<http://www.diva-portal.org>

Postprint

This is the accepted version of a paper published in . This paper has been peer-reviewed but does not include the final publisher proof-corrections or journal pagination.

Citation for the original published paper (version of record):

Urciuoli, L., Hintsa, J. (2017)

Adapting supply chain management strategies to security—an analysis of existing gaps and recommendations for improvement

International Journal of Logistics Research and Applications, 20(3): 276-295

Access to the published version may require subscription.

N.B. When citing this work, cite the original published paper.

Permanent link to this version:

<http://urn.kb.se/resolve?urn=urn:nbn:se:kth:diva-244441>

International Journal of Logistics Research and Applications

A Leading Journal of Supply Chain Management

ISSN: 1367-5567 (Print) 1469-848X (Online) Journal homepage: <https://www.tandfonline.com/loi/cjol20>

Adapting supply chain management strategies to security – an analysis of existing gaps and recommendations for improvement

Luca Urciuoli & Juha Hintsa

To cite this article: Luca Urciuoli & Juha Hintsa (2017) Adapting supply chain management strategies to security – an analysis of existing gaps and recommendations for improvement, International Journal of Logistics Research and Applications, 20:3, 276-295, DOI: [10.1080/13675567.2016.1219703](https://doi.org/10.1080/13675567.2016.1219703)

To link to this article: <https://doi.org/10.1080/13675567.2016.1219703>

Published online: 11 Sep 2016.

Submit your article to this journal [↗](#)

Article views: 358

View Crossmark data [↗](#)

Citing articles: 4 View citing articles [↗](#)

Adapting supply chain management strategies to security – an analysis of existing gaps and recommendations for improvement

Luca Urciuoli^a and Juha Hintsala^{b,c}

^aMIT International Logistics Programme, Zaragoza Logistics Center, Zaragoza, Spain; ^bCross-border Research Association, Lausanne, Switzerland; ^cDepartment of Operations, HEC Université de Lausanne, Lausanne, Switzerland

ABSTRACT

The purpose of this paper is to determine the main security threats in supply chains, to understand gaps in today's supply chain management strategies and to make recommendations to enhance security in the context of supply chain management. Previous research lacks comprehensive studies and recommendations about how supply chain managers deal with security issues in line with the business visions and strategies of their companies. The study methodology is based on an exploratory approach. Data were collected from 20 managers from international companies by means of self-administered surveys, one-to-one interviews and group interviews. Study findings point out risk management as an important tool at the disposal of managers for trading off performance and vulnerability. However, some important challenges also need to be considered, such as lack of data, insiders, IT vulnerabilities, regulatory frameworks, criminal behaviour, etc. Hence, recommendations are made for managers to improve their understanding of supply chain security.

ARTICLE HISTORY

Received 15 July 2015

Accepted 27 July 2016

KEYWORDS

Supply chain security; supply chain crime; risk management; management strategies

Introduction

Existing supply chain management strategies primarily focus on the improvement of performance of supply chain companies. Theories have largely emphasised how diverse tools, techniques and management approaches can be exploited by managers to deal with demand uncertainties and market volatility, for example, while maximising the respective profits. For instance, strategies related to contract management, quality management, risk management, network reengineering and make or buy decisions are widely acknowledged by researchers as techniques to increase performance of supply chains while minimising costs and negative environmental impacts (Christopher et al. 2011; Finch 2004; Melacini, Creazza, and Perotti 2011; Sheffi 2001; Zsidisin, Panelli, and Upton 2000). Likewise, splitting or adding production lines to quickly shift volume can help firms to stay competitive in the marketplace (Sheffi 2006; Tang 2006; Tomlin 2006; Tørhaug 2006).

Performance-driven supply chains can be vulnerable to disruptions (Jüttner, Peck, and Christopher 2003; Svensson 2000). Modern supply chain strategies have proven the necessity of implementing risk mitigation techniques to reduce vulnerability and disruption consequences of diverse risks (Jüttner, Peck, and Christopher 2003). The existing literature has already identified a plethora of relevant risks in supply chains, including environmental, cultural, financial, quality and safety risks (Manuj and Mentzer 2008). However, a risk driver that has not been properly addressed in previous

CONTACT Luca Urciuoli luca.urciuoli@gmail.com

© 2016 Informa UK Limited, trading as Taylor & Francis Group

This article was originally published with errors. This version has been corrected. Please see Corrigendum (<http://dx.doi.org/10.1080/13675567.2016.1238533>)

research is supply chain security (Williams, Lueg, and LeMay 2008). Too often, we witness cases of companies and managers that need to deal with crime incidents in their supply chains, including theft, counterfeit products and smuggling. Security has proven to have a strong impact on supply chain companies because of unexpected costs such as reduced sales revenues and damages, even to brand image. Despite this, supply chain managers lack proper understanding of supply chain security management and its major implications for supply chain management strategies; one reason for this is probably the limited research in this area as well as the lack of relevant theoretical frameworks to be used in research and educational contexts. As a consequence, the overall research question of this paper is: how can supply chain management strategies be tailored in order to improve supply chain security, that is, protection against unlawful actions against a supply chain?

The purpose of this paper is to increase the understanding of security threats in supply chains while identifying the major supply chain managerial gaps, thereby recommending approaches and precautions in existing supply chain management strategies.

Previous research lacks comprehensive studies and recommendations about how supply chain managers should deal with security issues, in line with their respective business visions and strategies. A major focus has been given to the adoption of supply chain risk management techniques, as well as to the vulnerability implications for supply chains (Jüttner, Peck, and Christopher 2003; Manuj and Mentzer 2008; Svensson 2000). Hintsä et al. (2010) provide a preliminary taxonomy of possible crime types that may be perpetrated in a supply chain; examples include theft, smuggling of prohibited items, hijacking, counterfeiting and terrorism. Williams, Lueg, and LeMay (2008) exalt the importance of organisational culture in protecting supply chains. Autry and Bobbitt (2008) developed a so-called Supply Chain Security Orientation framework highlighting the implications of good security for company financial outcomes and business continuity. However, very little has been done to highlight supply chain security management as a parallel activity to be coordinated and synchronised with the overall supply chain management functions.

This paper is composed of five sections: the introduction, followed by literature review; the methodology report, including strategies for data collections and analysis; the study results and the final section is on conclusions and managerial implications.

Literature review

Security risks are an emerging topic in the context of supply chain risk management, calling for heightened attention from supply chain and security managers (Manuj and Mentzer 2008; Sheffi 2001; Urciuoli 2010). The fear of a major disruption in supply chains has increased since the 9/11, 2001 terrorist attacks. As a consequence, supply chain security is now a fundamental requirement in an organisation and should be coordinated with supply chain management (Hameri and Hintsä 2009; Sheffi 2001; Urciuoli 2010).

Supply chains could be disrupted by security threats at any given time, including sea piracy, sabotage, vandalism and riots (Urciuoli et al. 2014). These threats could be voluntary actions perpetrated by external entities or simply actions performed by employees, the insiders in supply chain companies. For instance, insiders could provide significant support to external criminals by simply revealing weak points, providing authentication passwords, manipulating documents, etc. Likewise, desperate attempts to increase a company's revenues could end up in illicit actions, for example, breaching various regulatory frameworks (Hintsä et al. 2010; Urciuoli, Hintsä, and Ahokas 2013). Männistö, Hintsä, and Urciuoli (2014) provided a comprehensive taxonomy of possible crime types that may be perpetrated in a supply chain. In particular, it can be deduced that supply chain security should be extended to protections beyond the traditional cargo theft attacks and should also include more complex trading and financial illicit actions, including smuggling of prohibited or restricted items such as drugs and weapons, counterfeiting, money laundering, tax evasion, etc.

