Willys, H.H., and Ortiz, D.S. (2004), "Evaluating the Security of the Global Containerized Supply Chain", RAND Corporation, Santa Monica, CA.

Wilson, M.C. (2005), "The Impact of Transportation Disruption on Supply Chain Performance," *Transportation Research Part E*, 43(4): 295-320.

Acknowledgments: The author would like to thank the Next Generation Innovative Logistics (NGIL), a VINNOVA Excellence Center based at Lund Institute of Technology, Sweden, for the financial support provided for this study.

AUTHOR BIOGRAPHY

Luca Urciuoli (Ph.D., University of Lund, Sweden) is Research Director at the Cross-Border Research Association (CBRA) in Switzerland. Previously he worked as Project Manager at Volvo Technology where he patented an application for transport security. He earned an MSc Degree in Industrial Engineering at Chalmers, University of Technology in Sweden. His research interests include supply chain/transportation security and information and communication technologies. His papers have been published in diverse conference proceedings and in scientific journals. This paper was written while Dr. Urciuoli was at University of Lund. E-Mail: luca.urciuoli@gmail.com