J Transp Secur (2010) 3:105–125
DOI 10.1007/s12198-010-0042-3

A comprehensive framework for analysis and design of supply chain security standards

Juha Hintsa

Received: 24 February 2010 / Accepted: 4 March 2010 / Published online: 30 March 2010

Abstract An avalanche of new supply chain security (SCS) standards, programs and regulations have emerged since 2001. These have been developed and promoted by various governmental, supply chain and standardization parties. Due to political, economic, technical and legal reasons, no dominating global standard has been developed that covers all possible aspects of SCS. Instead, we have seen national and regional, transport mode-specific, crime issue-specific, and other types of more focused SCS standards gaining some popularity within supply chain operating communities. This paper intends to capture and explain the most relevant SCS standard characteristics, in order to form a pragmatic framework for the analysis and design of SCS standards for the benefit of governmental policy makers and business community supply chain and security experts. A theoretical framework derived from the literature is tested and further developed in a real-life SCS standardization feasibility study project. Recommendations are made as to how the framework might be exploited, and topics for future research are suggested.

Keywords Supply chain security (SCS) · Standardization · SCS standards · European Committee for Standardization (CEN) · Crime · Terrorism

Introduction

After the terrorist attacks in 2001, the "9/11 incidents", a new era started in the development of supply chain security (SCS) standards, programs, guidebooks, regulations and other initiatives. Prior to 2001 it was largely left to business to determine and manage their activities regarding the fight against theft and other forms of crime in supply chains. Governments also had their interest in SCS matters when it came to smuggling for tax evasion, the illegal narcotics trade, trade in

J. Hintsa (✉)
Cross-border Research Association, c/o BMT, Ave d'Echallent 74, CH-1004 Lausanne, Switzerland
e-mail: juha@cross-border.org

counterfeit goods or violations in compliance with environmental regulations, some of which may have even had life-threatening consequences. The events of 2001, however, changed this situation: governments, first in the US, and later worldwide, started to introduce SCS regulations and voluntary programs—the latter being included under the category of "SCS standards" in this paper—primarily to mitigate the risk of terrorism in global supply chains. At the same time, some private sector actors and some international organizations, including various global, regional and national standardization bodies, have become active in bridging any perceived gaps in the broad field of SCS, covering not just anti-terrorism, but also many traditional and emerging forms of crime in supply chains. One could even conclude that with all the new governmental and private sector SCS standards, there has been a real rush to secure supply chains, either against real or perceived threats.

The goal of this paper is to develop a comprehensive framework to help analyze existing and design new SCS standards in the future. For the purpose of this paper all SCS initiatives developed voluntarily by private sector, international organizations, and/or public administrations are categorized as "SCS standards", as long as they are not mandatory to implement (i.e. not regulations). Below are two key definitions regarding "SCS management" and "standards":

Supply chain security (SCS) management:

> *"SCS management covers all processes, technologies and resources exploited in a systematic way to fight against end-to-end supply chain crime; the primary goal of each single SCS measure is either to prevent a crime, to detect a crime, or to recover from a crime incident in the fastest possible time; single SCS measures fall typically within one of the following five categories: cargo, facility, human resources, information technology, and business network; the typical supply chain crime includes theft, smuggling, counterfeiting, sabotage, black-mailing for financial gain, terrorism for destruction, and any type of fraud and corruption (the detailed crime definitions subject to national and international regulations)."* (Hintsa et al. 2009*, with some printing mistakes corrected).*

> A standard: *"a document containing a series of requirements and/or recommendations in relation to products, systems, processes or services." Standards can also describe a measurement or test method or establish a common terminology within a specific sector. Standards are tools providing a consistent solution to recurrent problems. They are based on consensus reached in a dynamic process of hearing objections until a general agreement can be observed (see e.g. Hintsa et al. 2010).*

The framework for SCS standards is developed and tested in two steps in this paper: in step 1 a theoretical framework is derived from literature, and in step 2 this framework is tested and developed further with a practical case study. Behind this process, there is an intention to identify dimensions and parameters to answer questions such as:

- Why should a (new) SCS standard be developed in the first place?
- What are the main tangible goals and benefits of a (new) standard?
- Who are the parties behind a SCS standard development process?
- What does the development process for a SCS standard look like?
- What is the geographical coverage of a (new) SCS standard?

– What are the underlying philosophies with a (new) SCS standard?
– What are the other characteristics of the (new) SCS standard like?
– Who will ensure compliance with a (new) SCS standard?

These, and other related questions emerging from the literature will be dealt with in this paper, firstly in the development of a theoretical framework, then secondly by testing the framework under real SCS scenarios and, finally, drawing conclusions and making some suggestions for future research.

Development of a theoretical framework

According to a recent scenario study on 21st century supply chains and business-customs interaction, supply chain security (SCS) forms an important change driver for the future (Hameri and Hintsa 2009), thus providing background motivation for this paper in SCS standards:

> *"The vulnerabilities of international supply chains will increase in the future, driven by various external hazards and risks, lean operational models as well as changes imposed by regulatory countermeasures. Companies are particularly concerned about future disruptions in material supply and transportation, which will have negative impact on Just-in-time operations. In supply chain security management, companies will definitely be investing more in supply chain security measures; business—government relationships in security management will get deeper; and many of today's pilot-phase supply chain security technologies for crime prevention, detection and recovery will become mainstream tools in the future. It is anticipated that via various certification programs and "secure trade lane" schemes, there will be two or more categories of "secure vs. very secure operators and supply chains".* (Hameri et al. 2009)

Security concerns in trade, logistics and transport systems are not new phenomena: sea pirates have been threatening and attacking merchant ships for centuries, and bandits have been stopping and robbing trains since the invention of steam engines; these are just two obvious examples. Other illegal activities, such as the evasion and avoidance of duties and taxes, cross-border fiscal fraud, the smuggling of drugs, dangerous, harmful and prohibited goods, money laundering, and trade in counterfeit goods (WCO 2008), have appeared throughout time; they have represented opportunities for criminals, and attracted criminals, to a various extent throughout the years. Counter measures in the form of regulations and standards have evolved to remove the opportunity for crime and attraction of committing a crime. Many crime types are, therefore, a concern for both governmental and business; some crime types are of primary concern to the former while others are of more concern to the latter (Hintsa et al. 2010).