To highlight the supply chain managerial functions that are considered to be close to supply chain security issues, the literature review is classified in three categories: supply chain risk management,

Figure 1. Theoretical framework: pillars for supply chain security management.

information management and management of physical assets (Figure 1). These three categories can be seen as essential for firms willing to improve management of security risks. Since security threats form one of the many categories of risks that can distress a supply chain, supply chain risk management assumes a primary role in identifying, evaluating and mitigating security threats. This risk management function needs to be strictly linked to the management of the physical assets. First of all, products manufactured and moved in the supply chains are key targets of criminals. Secondly, the efficient management of assets could be altered by the introduction of security measures, leading to additional costs and operational delays. Finally, experts are pointing to the importance of cybersecurity in supply chains (Fossi et al. 2011). Also, in this case a paradox can be seen, that is, the same information and communication technologies that have contributed tremendously to the productivity and competitiveness of supply chain companies can, at the same time, increase vulnerability and exposure to security threats.

Supply chain risk management

Historical events have demonstrated that managers are often not fully aware of their supply chains' exposure to risks – an unconsciousness that may lead even to bankruptcy or other serious consequences for firms (Norrman and Jansson 2004). Reasons for this behaviour can be found across the past literature and can be related, for example, to a lack of visibility or control over the entire supply chain. Global supply chains face several varieties of risks, which makes it difficult for logistics or supply chain managers to dynamically tailor their strategies to minimise exposure to risks (Waters 2007). Secondly, managers typically have short – or medium – term targets to follow, with a major focus on the adoption of performance-driven strategies like globalisation, outsourcing, just-in-time or lean principles. However, such approaches may increase vulnerability and compromise the capability to respond to sudden or unexpected events (Aqlan and Lam 2015; Christopher and Peck 2004; Jüttner, Peck, and Christopher 2003). Hence, supply chain risk management is suggested as a systematic approach to identify and address diverse types of risks relevant for supply chains, including natural catastrophes, equipment failure and demand risks (Asbjørnslett 2009; Finch 2004; Franck 2007; Manuj and Mentzer 2008; Zsidisin, Panelli, and Upton 2000). In a risk management approach, particular attention should be paid to the type of response to risks. A manager can choose to reduce

the probability of the risk event occurring or to reduce the potential consequences, even to transfer the risk to another actor (Waters 2007). In any case, different responses may have different impacts, and managers need to choose among sets of disruption strategies by carefully evaluating their costs and benefits (Colicchia, Dallari, and Melacini 2011; Holland and Geoffrey Lockett 1997; Khan, Christopher, and Creazza 2012; Melacini, Creazza, and Perotti 2011; Tang 2006). Some researchers confirm that in certain occasions, disruptions cannot be avoided. Therefore, they suggest that supply chain management should concentrate on the enhancement of resilience capabilities, that is, to withstand disruptions while trying to avoid them (Christopher and Peck 2004; Sheffi 2001, 2006). Previous research puts major emphasis on the incorporation of resilience in the design of the supply chain by establishing parallel paths through multiple sourcing, evaluating several transport channels, shortening the supply chains (e.g. using domestic suppliers) or using specific contracts with suppliers in order to expand transport or manufacturing capacity in case of emergency (Norrman and Jansson 2004; Waters 2007).

Information management

Information management in supply chains is of vital importance to ensure timely processes and to cut costs related to overstock, unsatisfied customer demand and so forth. The latest developments of information technology applied to production, transport and consumption of goods has introduced mechanical automation, reduced workforce and thereby provided significant cost-savings to supply chains. Large enterprises that are willing to keep a dominant position in the supply chain as well as in distribution markets have to promote the application of advanced information systems (Dang, Yan, and Lai 2015).

The adoption of advanced information systems in supply chains means sharing and analysing large amounts of data among multiple actors. Both shippers and logistics companies share extended amounts of data, covering different needs of supply chain companies in order to make operations more efficient and flexible, including purchase orders, shipping instructions, bills of materials, warehouse packing lists and so forth (Dang, Yan, and Lai 2015; Liu 2014). This process, however, brings many challenges, especially in terms of connecting different legacy systems and ensuring interoperability. In addition, data to be extracted from multiple sources must be of good quality. In practice, it is often necessary to deal with incomplete data, and technicians have to ensure it is correctly cleaned and integrated and stored in a common database (Li, Guo, and Li 2014).

Finally, once the data quality and sharing has been finalised, analytical techniques can be used to support benefit delivery for businesses. Examples of information sharing for enhancing the competitiveness of supply chains are unlimited. To name a few examples: data can provide insights into managerial strategies; information can be shared to improve continuous replenishment and to allow customers to pull goods; strategic marketing and sales information can be shared, as well as inventory positions and cargo documents handled by freight forwarders and trucking companies can be exchanged. Yet another case is the usage of information sharing in supply chains as an effective approach to deal with supply chain disruptions, for example, those caused by financial, strategic, operational and hazard vulnerabilities (Blos et al. 2009). Some researchers suggest that proper information management may also improve the flexibility of supply chains (Glenn Richey, Skipper, and Hanna 2009). Lee and Özer (2007) find that by timely downstream sharing of information, upstream disruptions may be promptly avoided or their negative consequences minimised. Tomlin (2006) suggests that advance information could be used to deal with certain risks, for instance, labour disputes: if a firm has advance information that a strike is imminent, then mitigation inventory may be built in advance.

Physical assets management

Supply chains can be seen as sets of virtual organisations owning diverse types of assets and managing resources. A central part of the assets are the goods (raw materials, semi-finished products,

finished products, etc.) or cargo that are moved from the upstream to the downstream part of the supply chain and finally to the end customers (Bowersox, Closs, and Cooper 2002). In addition to the goods, other relevant assets and resources include machinery used and people working in supply chain companies (Gunasekaran 1999). The optimal management of these assets is fundamental to ensure that the key activities of supply chains – such as transportation, storage, goods handling and storing, packaging and labelling – happen in a cost-efficient manner (Croxtton and Zinn 2005; Kye, Lee, and Lee 2013). Simulation and mathematical programming have been broadly applied to optimise these activities. Wang, Wang, and Meng (2014) developed a mathematical programming model focusing on the optimisation of the ship route scheduling and interrelated cargo allocation scheme. Yao et al. (2015) propose a time-dependent vehicle routing problem with time windows to optimise in order travelled distance, number of vehicles and also fuel consumption. Hence, the model developed aims to reduce logistics enterprises' operation costs as well as alleviate environmental problems (Yao et al. 2015).

Finally, physical assets are directly exposed to security risks, particularly because cargo is the main target of criminals, especially a high value cargo. Next, transport assets and machinery used in the supply chain can also be stolen or used to facilitate criminal activities. For instance, drugs or weapons can be hidden in containers, trucks frames or packaging materials. Similarly, if criminals are not able to open a trailer or container to steal its contents, they might prefer to steal the whole conveyance (Urciuoli 2010). Personnel forms also a fundamental part of a supply chain. Without well-trained and motivated personnel, many activities devoted to assets optimisation could not be performed efficiently. Some authors suggest that up to 50% of costs along the entire supply chain are labour costs (Sillekens, Koberstein, and Suhl 2011). Optimum allocation of labour capacity along the supply chain is essential to ensure efficiency and flexibility (Bauer et al. 2007). Despite this, personnel can be considered to be a weak link in a supply chain (Glenn Richey and Reade 2009). Employees could act as insiders and support criminals in perpetrating their actions, or they could perpetrate a crime on their own, as they may have easy access to facilities or cargo (Urciuoli 2010).

Methodology

This study is exploratory and the methodology consists of a combination of different approaches. First of all, a literature review was performed. The screening of the literature helped the authors in pinpointing the theoretical frameworks that were used in the data collection and analysis (Stock 1995). Emerald, Elsevier and Springer were the scientific databases used for the searches, while the main keywords used were the following:

- Supply chain management
- Supply chain AND strategies
- Supply chain AND strategies AND security
- Supply chain AND security.

The keywords were directly derived from the research question. This study aims at understanding how supply chain management strategies need to be adapted to security management. Hence, searches focused on gathering existing work on these topics and, in particular, on the combination of supply chain management strategies and security. In addition, the results from the searches were screened in a systematic manner to effectively select all articles that were believed to be relevant (Jes-son, Matheson, and Lacey 2011; Tranfield, Denyer, and Smart 2003). As a result, 32 different journals were included in the literature review (Table A1 in Appendix), of which 10 had a quantitative nature and 22 had a qualitative nature.

Thereafter, data were collected by means of the following methods:

- self-administered surveys with open-ended questions,

- qualitative one-to-one interviews, and
- group interviews.

The above approaches were meant to elicit participants' perceptions of and experiences with supply chain crimes. A research protocol was used to ensure that the data collected with different methods could be triangulated (Patton 1999).

The whole study sample consists of 20 managers representing different international companies across a variety of industry sectors (Table 1). Respondents' positions include senior management, CEO and Vice President of operations. To ensure the possibility of collecting a larger variety of supply chain crimes, global manufacturing companies and Logistics Service Providers (LSP) with sales revenues over €500 million were invited to the study. In total, nine participants returned the survey form, six participated into the one-to-one interviews, and five joined the group interview sessions. Data collection took place between September 2010 and February 2011 as part of a European supply chain security roadmap project FP7-LOGSEC.

Self-administered survey. To explore crime problems in supply chains, a self-administered survey instrument with open-ended questions was used (see Appendix). Open-ended questions were used to allow respondents to elaborate on their opinions, views and experiences, reducing the subjectivity of interpretations to the minimum (Foddy 1994). The group of firms that was asked to fill in the surveys was approached through three European industry organisations: European Shipper's Council (ESC), European Association for Forwarding, Transport, Logistics and Customs Services (CLECAT) and Transported Asset Protection Association in Europe, Middle-East and Africa (TAPA EMEA).

Group interview. Two group interview sessions were arranged to explore further crime problems in supply chains. The simultaneous interviewing of multiple participants in a social context allows interviewees to reflect on their own perceptions vis-à-vis the views of others. Group interviews stimulate confrontation and spontaneous elaboration of concepts among participants (Frey and Fontana 1991; Morgan 1997). The first session took place in October 2010 and the second in November 2010. The sessions lasted around three hours and involved two and three managers, respectively. The sessions followed a preconceived protocol in which an experienced moderator asked participants to describe their crime concerns associated with various stages in their supply chains (Frey and Fontana 1991). To keep researcher bias to minimum, two assisting co-researchers documented the sessions by taking written notes.

Content analysis. Two researchers reviewed the textual survey and interview data row-by-row, aiming to identify general crime problems as well as gaps and challenges. The main aim of this session was to 'make replicable and valid inferences from texts [...] to the context of their use' (Krippendorff 2004). In particular, the analysis aimed to deduce a comprehensive list of crime problems in

Table 1. Type of companies and applied methods of data collection.

Industry sector	Total responses	Participants by method		
		Self-administered surveys	One-to-one interviews	Group interviews
Aerospace	1	1	0	0
Automobile	1	1	0	0
Beverage	1	0	1	0
Chemical	1	0	0	1
Communication/electronic	7	3	2	2
Food wholesale/retail	1	0	1	0
Logistics service provider	2	2	0	0
Machinery	1	0	1	0
Pharmaceutical	4	1	1	2
Textile	1	1	0	0
<i>Total (frequency)</i>	20	9	6	5
<i>Of total responses (%)</i>		45	30	25

supply chains, and finally gaps and challenges experienced by managers. The final results surfaced when the authors reached an agreement on appropriate categories and related gaps to be addressed.

Quality of research design

Lincoln and Guba (1989) proposed that the traditional quality criteria for positivistic/quantitative research have their parallel constructs in the realm of qualitative research. Internal validity, external validity, reliability and objectivity correspond to credibility, transferability, dependability and confirmability, respectively. Trustworthiness of research is a function of these four elements, as also confirmed by their widespread use in qualitative logistics research (Erlandson et al. 1993; Halldorsson and Aastrup 2003). In this study, credibility was addressed by triangulating data from different sources (surveys, one-to-one and group interviews). In addition, follow-up communications with respondents was performed as needed. To address transferability and dependability, respondents were selected from different industrial sectors, the main research context was thoroughly described in the study and a formal research protocol was developed. Finally, to guarantee confirmability, all evidence was documented in a database, content analysis techniques were used, all authors reviewed and agreed on the findings and a skilled moderator was used in the group interviews.

Results

The framework in Figure 2 summarises the results of this study. Supply chain security is analysed in terms of present and future threats. The identified gaps are clustered under the three main pillars, representing strategies to optimise performance and reduce vulnerability of supply chains:

- Supply chain risk management
 - (a) lack of incident data and
 - (b) lack of knowledge about crime trends.
- Information management
 - (a) cybersecurity,
 - (b) document forgery, and
 - (c) partners' trust and verification.
- Physical assets management

Figure 2. Summary of results clustered in the theoretical framework.

- (a) counterfeit products,
- (b) cargo in transit,
- (c) reverse flows, and
- (d) human resources.

Present and future supply chain security threats

Figure 3 illustrates the major crimes that respondents considered to pose significant threats in supply chains at the present. The threats are shown in the frequency order of the responses.

Respondents indicated theft in transit (23%) as the most relevant threat. Hence, cargo shipped through freight operators' networks is fairly more exposed to crime and therefore more vulnerable. This is true especially on the road, since trucks commonly need to stop in exposed parking areas or other isolated spots on the roadside (Freightwatch 2016). Other relevant threats follow closely: data theft/cybercrime (11%), bogus companies (10%), insider fraud (10%), smuggling (9%) and counterfeiting (9%). It is interesting to note that data theft/cybercrime is a present concern for companies. This threat relates to the use of the Internet and computers or other electronic devices to attack a supply chain or to facilitate a crime within a supply chain (Urciuoli, Mannisto et al. 2013). Finally, other crime threats that were less frequently indicated by the respondents are illegal immigration (5%, immigrants hiding in containers or trailers), sabotage (5%), product diversion (5%, diverting products to countries where they can be sold at higher prices and/or taxes can be avoided), product specification fraud (4%, e.g. using lower cost, potentially harmful ingredients) and environmental crime (2%, illegal acts harming the environment, e.g. illegal dumping or waste disposal) (Figure 3).

The next figure shows the diversification of the threats across the industry sectors of the respondents (Figure 4). Two crimes seem to be common to all industry sectors: theft in transit and data theft/cybercrime. In the former case, aerospace manufacturing was the only industry sector that did not indicate theft in transit as a present problem. As experts point out, cargo theft is driven by demand from the black market (Freightwatch 2016). Logically, components destined to the aerospace industry are difficult to resell either directly to final consumers or to distributors/factories.

Figure 3. Present crime threats.

Cybercrime is a present concern of chemical, electronics, pharmaceutical and aerospace companies and LSP. Hence, it can be argued that cybercrime is a concern of all supply chain stakeholders, regardless of the type of business or product.