Professor Hau Lee of Stanford University (Lee and Wolfe 2009) explains the overall shift of focus in supply chain security (SCS) since the terrorist attacks in 2001, from making supply chains 'theft-proof to tamper-proof',: '*Prior to Sept. 11, 2001, most discussions of freight transportation security focused on controlling theft and reducing contraband such as drugs, illegal immigrants, and the export of stolen*

cars and construction equipment. After Sept. 11, the highest-order definition of freight security changed from theft-proof to tamperproof. Terrorism and the threat of weapons of mass destruction have transformed perceptions of security across the supply chain.' Similar views are shared by other authors discussing the post-2001 anti-terrorism focus, including Russell and Saldanha (2003); Closs and McGarrell (2004); Willis and Ortiz (2004); Thibault et al. (2006) and Williams et al. (2008).

At the same time when anti-terrorism has been introduced into the SCS agenda, the other types of crime have not disappeared—one could even estimate that the opposite has indeed occurred. "One size does not often fit all"—even if some security approaches could work simultaneously against terrorism and other types of crime—thus, the first question being raised regarding existing and future SCS standards is:

SCS standard framework question 1: Is the main focus of a SCS standard anti-terrorism or anti-crime?

Related to this first question is the identity of the originators of the SCS standard: they could be public bodies (e.g. a customs or a transportation authority), an international governmental organization (e.g. International Standards Organization, ISO or the World Customs Organization, WCO), a business alliance (e.g. Transported Assets Protection Association, TAPA, to protect transported high value goods or Business Alliance for Secure Commerce, BASC, to minimize smuggling of narcotics from a high risk area) or anything in between. In particular, Gutierrez and Hintsa (2006) divide the originating actors for SCS standards into the following three groups: international organizations; governmental agencies; and private sector entities. The main goal of the standards can be any one of the following four: enhancing customs administrations security control capacity; reducing specific industry/geography vulnerability; developing global security standards; and technology development/pilot projects (Gutierrez and Hintsa 2006).

Several authors discuss the relevance of public–private-partnership approaches and the need for pro-active collaboration during the development and/or implementation process of the SCS standard. The implementation process could be carried out—independently from the actual originating, according to Sarathy (2006), Grainger (2007), and latterly Closs et al. (2008) who referred to the example of where firms may actively participate in the development of government standards or security initiatives as a '*public interface management*'. WCO (2008) explained it in a broader context of public–private relationships: '*Customs in the 21st century should enter into strategic pacts with trusted economic operators. Customs needs to understand the concerns of business, while business needs to know the requirements of customs.*' Even though the partnership approach is crucial for the (sustainable) success of any SCS standard, they tend to have one type of originating actor, thus raising the second question for the SCS standard framework:

SCS standard framework question 2: Are the main originating actors for a SCS standard public or private entities?

Next, taking the user perspective of a SCS standard, one should look first how supply chain management is being defined, as this provides the framework for any

SCS user-related discussions. For example, Closs and McGarrell (2004) state that '*supply chain management is the inter- and intra-organizational coordination of the sourcing, production, inventory management, transportation, and storage functions with the objective of meeting the service requirements of consumers or users at the minimum cost.*' Within this frame, White et al. (2004) divide the potential users of a SCS standard into two groups: (a) users of the freight transportation systems and (b) providers of the freight transportation systems. The former typically consist of 'cargo owners', like manufacturers, shippers, importers and retailers, whilst the latter consist of sea port/terminal operators, trucking, shipping and air cargo companies, and other logistics sector actors.

One immediate concern regarding the interplay between these two groups is the unbalanced sharing of SCS investment benefits and/or the SCS investment costs. This has been raised, for example, by Thibault et al. (2006) and Peleg-Gillai et al. (2006), the latter quoting '*...shippers often benefit from the investments made by LSPs, but the reverse is seldom true.*' This point, amongst other SCS interplay related arguments and concerns, makes it crucial to identify who is the primary user of a SCS standard:

SCS standard framework question 3: Is the primary party complying with a SCS standard a user or a provider of transportation services?

Relating also to this the third question is the issue of SCS standardization: what are the specific physical and non-physical security measures which are exploited to protect the various supply chain assets? White et al. (2004) lists the following elements as crucial in supply chain operations: '*Emerging security concerns affect all freight transportation modes (e.g., air, ocean, rail, highway, pipeline) and all components of the system: (a) the physical infrastructure, e.g., roads, bridges, tunnels, seaports, airports, plants, distribution centers, warehouses, pipelines and pipeline pumping stations; (b) the information infrastructure, e.g., traffic operations centers, communications systems for mobile assets; (c) people, e.g., truck drivers; (d) cargo, e.g., containers, hazardous materials; and (e) vehicles, e.g., ships, trains, trucks (power units, trailers, chasses), airplanes.*'

Gutierrez and Hintsa (2006) conducted an analysis of ten existing voluntary SCS standards, and concluded that security measures in these standards tended to fall into following five categories: facility security; cargo security; human resource security; information management security; and business network security. Some of the 25 typical security measures under these five categories are of a physical security nature, such as facility protection, access control and cargo protection; some are of a non-physical nature, such as personnel training and business partner evaluation systems. This observation raises the fourth question for the SCS standards framework:

SCS standard framework question 4: Q4. Does a SCS standard place emphasis on physical security measures or on non-physical security measures?

A SCS standard, just like a standard in any domain, can have geographical scope between anything from a purely national standard to a regional standard, or to a global standard: which geographical approach works the best, depends on the case in hand. Examples of national SCS standards include the Swedish Stairsec program and

British Standard, BS, 'Guide for security of buildings against crime' (BS 8220-3:2004). Examples of regional SCS standards include the Latin American BASC-program, the US C-TPAT, and the European Union AEO-program. On a global scale, the most obvious standards are ISO 28000 series and WCO SAFE Framework of standards (see e.g. Lake et al. 2005; Grainger 2007; Kommerskollegium 2008; Donner and Kruk 2009).

It is clear that especially global manufacturing, trade and logistics companies are in favor of the last category, i.e. global standards: harmonization and standardization of security processes internationally and domestically remain important goals for multi-nationals (Lee and Wolfe 2009). Closs and McGarrell (2004) also talk about the shift from country or geographic focus to a global focus in respect of SCS management. However, the reality still being that SCS standards are mostly either regional or national, raise the fifth question for the development of a SCS standard framework:

SCS standard framework question 5: What is the geographical coverage of a SCS standard: local versus global?

The customs originated SCS standards focus on international application, i.e. cross-border supply chains with customs transactions. National or regional trade, without crossing customs borders, falls into the category of inland SCS standards. Even with the "cross-border SCS standards", however, many of the actual security requirements take place inland, primarily in the country of import (i.e. the home country for the customs authority in question) but also, in some cases, abroad and mainly in the country of origin/country of departure (see e.g. Hintsa et al. 2010). Even though the content and requirements of a cross-border SCS standard can look very similar to an inland SCS standard, it is crucial to differentiate from the beginning, which one of the two is the primary scope for a SCS standard:

SCS standard framework question 6: Does a SCS standard focus on cross-border supply chain issues or inland supply chain issues?

Linked with the two previous questions (regarding the geographical scope and cross-border versus inland scope of a SCS standard) the next important issue is about cross-recognition (or mutual recognition) between two or more SCS standards. This is especially relevant with non-global SCS standards having a cross-border (i.e. customs) focus (see e.g. Hintsa et al. 2010).

Skinner et al. (2008) define the goal of mutual recognition as: '*to link the various international industry partnership programs, so that together they create a unified and sustainable security posture that can assist in securing and facilitating global cargo trade.*' From a business perspective, mutual recognition between various national and/or regional SCS standards appears to be a key issue, when following writings in trade journals, practitioner guidebooks and industry conferences (see e.g. Edmonson 2005; Kommerskollegium 2008; Miller 2009; Donner and Kruk 2009).

From a governmental perspective, a European Commission DG TAXUD[1] officer (Wright 2009) talked about the perspective for mutual recognition through

[1] Directorate General for Taxation and Customs Union.

international agreements, as one of the potential benefits for AEO-security. He also highlighted that EU–US customs security co-operation has the '*key objective of reciprocity and mutual recognition, targeting for implementation of mutual recognition between the two programs (C-TPAT and EU AEO) during 2009.*' The relevance of customs-to-customs mutual recognition schemes is also explained by ECMT et al. (2005): '*Mutual recognition of exporting, transit and importing Customs control and risk management processes will go a long way to facilitate early and effective security screening for containerized consignments.*'

To conclude: mutual recognition issues, during the (obvious) absence of one "ultimate global one-size-fits-all" SCS standard, leads one to the seventh question for the development of a SCS standard framework:

SCS standard framework question 7: Is a SCS standard being recognized by one or more other SCS standards?

The next issue deals with various audit, validation and verification processes related to the compliance with a SCS standard, before, during and after the certification process. An example of a government-conducted verification is that of the C-TPAT program: the status is first granted following a security profile filled by the applicant, and followed by customs verification within 3 years (Sheu et al. 2006). An example of a third (business) party audit scheme is that of the BASC program: BASC certification is valid for 1 year and can be renewed after passing a second security audit (Gutierrez et al. 2007).

Several authors, including Russell and Saldanha (2003), Sheu et al. (2006), Sarathy (2006) and Williams et al. (2008), explain about announced and unannounced security audits and inspections between the supply chain partners where, for example, shippers carry out audits on carriers. Sarathy (2006) highlights the importance of ' *...cooperative strategies with supply chain partners—assessing and auditing security readiness.*' These various SCS standard verification schemes introduces the eighth question for the development of the SCS standard framework:

SCS standard framework question 8: Are the detailed SCS standard requirements verified by a government party or by a business party?

By definition, SCS regulations such as ISPS-code (with the International Maritime Organization, IMO), Aviation security (with the International Civil Aviation Organization, ICAO) and the 24 h rule (for all maritime cargo heading to the US) tend to establish a level playing field in relation to their implementation, i.e. all actors impacted by the regulation in the supply chain are required to implement the same security measures (see e.g. Lake et al. 2005; Grainger 2007; Bichou 2008; Hintsa et al. 2010; Donner and Kruk 2009). An alternative to this is a risk-based approach in SCS standard design and implementation requirements, where the tangible requirements to comply with a SCS standard are fixed. This is based on the anticipated or perceived threats, vulnerabilities, risk likelihoods and consequences with a particular supply chain / actor / time / environment etc. In addition, risk assessment or risk management can form part of a SCS standard itself, creating an

iterative process of assessing threats and vulnerabilities and optimum risk mitigation strategies and measures for the various actors in the supply chain (see e.g. Hintsa et al. 2010).

Numerous papers exist both in academic and in practitioner domains, highlighting the relevance of risk-based approaches in SCS management. Academic contributions include Kwek and Goswami (2003); Sarathy (2006); Bichou (2008) and Rucinski (2009), and contributions from so-called practitioners include Eggers (2004); UIRR (2007); Solnik (2009), Burkhardt (2009) and Donner and Kruk (2009). From a government perspective, it appears to be well understood that '*scarce resources need to be targeted to the higher end of the risk continuum*' (WCO 2008). These and many other arguments raise the ninth question for the development of a SCS standard framework:

SCS standard framework question 9: Is a SCS standard built on the basis of risk assessment or on the provision of a level playing field?

Following on from, and related to the previous question regarding exploiting risk assessment as part of the overall SCS standard design and implementation process, comes the topic of whether a SCS standard should focus on preventing incidents or on helping to recover after an incident has occurred, sometimes referred to as 'supply chain resilience'. Several academics including Helferich and Cook (2002); Russell and Saldanha (2003); Kwek and Goswami (2003); Wright et al. (2006) and Sarathy (2006) talk about various ways of grouping security measures into 'prevention versus recovery'—categories, the former presenting '*planning—mitigation—detection—response—recovery*' as the list of possible security actions.