Among the industry sectors, electronics companies seem to face the highest variety of crime attacks (all *modus operandi* except shoplifting), followed by machinery and food wholesale. As stated before, these products are largely demanded by final consumers willing to buy from the black market. Likewise, machinery and food can be easily resold to small retailers (especially online) or workshops. The company in the machinery sector had broader concerns since it deals with several business segments, including oil and gas, where security problems may appear in a wide variety of *modus operandi*. On the contrary, textile manufacturing industries indicate only theft in transit as the main crime type. Similarly, alcoholic beverage manufacturing and distribution has only two major concerns: theft in transit and bogus companies (Figure 4). Alcoholic beverages are considered high value goods that can be stolen from supply chains and easily traded in the black market. Just like with cigarettes, excise tax liabilities may kick in even when products are stolen, thus remarkably increasing the total cost of cargo theft.

As shown in Figure 5, many present threats are still considered relevant in the future, including theft in transit (15.1%), insider fraud (9.1%), counterfeiting (9.1%), etc. This indicates that most likely the industry does not expect to have effective countermeasures to these problems. The only exception is the threat of bogus companies, which for the future is expected to be much lower (down to 3% from 10%). Finally, many respondents seem to agree that data theft/cybercrime will grow to be even more relevant as a threat in the future (36.3%). This is in accordance with existing industrial reports pointing to cybercrime as a major concern. Symantec has alerted that malicious cyberattacks increased by 81% in 2010; 50% of these attacks were targeting the business sectors (Fossi et al. 2011). Overall, experts believe that the number of these types of attacks will continue to increase in the future (Cisco 2011). The most worrying fact is that data intrusion, theft or manipulation is the catalyst for several crimes in the diagram. Hence, the expected increase in cybercrime will ultimately influence the remaining security threats shown in Figure 5.

By examining the future threats across the industry sectors of the respondents, one can observe that cybercrime is commonly perceived as a major risk by respondents from several sectors, including food wholesale, chemical, electronics, textile and LSP. On the other hand, other crimes seem to be highly diversified in different sectors: bogus companies will continue to be a problem for LSP,

Figure 4. Present threats across industry sectors.

Figure 5. Future supply chain security threats.

corporate identity theft for the aerospace industry, shoplifting for food wholesale/retail and finally corruption for the electronics industry (Figure 6).

Supply chain risk management gaps

Supply chain risk management is a tool at the disposal of managers to ensure that security risks, among all other supply chain risks, are continuously addressed. The most important gaps related to the implementation of risk management techniques in this study include the lack of data about threats and the necessity to continuously adapt to changing crime trends. Existing risk management techniques are based on the fact that managers have the ability to measure and assess risks in terms of likelihood of happening (Asbjørnslett 2009), but if data are unavailable, this procedure becomes obsolete.

Lack of incident data

Respondents from manufacturers of electronics products, pharmaceuticals and LSP highlight the relevance of crime incident data, statistics and trend analysis in order to enable risk analysis. The

Figure 6. Future threats per industry sector.

examination of past trends may raise awareness of new *modus operandi* among criminals. In addition, many operators lack access to a robust and comprehensive European database where information about cargo crime *modus operandi* and trend statistics could be used to enhance awareness and thereafter identify proper countermeasures.

...Monitoring supply chain security incidents across all industries is therefore of great value (thereby generating isomorphic learning). (Pharmaceuticals)

... a shared database for European operators is needed ... as cross-border crime cannot be reported today. (Electronics)

Crime trends analysis

In addition, respondents from pharmaceuticals and alcoholic beverages sectors suggest that risk management techniques should be able to consider the dynamicity of crime, that is, criminal actors adapt their behaviour to match (or overcome) the security measures that are introduced in supply chains. Hence, managers need to be proactive and continuously set up strategic and operational plans for quick counter-actions.

...There is the obvious gap between proactive criminal initiatives and the Company's reactive response. Ideally, the security posture – processes, procedures, and over-arching protective security – serves to deter criminal elements, but trends may develop or be identified requiring rapid counter-action. (Pharmaceuticals)

The most inventive minds are in the criminal world. We can expect new methods of committing crimes from these people and we will need to learn from others' misfortunes.... (Alcoholic beverages)

Information management gaps

Major gaps related to the management of information exchange in supply chains have been grouped within the following topics: cybersecurity, document forgery and partners' trust and verification.

Cybersecurity

Cybersecurity is one of the major growing problems for supply chains. The majority of industry sectors considered this threat to be a major concern for the future. Sensitive data on product design, recipes, manufacturing techniques, cargo routes, etc. could be stolen and used illicitly by other organisations to perpetrate crime. This was a clear message from the study participants:

...We rarely have any criminal theft or loss. The biggest concerns from our perspective are cybersecurity and sabotage (e.g. embedding of Trojan horses into avionics or IT systems) within the supply chain. (LSP)

...Cybersecurity appears to be becoming a huge priority for government and industry. Overall IT security against penetrations continues to be a concern. (Food wholesale/retail)

Hence, it appears that supply chain actors are increasingly realising the vulnerability of their IT systems and consequently the importance of protecting them. This specific vulnerability is seen as a growing support activity to facilitate cargo crime.

...It is clear throughout the transport/logistics industry that specific cargo details and trucking/aircraft data are recorded digitally on proprietary and public networks. Every high value transport load within Europe will therefore be developed, organized, and coordinated on data processing systems. Breaching these systems using either internal or external resources allows criminals to identify which loads/trucks to attack. (Alcoholic beverages)

Hence, IT systems that are normally meant to speed up supply chains, remove complexity, reduce personnel costs and increase performance are foreseen to become the most vulnerable layer of supply chains, with costly negative consequences if intrusions cause disruptions or similar problems. Lack of protection of IT systems may have diverse consequences and may even lead to the shutdown of

operations in facilities where automated systems are in use. As a general observation, automation has reduced the need for human work and intelligence in logistics operations, also allowing the use of less skilled employees. As a downside, when problems occur in the IT infrastructure, there is typically insufficient manpower and knowledge to execute operations manually.

One security manager pointed out that it may be difficult to determine where the vulnerable points are in complex IT systems and infrastructures. This complicates the work of managers in determining where and how to counteract security problems.

We just need an infrastructure, both physical and information infrastructure. Vulnerability means condition, where we have no alternatives – we cannot move forwards or backwards, we cannot change transport mode, we can just wait. We just don't know in advance, where these vulnerable points and vulnerable infrastructure are. (Pharmaceuticals)

Another issue identified by respondents is that the protection of the information and communication layer may become cumbersome due to the increasingly common approach of outsourcing information services to third parties. This implies a lack of direct control of the security level used by the contracted partners but also a lower visibility of the physical security of the IT infrastructure itself (*who is guarding the guards?*): detection of component substitution, different access levels, resistance against mechanical, electrical or magnetic tampering and sabotage, reliability tests under defined environmental conditions, duplicated transmission paths and firewalls. Overall, low security in a facility means that intruders can enter the facility and manipulate the IT infrastructure and/or steal important data. As one respondent stated:

Information security is an enormous challenge. We cannot confine a problem inside of one box located inside of one facility. Many of our information services are outsourced. Vulnerable switches, routers and components are located in unknown facilities, often behind poor physical security. Maybe, it is not easy to penetrate into our information systems, but it is certainly easy to remove components, put them in a pocket and walk away. This could stop our payments systems and shut down our stores. The crime motivation could be a theft, because we use reliable and valuable components in our information systems, which cannot be bought in every corner. (Textile)

Another problem indicated by one of the respondents is that information security experts commonly experience difficulties in communicating their issues in a manner that top management understands. This lack of communication and understanding determine ambiguity about how IT systems should be correctly protected.