From a governmental perspective, a European Commission officer (Liem 2009) talks about '*building up capabilities related to the phases of a security incident', with following six phases: (a) identify (incident related); (b) prevent (threat related); (c) protect (target related); (d) prepare (operation related); (e) respond (crisis related); and (f) recover (consequence related)*.' The UK Home Office, under their anti-terrorism agenda (not only SCS), presents the following four phase model: '*The new strategy retains the framework of the old strategy—four main areas of work known as 'the Four Ps'—Pursue, Prevent, Protect and Prepare.*'[2]

One angle for the balancing act between the various phases in security management is presented by Lee and Wolfe (2009) who draw analogies between total quality management and SCS, by placing emphasis on quality problem prevention, source inspection, process controls and continuous improvement cycle over quality inspections (at the end of the process or supply chain). Even though the 'nature of the beast' is different with quality and security—as an example, the enemy of the latter, i.e. criminals and terrorists, can learn quickly how to avoid new security measures: a SCS standard can be based primarily on preventative measures, following the analogy used by Lee and Wolfe (2009), if seen as providing security,

[2] http://www.homeoffice.gov.uk/about-us/news/taking-new-approach-ct , retrieved 6.12.2009.

and cost-efficient. This brings us on to the tenth question for the development of a SCS standard framework:

SCS standard framework question 10: Does a SCS standard have a primary focus on incident prevention or post-incident recovery?

Looking at the overall nature of existing SCS standards, one can observe a spectrum of approaches: from covering overall security management systems and standard frameworks (such as ISO 28000 series and WCO SAFE Framework of Standards), to generic security questions / check lists (such as C-TPAT and EU AEO), to focused technical norms (such as BS 8220-3:2004 Guide for security of buildings against crime) (see e.g. Hintsa et al. 2010). One could observe here a potential link with question five above: maybe the global SCS standards lean to the direction of overall management / framework systems, while the national SCS standards are more focused on dealing with specific security issues. In any case, the extremes of this spectrum should lead us to as the eleventh question for the development of a SCS standard framework:

SCS standard framework question 11: Is the basic nature of a SCS standard reflective of an overall management system or a targeted norm?

The benefits from implementing and complying with a SCS standard remains one of the most debated areas in the whole domain of SCS academic and practitioner literature. The first question in this SCS standard framework, regarding anti-crime versus anti-terrorism, contains the assumption that SCS standards should provide some direct security-related benefits: for example, they should result in less crime attempts or realized incidents, otherwise the whole concept of implementing "security standards" could be misleading. Of course, one must also be aware of the complexities in the assessment of SCS standards: how can you measure something which did not happen? Firstly, one is rarely in possession of accurate statistics of realized security incidents. Secondly, one does not usually know about all possible criminal attempts which failed due to the existence of a security standard; and thirdly, crime incidents can simply go down due to criminals shifting their focus into "more lucrative business", regardless of any security efforts in the supply chain (see e.g. Hintsa et al. 2010).

Numerous authors including Rice and Spayd (2005), Sheu et al. (2006), Peleg-Gillai et al. (2006), Gutierrez et al. (2007), Diop et al. (2007) and Hintsa and Hameri (2009) talk about qualitative and, to some extent, quantitative benefits following SCS standard implementation and compliance. However, most of these so called direct, indirect and collateral benefits regarding higher asset utilization, better supply chain visibility, lower inventory levels etc. are extremely difficult to measure and to link with the actual security enhancements in the supply chain, thus such "non-government granted benefits" are left out from this framework.

Furthermore, several authors have undertaken analysis of specific government agency–granted benefits in the supply chain, and few examples (without quantification) are listed below. Sarathy (2006) talks about '*reduced delays caused by security concerns—green lane (concept)*'. Peleg-Gillai et al. (2006) identify '*more efficient*

customs clearance process, with reductions in cargo delays, and reduction in cargo inspections/examinations.' Gutierrez et al. (2007) point out '*facilitation of border crossing operations (with) fast/stable/predictable border crossing process and preferential treatment in alert and post disaster situations.*' Finally, Diop et al. (2007) lays out schemes for '*reduced inspection costs and reduced border crossing times.*'

As such government agency-granted benefits can be considered (the most) deterministic type of SCS standard benefits. Therefore the twelfth question for the development of a SCS standard framework is:

SCS standard framework question 12: Do government agencies provide tangible benefits attached to a SCS standard?

The penultimate question deals with possibilities of having two or more levels of security certification within a single SCS standard. A higher level of certification would be expected to deliver more benefits than a "Basic level certification", as for example, government-granted benefits as discussed in the previous question. The conceptual basis for this was first presented by Rice and Caniato (2003), who classify "packages" of security responses and measures into the following four groups: Level 1—Basic initiatives; Level 2—Reactive initiatives; Level 3—Proactive initiatives; and Level 4—Advanced initiatives.

Looking at actual SCS standards, one case has been identified where there are two or more certification levels in place: the US C-TPAT program, which has a three-tier structure. In a cost-benefit survey with the C-TPAT participants (Diop et al. 2007), it is stated that '*Tier 3 companies were to receive the maximum level of benefits provided under the program.*' The Swedish customs security program called STAIRSEC represents a different case of SCS certification levels: in order to be eligible to apply for this program, a company must be fist certified in a 5-level trade facilitation program called STAIRWAY, to a minimum level 3 or above (up to level 5) (Kommerskollegium 2008).

Lastly, one can also look at the various government anti-terrorism threat level-systems: for example, the UK Home Office have five threat levels: '*Low—an attack is unlikely; Moderate—an attack is possible, but not likely; Substantial—an attack is a strong possibility; Severe—an attack is highly likely; Critical—an attack is expected imminently.*'[3] One could speculate whether 'benefit' schemes exist, that would allow supply chain operators with a high level of SCS certification to operate during high threat level situations and/or post-incident situations. Even if such schemes would not exist today, this whole issue of SCS certification levels remains the penultimate question to be answered in the development of a SCS standard framework:

SCS standard framework question 13: Does a SCS standard have more than one certification level in place?

Finally, the issue of costs and financing SCS remains a major topic of practitioner and academic debates. By nature, governments have the tendency to introduce SCS standards for ever greater security, protecting society from terrorism concerns or

[3] https://www.mi5.gov.uk/output/what-are-threat-levels.html , retrieved 6.12.2009.

some other forms of crime which pose a threat to government finances or other interests (e.g. violations against customs regulations). Businesses are concerned more about "over investment" in SCS. As only some of the SCS costs on the infrastructure side may fall naturally into the government's remit, most other SCS investment and operational costs must be financed by supply chain operators themselves (see Diop et al. 2007; Hintsa et al. 2010). Even though at the end of the day it is the consumers and tax payers, i.e. private citizens, who pay the cost of SCS in the product prices and/or government taxes, it is crucial to raise this last question for the SCS standard framework:

SCS standard framework question 14: Is a SCS standard financed by public entities or by private entities?

To conclude on the development of the theoretical framework, these 14 questions, i.e. "14 dimensions for the SCS standard framework", each with two basic optional replies, are visualized in Figure 1 below.

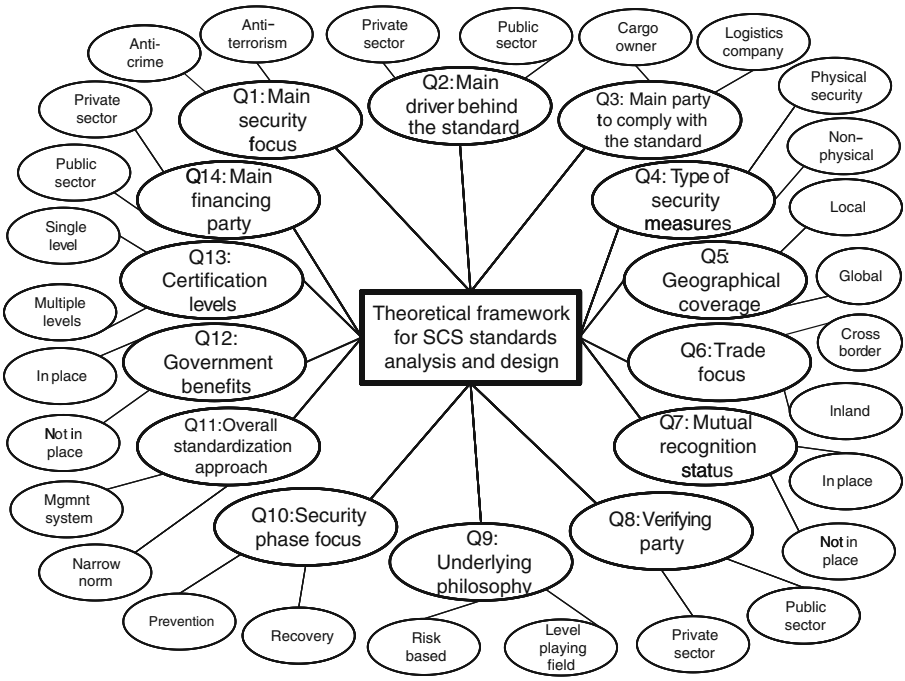

Figure 1 Theoretical framework for SCS standards analysis and design

Case study on the framework

> *"One of the first advantages of standardization is that it enables public authorities to limit regulations to cases where compulsion is essential. Standardization thus economizes on the making of regulations"* (Deming 1991).

In this chapter the theoretical framework for SCS standard analysis and design is tested and partially further developed with a real case in SCS standardization: "A feasibility study for a possible SCS standard in Europe".[4] This study was mandated by the European Committee for Standardization (CEN),[5] and Cross-border Research Association (CBRA) was granted the study contract. A team of four CBRA researchers conducted this study between January and November 2009. The study included 21 interviews with European experts in SCS, trade association and standardization fields, as well as a supply chain operator survey with 86 companies in manufacturing, logistics and distribution/retail sectors. Besides a set of recommendations for the actual SCS family of standards (not presented here), the study concluded with the framework level recommendations, explained below by answering the 14 questions, and illustrated in Figure 2 at the end of this chapter.[6]

Q1. Is the main focus of a SCS standard anti-terrorism or anti-crime?

The experts interviewed in the CEN-study shared a uniform view that (a) crime, including cargo theft, is on a growing trajectory in Europe, and that (b) terrorism in supply chains is not a major concern for supply chain operators in Europe today. Quoting from an expert highlighting the first point was: "*you see a rise in criminality (since 2001)... problems with thefts in trucks... increasing theft in storage areas... there is more awareness with stakeholders... the supply chain is the weakest link...*". Another expert stated that "*crime in supply chains has increased (since 2001), including smuggling, counterfeiting, parallel trade and theft...*". Regarding the latter point on terrorism in supply chains, one expert shared his concern that "*we have to pay millions for supply chain (security), even though there has been no incident of terrorism".*

Regarding whether one SCS standard, or even a single security measure, could tackle both anti-terrorism and anti-crime aspects of supply chain security, there was less consensus between the interviewed experts. One expert seeing the two issues as non-connected said that " *(the two have) nothing in common, as the consequences and responses are so different".* Another expert seeing similarities stated (without specific examples) that "*the link between security and normal criminal activity and protection against terrorist actions… there is a link, certainly: if you increase anti-terrorism, you increase security against normal crime".*

Finally, having this aspect tested in a survey for supply chain operators,[7] the CEN-study concludes that the main focus of a new SCS standard should be "normal

[4] In this paper, this study is referred to as "CEN-study".
[5] The official name and number of the CEN Technical committee is ´CEN/TC 379 Supply Chain Security´.
[6] The first draft of the full report is available by (email) request to the author of this paper.
[7] The full results of the CEN SCS feasibility study, supply chain operator survey, will be published as a separate paper, with proper statistical analysis included.