Document forgery

Another well-known technique to take advantage of a supply chain is to produce and exchange fake documentation, that is, document forgery. For instance, falsification of shipping documents was indicated as the most important issue related to fraud. This information is normally transmitted by fax or other information exchange technologies. It may even happen that shippers tweak the weights of their products just to claim more money from their customers.

Fraudulent product certifications – on quality, performance parameters, etc. – are not new in supply chains and, in particular, in the manufacturing sector. The buyer's challenge is to ensure that the products match the description in the documentation. Product quality verification may be performed, but this is expensive and can only be performed with a small sample of products.

...an Asian producer falsified the product certificates, by stating that the working life [of the product] was 10.000 hours, when in fact, in reality it was only 5.000 hours. (Electronics)

Some companies have found semi-systematic ways of detecting forgeries. However, such approaches typically require continuous supervision, planning and the commitment of top managers.

Unfortunately, operators are still far from having robust solutions that ensure the authenticity and integrity of documentation. This is particularly true where the inspection of documents is

being performed by relatively untrained cargo handling staff. Mistakes are easy to make, corrupt personnel can be involved and/or insider crime may be occurring.

Partners' trust and verification

False information can also be advertised to generate trust across supply chain companies. This kind of information can relate to company websites; email addresses; register-of-commerce extracts; operating licences; driver identification; business licences; truck licence plates; trade documents and data in supply chain systems; product test certificates and product labels or even police personnel. For instance, in some countries, illicit companies can steal the identity, that is, logo and name, of legitimate and well-known companies to attract customers and thereby perpetrate other illicit operations. These companies are able to produce fake information as stamps, orders, invoices, etc. As one respondent stated:

... bogus [road freight] carriers might operate normally and legally for a while without drawing suspicion to themselves, in order to gain the trust of customers before stealing valuable shipments from them. (Alcoholic beverages)

Even a potential downstream customer in the supply chain, for example, a distributor, an agent or a retailer, could turn out to be a bogus company. This customer could make an order and vanish without paying, as soon as a consignment is delivered.

Another gap highlighted is that supply chain businesses are often regulated by trust, and no recommendations or regulatory frameworks are at the disposal of managers to verify a trusted partner. For instance, respondents claimed that regulations do not always support the verification of licences. Likewise, the verification of trusted partners in a supply chain, which is often composed of multiple tiers of subcontractors, is often a challenging task.

Physical assets management gaps

Major consequences and implications of security threats concern the physical assets of supply chains. Main gaps that were highlighted by respondents include: counterfeit products, cargo in transit, reverse flows and human resources.

The production and distribution of counterfeit products is a major problem today for intellectual property owners, customers and supply chain systems as a whole. Counterfeit products can lead to losses in company sales revenue and government tax revenue, damage brand reputation, harm the health and safety of consumers and so forth. For example, the consequences can be devastating with pharmaceutical counterfeits due to total or partial lack of the key substance(s), improper handling of the cold chain, etc. Across most commodities, differentiating between original and counterfeit products, for example, during customs controls, can be a very difficult, time-consuming task. Fraudulent test certificates and trade documents can be exploited to facilitate this illicit activity.

Cargo in transit

When the study participants were asked where the supply chain is most vulnerable, the most common answer was *in-transit*. In particular, this specific gap was pointed out by several industry sectors, including LSP, pharmaceuticals, electronics, beverages, etc.

...It's trucks I would hit if I was a criminal – warehouses are harder targets. (Pharmaceuticals)

Accessing vehicles and trailers is not always done for the purpose of theft; sometimes it is also done for the purpose of illegal immigration and people smuggling across borders. This carries its own security risks and problems for cargo owners.

From a managerial perspective, the most relevant gaps and challenges to overcome include the lack of protection of vehicles and cargo moving on roads and the lack of protection in parking places. Poor protection of the vehicle and the cargo itself was identified as a main area of weakness. In some

cases, there is a complete lack of security solutions; in other cases, implemented measures are too simple to deceive.

'Cargo at rest is cargo at risk' goes an industry proverb. Respondents indicated that the poor protection of parked vehicles and cargo is a common cause for vulnerability. The challenge of managers is to locate secured parking places and also to afford the prices to enter these places.

...There is a lack of fully secured parking places in Poland and many member states in the EU. (LSP)

Poor training of operators can also be a major concern, exposing the supply chain to security risks. According to many respondents, frauds and breaches in security commonly happen during logistics handovers. In other cases, lack of inspection of cargo during transport may imply that theft or manipulation cannot be detected until the cargo arrives at its final destination. At that point, it is practically impossible to determine who was liable for the damage.

Reverse flows

Supply chain security does not end at the retailers or the final consumers; it actually follows the entire supply chain loop, including reverse flows for waste and disposal. Reverse flows can be a surprisingly vulnerable part of a supply chain, especially for the pharmaceutical and electronic industry sectors. Pharmaceutical companies have concerns that waste medicines (expiry date passed) flows are deviated, while later re-entering the markets illegally. Similarly, electronic companies are aware of the possibility that their waste materials could be deviated and illegally disposed of in a manner to harm the environment and human health or that specific components could be used in counterfeit products.

One company stated that it was concerned about products that were meant to be destroyed when they are past their due date or when some flaw has been noted, leading to recall of a production lot:

...the destroying company claims that they have destroyed the products but actually they put the products back to market. (Pharmaceuticals)

A similar concern was raised by another manufacturer:

...waste products and returns of products are prone to all kinds of diversions, which may violate import/export laws or cause harm to production. (Electronics)

Another worry related to environmental crime:

...due to the WEEE directive (waste electrical and electronic equipment), the rules and requirements are very strict: therefore, any related crime would most likely be undertaken by 'rogue traders'. It also raises the grey area as to when a product legally becomes scrap: sometimes old or redundant goods are passed on to anyone who might make use of them: this therefore means it retains a value and cannot be construed as scrap. Some companies get caught out by this. (Electronics)

Finally, the weaknesses of waste recycling flows, and the potential for creating valuable waste that can then be stolen and sold again, was raised:

...[part of the process is to] put holes into the lamps – which results in a lot of metal waste, and recycling. Containers used for collecting the waste have to be moved away from where people can access them and possibly hide things within them and smuggle stolen items out. (Electronics)

Human resources

Supply chain personnel is widely recognised as the backbone of any type of supply chain. This includes, for instance, factory and warehouse workers, supply chain planners and administrators, truck and crane drivers, aeroplane pilots and ship captains. However, hiring the *right people* and avoiding bringing in the *bad apples* is a difficult task, as individual level behaviours, needs and motivations are difficult to recognise, and they have a tendency to change over time. This problem was particularly highlighted by the electronics and chemical industries. An employee getting into

financial trouble and borrowing money from fraudulent lenders can be enticed to pass inside information to a criminal organisation, either to pay back her debts or to avoid injury being inflicted on herself and/or her family when she is unable to repay her debt. Another employee could be radicalised, say over a multi-year period, and become part of a terrorist cell. Such things may happen and are very difficult to predict in advance.

Today, supply chain companies exploit the option of employees' background checks to the extent allowed by the national regulations. However, these methods may have major flaws that – if not properly considered – could be critical in ensuring the protection of supply chains from crimes committed by insiders. First of all, it goes without saying that background checks may give a false sense of security, in particular if employees have not been caught yet or if they have become radicalised.