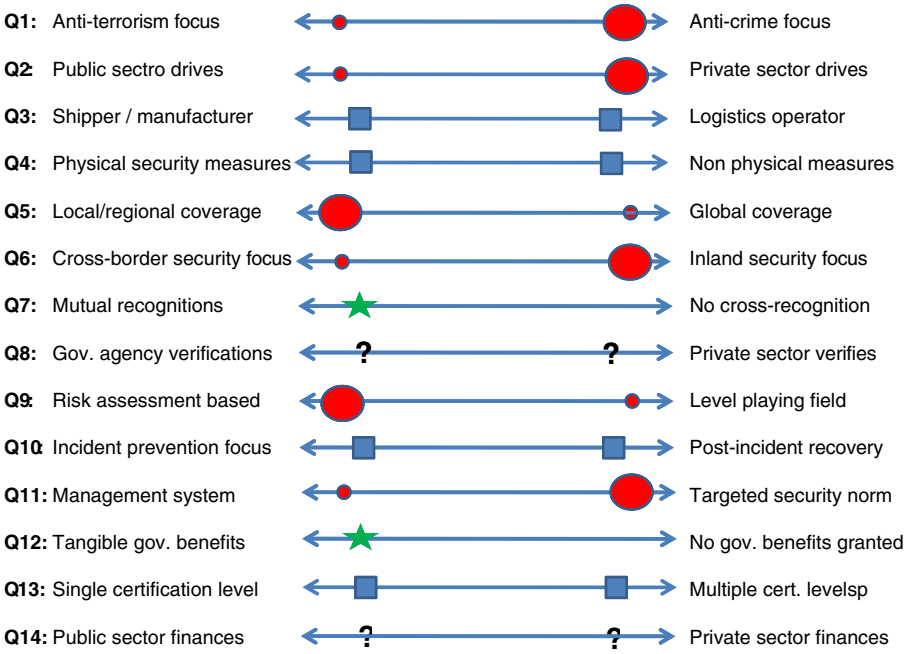

Figure 2 Summary of the CEN-study framework level recommendations

crime", in particular cargo theft. However, synergies with anti-terrorism measures should be explored, whenever feasible.

Q2. Are the main originating actors for a SCS standard public or private entities?

As Deming (1991) has stated, (voluntary) standards can be a way to avoid (mandatory) regulations, and this was given as an implicit starting point for the CEN-study—i.e. instead of having a European regulation for minimum SCS requirements in intra-EU supply chains, the feasibility of a voluntary CEN standard (or family of standards) was to be studied. Thus, regarding this question 2 of the SCS standards framework, the CEN-study concludes that business / private entities should be in the driver's seat, as businesses normally know best where the main crime issues are, and what should be done to mitigate the crime risks, in a cost efficient manner. However, with some specific standards, the collaboration and/or recognition of government agencies may be useful, thus a public–private-partnership attitude is recommended.

Q3. Is the primary party complying with a SCS standard a user or a provider of transportation services?

The scope for the CEN-study included various types of actors in the supply chain: manufacturers, shippers, logistics service providers, carriers, wholesalers, and retail companies, amongst others. No initial distinction between the various actors was made. After identifying a set of tangible standard ideas and testing them in a supply chain operator survey, it turned out that some (sub)standards can be targeted

for all actors, and some only to certain type of actors, in particular logistics companies.

Related to this question was the issue of whether or not SCS standards should focus on multi-modal transport and interconnectivity between various transport modes; or else whether it should enhance security for single actors and/or industry sectors. The study recommendation was as follows: new SCS standards should not emphasize one over the other—but this decision should be made on a case by case basis, potentially involving both aspects in the standard / family of standards.

Q4. Is the primary content of a SCS standard made of physical security measures versus non-physical measures?

The mandate for the CEN-study didn't specify in any way whether the focus should be on tangible physical security surrounding facilities, conveyances, cargo, products, IT-centers etc., or whether the possible standard should focus on non-physical issues such as risk management processes, data exploitation, employee training, to name but a few. Even though a slight emphasis is set on the non-physical security measures, based on gap analysis, cost analysis, and user needs analysis carried out in the CEN-study operator survey, these two alternatives are recommended to be treated on equal basis regarding development of any new SCS standard.

Q5. What is the geographical coverage of a SCS standard: local versus global?

The interviewed experts didn't have a consensus view whether new SCS standard development (if any were indeed required) should be more global, regional or local in nature. Sample arguments for the global approach included: "*Trade is global by nature, and thus only global standards for SCS are necessary...we fear that EU goes ahead with its own SCS requirements (while this would be followed by other regions).*"; and *"...if a standard, then a global one...otherwise there will be a disconnect with supply chains…".* Opposite views were shared by another two experts, of which the first one emphasized the regional approach by saying that "*Europeans have to comply with SCS regulations, all focusing on international trade... as this initiative concerns intra-EU supply chains.*" and the second one hinted towards the necessity of a local approach by stating that "*Cross-European haulage is small, involving some countries like Ireland and Scandinavia, (otherwise it is) mostly about national movements".*

The CEN-study finally concludes that SCS standards can have a regional focus, as has happened before with various SCS initiatives for example in Latin America, the US and in Europe: this approach might allow more focus on regional matters, via inputs by experts in the region, as well as faster design and implementation lead time, than a global initiative. Also, the majority of the companies participating in the operator survey, saw transnational crime as a growing concern in Europe, thus indicating the need to develop tools and standards to fight against it. At the same time, regional SCS standards should be linked with global (or other regional) standards, in order to facilitate global trade, and to support the fight against crime also on a worldwide basis, whenever feasible.

Q6. Does a SCS standard focus on cross-border security issues or inland security issues?

Most of the post-2001 SCS standards have a customs authority interest behind them: therefore, they imply a strong focus on security issues related to cross-border movements of goods and cargo. One should not duplicate existing work in SCS standards: therefore, one ought to complement the existing standards, in cases where gaps exist. The CEN-study recommended focusing on inland security issues, without forgetting to proactively seek links and/or recognitions with the existing customs SCS initiatives, on a case-by-case basis.

Q7. Is a SCS standard being recognized by one or more other SCS standards?