...a clean record shown by background checks can only ever prove that the people involved in crime haven't yet been caught! (Electronics)

Secondly, it often happens that companies do not really have the time or the resources necessary to hire personnel, and therefore it is a common practice to use third party employment agencies. Unfortunately, as it was highlighted during the study, some of the agencies that do the checks seem to be unregulated.

Finally, among the top concerns of respondents regarding the difficulties in implementing and maintaining security programmes were personnel attitudes and solidarity in the working community. As a consequence, for example, minor crimes detected may not be communicated to the middle or top management.

... There is a production team solidarity and spirit – we are used to dealing by ourselves with problems and we say nothing to the hierarchy, which doesn't understand our problems and working conditions We know each other in the team and even if we don't like somebody, we will never denounce one of our colleagues, except in the case of a blood crime. (Chemicals)

Discussion and conclusion

Existing theoretical frameworks in the supply chain management discipline emphasise the importance of improving performance through development of tailored strategies, adoption of risk management principles and optimal management of information systems and physical assets. In this context, this paper unveils important security challenges that are being encountered by supply chain managers. In particular, these challenges may undermine the work done to improve performance, while bringing unexpected losses and shrinking revenues in a significant manner.

The analysis of previous literature confirms the importance of considering security risks in supply chain management (Hameri and Hintsa 2009; Sheffi 2001). Security threats can be interpreted as unlawful actions against the supply chain; hence, not only cargo theft attacks but even more complex trading and financial illicit actions aiming to evade tax payments, perform money laundering or attempt to smuggle prohibited items into a country (Hintsa 2011; Männistö, Hintsa, and Urciuoli 2014; Sheffi 2001). Data collected in relation to potential security threats to supply chains show that actually cargo theft represents the majority of security events taking place in the supply chain. However, the respondents could provide a comprehensive list of additional threats that are classified as security threats, including cybercrime, counterfeiting, product deviations, smuggling, etc. Previous research has pointed at these threats in separate studies (Closs and McGarrell 2004; Grainger 2007; Sheffi 2001; Urciuoli, Mannisto et al. 2013) but does not provide a unified view based on empirical data. In particular, the prediction of future supply chain security threats shows a clear domination of cybersecurity. Some studies had warned about the risks of cybercrime in supply chains (Urciuoli, Mannisto et al. 2013; Warren and Hutchinson 2000), but too little evidence has been provided.

One of the main pillars for enabling effective and efficient supply chains is the seamless exchange of information from suppliers all the way to final customers (Blos et al. 2009; Dang, Yan, and Lai 2015; Glenn Richey, Skipper, and Hanna 2009; Tomlin 2006). Information elements typically include

several documents proving regulatory compliance or cargo authenticity. However, there is an overall increased attention towards the security of information systems, raising the opportunity to highlight these issues within the supply chain and logistics scientific communities. While these systems may improve supply chain efficiency, it has also been proven that security can be affected (Urciuoli, Manisto et al. 2013). The data collected in this study indicate that major security breaches can rise from the exchange of information. Fake or falsified documentation could be used to state quality, authenticity, integrity or other relevant cargo properties. Falsifying documents can also be used for registering a fake or bogus company – a method used mainly by fake freight forwarders or LSP. These companies may use the names of well-established and known companies, operate for some time in order to develop trust and then suddenly steal all cargo and disappear. Finally, electronic information exchanged in the supply chain could be accessed, stolen and manipulated for the purpose of committing a crime. The respondents highlight cybercrime (including data theft and manipulation) as the main future threat to be taken into account in supply chain management. Cybercrime could be used to attack competitors, to acquire knowledge about competitors' strategies, to provoke disruptions, to target cargo in the supply chain and so forth.

Physical assets including cargo, transport vehicles, transport and storage infrastructure, and the human resources working in the supply chain, naturally constitute the backbone of a supply chain. Research has developed several techniques to optimise assets usage, reducing costs while improving performance (Wang, Wang, and Meng 2014; Yao et al. 2015). However, the same assets can be attacked by criminals to steal or perpetrate other illicit actions, thus calling for proper monitoring and protection. Human resources can be the weakest link in supply chains. Workers could willingly act as insiders or be forced to collaborate with criminal groups (Glenn Richey and Reade 2009). Techniques used to corrupt the supply chain are multiple and can be difficult to detect with existing methods, especially if employees are radicalised. In addition, the study results highlight the high risk posed to cargo in transit, especially when transported on the road.

Previous research has indicated the importance of trading off risks and performance in order to preserve the vulnerability of supply chains (Christopher and Peck 2004; Jüttner, Peck, and Christopher 2003; Tang 2006; Tomlin 2006). Supply chain managers need to develop capabilities to optimise performance of their supply chains without affecting vulnerability (Christopher and Peck 2004; Peck 2006). The supply chain risk management function is a known systematic approach to accomplish this task (Asbjørnslett 2009; Manuj and Mentzer 2008; Sheffi 2001). However, previous studies suggest that it is difficult for logistics or supply chain managers to dynamically tailor their strategies to minimise exposure to risks (Waters 2007). As this study reveals, practitioners need to be aware that securing supply chains implies challenges, and therefore a deeper understanding of several topics: crime, regulations, human behaviour, security technologies, information technology, data collation and statistics, IT systems interoperability, personnel training, regulatory frameworks and supply chain visibility, including reverse flows. The theoretical framework proposed in this paper aims to set up the basis to let the supply chain security emerge as an independent research area. The same framework may be exploited by supply chain managers to understand the importance of coordinated actions between three main areas:

- *Supply chain risk management.* The data analysed in this study reveals the importance of working further with security awareness and risk management; increasing knowledge of crime trends and awareness of security measures; and building a culture and approach that more proactively and successfully responds to security risks and threats. In particular, risk managers should be aware that security measures may become obsolete as soon as criminals change their modus operandi.
- *Information management.* IT systems and other information exchanged in supply chains are meant to improve performance while inadvertently introducing new, unwanted vulnerabilities. Supply chain managers should be aware of this as well as confident about the usage systems and technologies for authentication and certification of people, companies, documents and

data in the supply chain. With improved assurances that the people and information in the supply chain are trustworthy, deception may be filtered out and fraudsters deterred.

- *Physical assets management.* Protecting cargo, vehicles and drivers during transportation and logistics handovers as well as during breaks/stops/parking is of outmost importance. In addition, supply chain managers should be able to assess and procure services from secure companies. Likewise, they should have knowledge of existing security solutions and the pros and cons, as well as limitations and constraints, of their implementation.

The main limitation of this paper is that it is based on an exploratory investigation and on a convenient sample of companies and respondents. The exploratory study was necessary because of the lack of established theoretical frameworks. As a result, the generalisability of the results could be compromised. Hence, future research could be focused on validating the developed framework with case studies and/or surveys.

Finally, future research should be driven with established methods to examine in more detail whether the gaps identified in this paper are valid for a broader group of supply chain companies and managers. This particular task has been currently initiated within a large scale supply chain security research, development and demonstration project, the European Union funded FP7 project CORE. This investigation makes use of qualitative methodologies that are normally preferred in exploratory studies in underexplored research contexts. Hence, it is challenging to reach a holistic understanding of the phenomenon investigated and our recommendation is to build upon this study to perform additional quantitative studies. Likewise, economic models aiming to identify trade-offs of security costs versus operational benefits could be investigated more deeply.

Acknowledgements

This publication reflects only the authors' views and the European Union is not liable for any use that may be made of the information contained therein.

Disclosure statement

No potential conflict of interest was reported by the authors.

Funding

The research leading to these results has received funding from the European Union Seventh Framework Programme (FP7/2007–2013) under the grant agreement no. 241676 (LOGSEC project, www.logsec.eu).