Mutual recognition—or more commonly the lack of them—is a major topic in the world of SCS standards; this is also true within the CEN-study. One of the experts elaborated on the issue by saying that "n*ow you get all different agencies involved in terrorism... too many programs, too difficult... no one-stop-shop. regarding SCS, the one-stop-shop, mutual recognition of programs is crucial... with EU AEO and regulated agent status...".*

Following the outcomes of the operator survey, mutual recognition with other European, and other regional or global SCS standards is recognized as an important component for a possible new SCS standard; however, the practical details will depend on the final scope and content of any possible new SCS standard, to be investigated on a case-by-case basis.

Q8. Are the detailed SCS standard requirements verified by a government party or by a business party?

This crucial question on which external party, if any, does the security audits, falls mostly out of scope for the CEN-study, thus it is not answered here. The assumption is that normal CEN-protocols and procedures will be followed for any types of verification, auditing, certification and monitoring activities—but this requires further analysis and laying out the options.

Q9. Is a SCS standard built on the basis of risk assessment or on the provision of a level playing field?

There was a clear consensus amongst the experts in the CEN-study that any new SCS standard development should be based on risk assessments, rather than a level playing field-approach. Four expert quotes were as follows: "*The main change now (compared to previous SCS initiatives): instead of securing the whole supply chain, we must do risk assessment first…" ; "Risk management approach is very important… you should identify the problem you want to tackle…then you look at the context…you can tailor-make measures to your situation…the outcome could be: you have to protect yourself in this and this area—but not giving another checklist"* ; *"If you don't have credible risk assessment in place (for containers), you should open every box… this is not feasible"*; and *"… must be risk based, no one-size-fits-all approach works…"*

Thus, the CEN-study conclusion is that a risk based approach is recommended, instead of a "level playing field" approach. It means that one should avoid any SCS standard which would automatically lead to identical implementation of SCS requirements, even where they were dealing with different threats and/or vulnerabilities between various supply chains (i.e, different geographies, industry sectors, transport modes etc.). However, with some aspects of SCS standards there may be a minimum requirement level on how to implement them.

Q10. Does a SCS standard have a primary focus on incident prevention or post-incident recovery?

This question was partially dealt in the CEN-study by analyzing five existing SCS standards on security requirements (or security check lists). This analysis provided a profile of the current programs, to which extent they address prevention, detection and recovery aspects of security management in supply chains.[8] Prevention turned out to be the most popular aspect in the existing SCS standards, followed by detection and recovery aspects, both covered in a fairly equal manner.

As the outcome of the whole CEN-study, no categorical recommendations are made towards one security phase over the other. Depending on the individual standard recommendations, some of them focus more on prevention aspects, while some of them cover all security phases.

Q11. Is the basic nature of a SCS standard reflective of an overall management system or a targeted norm?

The CEN-study recommends focusing on SCS standards aiming to solve specific issues regarding crime in supply chains—instead of developing a generic management standard (cases of which exist already, e.g. ISO28000 series); or a 'another security check list'-type standard. However, it would be useful if the specific standards were linked into a broader management system, in order to avoid too scattered a landscape of standalone SCS norms—again to be addressed on a case-by-case basis.

Q12. Do government agencies provide tangible benefits attached to a SCS standard?

As discussed before, governmental agencies (mainly customs) may be in the position to provide tangible benefits for companies which comply with one or more SCS standards, particularly with those originating from customs. Such benefits can consist of lower risk scores for the compliant companies, with less documentary and/or physical inspections, and of licenses to operate under high threat or post-incident situations.

As the CEN-study's main focus is on intra-EU security issues, the cross-border related benefits form a lower priority; however, in some of (sub)standards governmental recognition could lead to tangible benefits for business, for example during the high threat / post-incident situations.

[8] The detailed outcome of the CEN-study SCS standards in-depth analysis will be published as a separate journal paper.

Q13. Does a SCS standard have more than one certification level in place?

Thinking of the single SCS label versus multi SCS label-systems, the CEN-study does not make actual recommendations in one direction or another. It can make sense to start with a single label system, but nothing prevents adding later one or more new levels in the overall SCS standards system—assuming this would be perceived as beneficial by the business community (for example with recognition by a government agency).

Q14. Is a SCS standard financed by public entities or by private entities?

This important question about financing of SCS was outside the scope of the CEN-study. However, the assumption is that the cost of the type of SCS standard explored and developed in the study would normally fall to the private sector to cover.

Figure 2 below visualizes the recommendations made in the CEN-study, in relation to the SCS standards framework and its' 14 dimensions, with following shape and color symbols:

- Big red circle = main recommendation in the CEN-study
- Small red circle = consider a link with this, whenever feasible
- Blue square = the CEN-study does not differentiate between the two options
- Green star = the study finds these as positive objectives, but did not cover in detail
- Question mark = the CEN-study does not cover this dimension

Conclusions, discussions and topics for future research

The intent of this paper has been to develop a framework for supply chain security (SCS) standard analysis and design, primarily targeted for governmental policy makers and private sector supply chain, security and standardization specialists. The baseline assumption is that no "super-standards" exist, capable of tackling all SCS aspects in adequate detail, and in a cost-efficient manner; therefore there is a need to focus on a limited set of aspects while designing and implementing new SCS standards. The framework was first derived from academic and practitioner SCS literature and then tested in a real life SCS standardization feasibility study project. The theoretical framework consisted of 14 questions (i.e. "14 dimensions"), initially with two optional answers each. During testing of the framework as part of the CEN-study several observations regarding interdependencies, mutual exclusivities, requirements for balancing, easy-to-say/difficult-to-do-aspects, and a few other points were made, which are explained below.

First, looking at the interdependencies between the 14 dimensions of the framework (see Figure 2 above), the broadest linking is most likely when the public sector is the originating actor and the driver for the standard development (Q2). Being that this is more often a customs authority in the post-2001 SCS era, links would frequently include the following: an anti-terrorism focus (Q1), local/regional coverage (Q5), a cross-border trade focus (Q6), mutual recognitions with other customs SCS programs preferred (Q7), customs conducting the verifications (Q8), and tangible government benefits promised (Q12). Other interdependencies may also

exist, e.g. SCS standards with global coverage (Q5) could have the tendency towards SCS management systems (Q11), instead of focused norms—these and other possible interdependencies remain a topic for future research.