ORCID

Luca Urciuoli <http://orcid.org/0000-0002-9417-9421>

References

- Aqlan, Faisal, and Sarah S. Lam. 2015. "Supply Chain Risk Modelling and Mitigation." *International Journal of Production Research* 53 (18): 1–17. Advance online publication.
- Asbjørnslett, Bjørn Egil. 2009. "Assessing the Vulnerability of Supply Chains." In *Supply Chain Risk*, edited by George A. Zsidisin, Bob Ritchie, 15–33. New York: Springer.
- Autry, C. W., and L. M. Bobbitt. 2008. "Supply Chain Security Orientation: Conceptual Development and a Proposed Framework." *The International Journal of Logistics Management* 19 (1): 42–64.
- Bauer, Frank, Hermann Groß, Rafael Muñoz de Bustillo y Llorente, Enrique Fernández Macías, and Georg Siegl. 2007. "Cross-country Comparison of Operating Hours, Capacity Utilisation, Working Times and Employment." In *Operating Hours and Working Times*, edited by Lei Delsen, Derek Bosworth, Hermann Groß, and Rafael Muñoz de Bustillo y Llorente 41–71. Springer.

- Blos, Mauricio F, Mohammed Quaddus, HM Wee, and Kenji Watanabe. 2009. "Supply Chain Risk Management (SCRM): A Case Study on the Automotive and Electronic Industries in Brazil." *Supply Chain Management: An International Journal* 14 (4): 247–252.
- Bowersox, Donald J., David J. Closs, and M Bixby Cooper. 2002. *Supply Chain Logistics Management*. Vol. 2. New York: McGraw-Hill.
- Christopher, Martin, Carlos Mena, Omera Khan, and Ozgur Yurt. 2011. "Approaches to Managing Global Sourcing Risk." *Supply Chain Management: An International Journal* 16 (2): 67–81.
- Christopher, Martin, and Helen Peck. 2004. "Building the Resilient Supply Chain." *The International Journal of Logistics Management* 15 (2): 1–14.
- Cisco. 2011. "Security Annual Report – Highlighting Global Security Threats and Trends." http://www.cisco.com/en/US/prod/collateral/vpndevc/security_annual_report_2011.pdf.
- Closs, D. J., and E. F. McGarrell. 2004. *Enhancing Security Throughout the Supply Chain*. Washington, DC: IBM Center for the Business of Government.
- Colicchia, Claudia, Fabrizio Dallari, and Marco Melacini. 2011. "A Simulation-Based Framework to Evaluate Strategies for Managing Global Inbound Supply Risk." *International Journal of Logistics Research and Applications* 14 (6): 371–384.
- Croxtan, Keely L, and Walter Zinn. 2005. "Inventory Considerations in Network Design." *Journal of Business Logistics* 26 (1): 149–168.
- Dang, H., Yan, J. H., and Lai, Y. 2015. "Discussion about the Influence of the Computer Information Technology on the Logistics Management." In *Advanced Materials Research*, edited by Wen-Pei Sung, and Jimmy (C.M.) Kao, Vol. 1079, 1158–1161. Trans Tech Publications.
- Erlanson, David A., Edward L. Harris, Barbara L. Skipper, and Steve D. Allen. 1993. *Doing Naturalistic Inquiry: A Guide to Methods*. Newbury Park: Sage.
- Finch, Peter. 2004. "Supply Chain Risk Management." *Supply Chain Management: An International Journal* 9 (2): 183–196.
- Foddy, William. 1994. *Constructing Questions for Interviews and Questionnaires: Theory and Practice in Social Research*. Cambridge: Cambridge University Press.
- Fossi, Marc, Gerry Egan, Kevin Haley, Eric Johnson, Trevor Mack, Téo Adams, Joseph Blackbird, Mo King Low, Debbie Mazurek, and David McKinney. 2011. "Symantec Internet Security Threat Report Trends for 2010." *Volume* 16: 1–20.
- Franch, C. 2007. "Framework for Supply Chain Risk Management." *Supply Chain Forum: An International Journal* 8 (2): 2–13.
- Freightwatch. 2016. "Europe Intelligence Note." <http://www.freightwatchintl.com/intelligencecenter/securitynews/freightwatch-international-scic-europe-intelligence-note-12-february>.
- Frey, James H., and Andrea Fontana. 1991. "The Group Interview in Social Research." *The Social Science Journal* 28 (2): 175–187.
- Glenn Richey Jr, R., and Carol Reade. 2009. "Human Resource Management Implications of Terrorist Threats to Firms in the Supply Chain." *International Journal of Physical Distribution & Logistics Management* 39 (6): 469–485.
- Glenn Richey Jr, R., Joseph B. Skipper, and Joe B. Hanna. 2009. "Minimizing Supply Chain Disruption Risk Through Enhanced Flexibility." *International Journal of Physical Distribution & Logistics Management* 39 (5): 404–427.
- Grainger, A. 2007. "Supply Chain Security: Adding to a Complex Operational and Institutional Environment." *World Customs Journal* 1 (2): 17–29.
- Gunasekaran, Angappa. 1999. "Agile Manufacturing: A Framework for Research and Development." *International Journal of Production Economics* 62 (1): 87–105.
- Halldorsson, Arni, and Jesper Aastrup. 2003. "Quality Criteria for Qualitative Inquiries in Logistics." *European Journal of Operational Research* 144 (2): 321–332.
- Hameri, Ari-Pekka, and Juha Hintsa. 2009. "Assessing the Drivers of Change for Cross-border Supply Chains." *International Journal of Physical Distribution & Logistics Management* 39 (9): 741–761.
- Hintsa, Juha. 2011. *Post-2001 Supply Chain Security – Impacts on the Private Sector*. Lausanne: HEC Lausanne.
- Hintsa, J., J. Ahokas, T. Männistö, and J. Sahlstedt. 2010. *CEN Supply Chain Security (SCS) Feasibility Study – Final Report*. Lausanne.
- Holland, Christopher P., and A. Geoffrey Lockett. 1997. "Mixed Mode Network Structures: The Strategic use of Electronic Communication by Organizations." *Organization Science* 8 (5): 475–488.
- Jesson, Jill, Lydia Matheson, and Fiona M. Lacey. 2011. *Doing Your Literature Review: Traditional and Systematic Techniques*. Los Angeles: Sage.
- Jüttner, U., H. Peck, and M. Christopher. 2003. "Supply Chain Risk Management: Outlining an Agenda for Future Research." *International Journal of Logistics: Research and Applications* 6 (5): 197–210.
- Khan, Omera, Martin Christopher, and Alessandro Creazza. 2012. "Aligning Product Design with the Supply Chain: A Case Study." *Supply Chain Management: An International Journal* 17 (3): 323–336.
- Krippendorff, Klaus. 2004. "Reliability in Content Analysis." *Human Communication Research* 30 (3): 411–433.

- Kye, Dongmin, Jeongeun Lee, and Kang-Dae Lee. 2013. "The Perceived Impact of Packaging Logistics on the Efficiency of Freight Transportation (EOT)." *International Journal of Physical Distribution & Logistics Management* 43 (8): 707–720.
- Lee, Hau, and Özalp Özer. 2007. "Unlocking the Value of RFID." *Production and Operations Management* 16 (1): 40–64.
- Li, Changming, Lihong Guo, and Zhixin Li. 2014. "Design of Decision-Making System of Emergency Logistics Information System Based on Data Mining." *Journal of Digital Information Management* 12 (6): 383–386.
- Lincoln, Yvonna S., and Egon G. Guba. 1989. *Fourth Generation Evaluation*. Sage.
- Liu, X. Y. 2014. "Design of Logistics Information System Based on RFID Technology." In *Applied Mechanics and Materials*, edited by Maode Ma, and Xilong Qu, Vol. 608, 343–346. Trans Tech Publications.
- Männistö, Toni, Juha Hintsa, and Luca Urciuoli. 2014. "Supply Chain Crime-Taxonomy Development and Empirical Validation." *International Journal of Shipping and Transport Logistics* 6 (3): 238–256.
- Manuj, Ila, and John T. Mentzer. 2008. "Global Supply Chain Risk Management Strategies." *International Journal of Physical Distribution & Logistics Management* 38 (3): 192–223.
- Melacini, M., A. Creazza, and S. Perotti. 2011. "Analysis of Supply Chain Planning Centralisation for Multinational Companies." *International Journal of Logistics Systems and Management* 9 (4): 478–500.
- Morgan, David L. 1997. *Focus Groups as Qualitative Research*. Vol. 16. Sage.
- Norrman, Andreas, and Ulf Jansson. 2004. "Ericsson's Proactive Supply Chain Risk Management Approach after a Serious Sub-supplier Accident." *International Journal of Physical Distribution & Logistics Management* 34 (5): 434–456.
- Patton, Michael Q. 1999. "Enhancing the Quality and Credibility of Qualitative Analysis." *Health Services Research* 34 (5 Pt 2): 1189–1208.
- Peck, H. 2006. "Reconciling Supply Chain Vulnerability, Risk and Supply Chain Management." *International Journal of Logistics: Research and Applications* 9 (2): 127–142.
- Sheffi, Y. 2001. "Supply Chain Management under the Threat of International Terrorism." *The International Journal of Logistics Management* 12 (2): 1–11.
- Sheffi, Yossi. 2006. "Resilience Reduces Risk." *Logistics Quarterly* 12 (1): 12–14.
- Sillekens, Thomas, Achim Koberstein, and Leena Suhl. 2011. "Aggregate Production Planning in the Automotive Industry with Special Consideration of Workforce Flexibility." *International Journal of Production Research* 49 (17): 5055–5078.
- Stock, James R. 1995. "Advancing Logistics Research and Thought Through the Borrowing of Theories from Other Disciplines: Some Old Ideas Whose Times Have Come." Paper presented at the proceedings of the twenty fourth annual transportation and logistics educators conference, San Diego, CA.
- Svensson, Göran. 2000. "A Conceptual Framework for the Analysis of Vulnerability in Supply Chains." *International Journal of Physical Distribution & Logistics Management* 30 (9): 731–750.
- Tang, Christopher S. 2006. "Robust Strategies for Mitigating Supply Chain Disruptions." *International Journal of Logistics: Research and Applications* 9 (1): 33–45.
- Tomlin, Brian. 2006. "On the Value of Mitigation and Contingency Strategies for Managing Supply Chain Disruption Risks." *Management Science* 52 (5): 639–657.
- Tørhaug, Magne. 2006. "Petroleum Supply Vulnerability due to Terrorism at North Sea Oil and Gas Infrastructures." In *Protection of Civilian Infrastructure from Acts of Terrorism*, edited by Konstantin V. Frolov, and Gregory B. Baecher, 73–84. Springer.
- Tranfield, David, David Denyer, and Palminder Smart. 2003. "Towards a Methodology for Developing Evidence-Informed Management Knowledge by Means of Systematic Review." *British Journal of Management* 14 (3): 207–222.
- Urciuoli, Luca. 2010. "Supply Chain Security – Mitigation Measures and a Logistics Multi-layered Framework." *Journal of Transportation Security* 3 (1): 1–28.
- Urciuoli, Luca, Juha Hintsa, and Juha Ahokas. 2013. "Drivers and Barriers Affecting Usage of E-customs – A Global Survey with Customs Administrations Using Multivariate Analysis Techniques." *Government Information Quarterly* 30 (4): 473–485.
- Urciuoli, Luca, Toni Männistö, Juha Hintsa, and Tamanna Khan. 2013. "Supply Chain Cyber Security-Potential Threats." *Information & Security* 29 (1): 51–67.
- Urciuoli, L., S. Mohanty, J. Hiints, and E. G. Boekesteijn. 2014. "The Resilience of Energy Supply Chains: A Multiple Case Study Approach on Oil and Gas Supply Chains to Europe." *Supply Chain Management: An International Journal* 19 (1): 46–63.
- Wang, Hua, Shuaian Wang, and Qiang Meng. 2014. "Simultaneous Optimization of Schedule Coordination and Cargo Allocation for Liner Container Shipping Networks." *Transportation Research Part E: Logistics and Transportation Review* 70: 261–273.
- Warren, Matthew, and William Hutchinson. 2000. "Cyber Attacks Against Supply Chain Management Systems: A Short Note." *International Journal of Physical Distribution & Logistics Management* 30 (7/8): 710–716.
- Waters, C. D. J. 2007. *Supply Chain Risk Management: Vulnerability and Resilience in Logistics*. London: Kogan Page.

- Williams, Z., J. E. Lueg, and S. A. LeMay. 2008. "Supply Chain Security: An Overview and Research Agenda." *The International Journal of Logistics Management* 19 (2): 254–281.
- Yao, Enjian, Zhifeng Lang, Yang Yang, and Yongsheng Zhang. 2015. "Vehicle Routing Problem Solution Considering Minimising Fuel Consumption." *IET Intelligent Transport Systems* 9 (5): 523–529.
- Zsidisin, George A., Alex Panelli, and Rebecca Upton. 2000. "Purchasing Organization Involvement in Risk Assessments, Contingency Plans, and Risk Management: An Exploratory Study." *Supply Chain Management: An International Journal* 5 (4): 187–198.

Appendix

Table A1. Main journals used for the literature review.

Journal title	No.
<i>Advanced Materials Research</i>	1
<i>Applied Mechanics and Materials</i>	1
<i>IET Intelligent Transport Systems</i>	1
<i>International Journal of Logistics Research and Applications</i>	3
<i>International Journal of Logistics Systems and Management</i>	1
<i>International Journal of Physical Distribution & Logistics Management</i>	5
<i>International Journal of Production Economics</i>	1
<i>International Journal of Production Research</i>	2
<i>Journal of Business Logistics</i>	1
<i>Journal of Digital Information Management</i>	1
<i>Journal of Transportation Security</i>	1
<i>Logistics Quarterly</i>	1
<i>Management Sciences</i>	1
<i>Operating hours and working times</i>	1
<i>Organization Science</i>	1
<i>Production and Operations Management</i>	1
<i>Supply Chain Forum: an International Journal</i>	
<i>Supply Chain Logistics Management</i>	1
<i>Supply chain management: an international journal</i>	4
<i>Supply Chain Risk</i>	1
<i>The International Journal of Logistics Management</i>	2
<i>Transportation Research Part E: Logistics and Transportation Review</i>	1
	32

Open-ended survey and interview questions

- Please give a high level description of your supply chain and supply chain management strategy?
- How is risk management organized in your company, regarding the supply chain?
- Which crime types are your company and supply chain most vulnerable to today?
- Can you please describe your overall security management system?
- Which are the main methods and approaches to securing your supply chain?
- Where do you see gaps in your security management today?
- Where do you see the most worrying trends to be regarding crime in the future?
- Can you identify the top three crime issues in the future for your supply chain – and views on future security measures designed to counter or combat them?
- What would you put as the number one priority in a strategic roadmap for European supply chain security for the next 5 years?