Second, very few of the 14 dimensions contain two mutually exclusive basic options, just the following three: mutual versus no mutual recognitions (Q7), tangible government granted benefits or no benefits (Q12) and single certification level system versus multi-level certification system (Q13). The other 11 dimensions normally require a balancing approach between the two extreme options. For example Q3 can imply that logistics operators become the primary user group for a new SCS standard, while shippers have only a limited set of requirements relevant for them in that standard. Another example, Q10 can lead to a standard where 75% of the security measures have a prevention focus, and 25% a recovery focus. A third example is Q14, where careful research and analysis can lead into a recommendation of joint financing between the public and private entities regarding certain aspects of a new SCS standard.

Third, some of the dimensions and the options of the framework may be very complicated to execute in real life—i.e. "easy to say, (very) difficult to do". One potential example is with Q9, the option to go for risk assessment based SCS standard, instead of a level playing field-type of approach. The immediate questions raised include: who has the capabilities to carry out highly professional, objective and non-biased threat, vulnerability, risk likelihood and risk consequence analysis? How is the outcome of such analysis reflected in the practical security requirements of a specific SCS standard, with a specific supply chain and company? These and other questions require deep expertise from the standard development and verification teams in order to come up with feasible, security-efficient and cost-efficient approaches.

Fourth, one should also consider emerging sub-issues under any of the 14 dimensions. For example if a new SCS standard is driven by the private sector (Q2), then one should agree early on, whether the standard design and development is driven by the supply chain operators (e.g. shippers, logistics service providers, wholesalers etc., i.e. "users of SCS"), or whether the development should be driven by security service and/or technology companies. Here the latter group of actors might be in possession of the very latest and privileged knowledge on SCS issues and available solutions, but it might also be in a biased position to promote "expensive SCS measures", "dooms day threat scenarios" etc. Another question requiring deeper drilling is the one of financing SCS costs (Q14): if the private sector becomes the main financing party, one should clarify how the costs are to be shared between the various actors, in particular providers versus users of transportation services.

Additional topics requiring further research include the following:

- Which security measures are efficient (and cost-efficient) in both anti-terrorism and anti-crime work?
- How do security measures differ in the fight against different types of crimes, including theft, goods smuggling, and human trafficking?
- How would an optimized public–private-partnership scheme (security focus, legal aspects, trust between the parties, verifications, government granted

benefits, cost sharing etc.) look like as regards aspects of the SCS standard design, implementation and verification?
- Is it feasible (legally, technically, economically etc.) to match different SCS certification levels with different (governmental) threat levels?
- What kind of role "secure trade lane platforms", such as European Framework Program 7 (FP7) project INTEGRITY[9] could play in the future of SCS standardization?

As the final recommendation, the author of this paper suggests that all interested governmental, business and academic parties test out the framework regarding their own SCS standardization interests, and report back any findings, including any possible gaps and shortcomings with the framework presented in this paper.

Acknowledgements The author expresses his gratitude in relation to the development of this paper to the following individuals: Professor Ari-Pekka Hameri (Faculté des Hautes Etudes Commerciales, HEC, of University of Lausanne), Professor Matthias Finger (Ecole Polytechnique Fédérale de Lausanne, EPFL), Professor Jan Holmström (Helsinki University of Technology, HUT), PhD-student Juha Ahokas (HUT), Researcher Toni Männistö (HUT), Researcher Jukka Sahlstedt (HUT), Mr. Roeland van Bockel (Dutch Transport Administration), Mr. Arthur Carlebur (Netherlands Standardization Institute, NEN), Mr. Peter Cullum (UK Road Haulage Association, RHA), Mr. Roger Warwick (Italian Organization for Standardization, UNI), Mr. Philippe Bonnevie (The French Shippers Council, AUTF), Mr. Marcus Gersinske (Association of German Transport Companies, VDV), Dr. Andrew Traill (European Shippers Council, ESC), Mr. Bryce Blegen (Trusted Trade Alliance, USA), Dr. Michael Wolffgang (University of Muenster, Germany), Mr. Lars Karlsson (World Customs Organization, WCO, Belgium), Mr. Allen Bruford (WCO), Ms. Carol West (Private Sector Consultative Group, PSCG, to WCO), Mr. Malcolm McKinnon (SITPRO, UK), Ms. Mayra Hernandez (Business Alliance for Secure Commerce, BASC, Colombia), Mr. Dietmar Jost (Booz, Germany), Ms. Susanne Aigner (European Commission DG TAXUD), Mr. Wolfgang Elsner (European Commission DG TREN), Dr. Olena Pavlenko (The Ukrainian Academy of Customs), Ms. Tatyana Chika (The Ukrainian Academy of Customs) and Ms. Kseniia Kashcheieva (The Ukrainian Academy of Customs). Regarding the funding of the research and writing work, the author acknowledges the following parties: The European Committee for Standardization (CEN); Swiss Science Foundation (SNF), Framework Program 7 project INTEGRITY; and Helsinki University of Technology, Business, Innovation, Technology research center (HUT BIT).

References

Bichou K (2008) Maritime security and risk-based models: review and critical analysis. Discussion paper prepared for the OECD/ITF Round Table of 11–12 December 2008 on Security, Risk Perception and Cost-Benefit Analysis

Burkhardt M (2009) COUNTERACT and INSECTT: pragmatic approaches to enhancing security. Inland Transport Security seminar, Geneva, 15 January

Closs D, McGarrell E (2004) Enhancing security throughout the supply chain. Special report series, IBM Center for The Business of Government, available at: www.businessofgovernment.org

Closs D, Speier C, Whipple J, Voss M (2008) A framework for protecting your supply chain. Supply Chain Manag Rev 12(2):38–45

Deming W (1991) Out of the crisis. MIT, 507 pages. ISBN 0911379010

Diop A, Hartman D, Rexrode D (2007) Customs-trade partnership against terrorism: cost/benefit survey. Report prepared for U.S. Customs and Border Protection. University of Virginia

Donner M, Kruk C (2009) Supply chain security guide. Published by World Bank. http://siteresources.worldbank.org/INTPRAL/Resources/SCS_Guide_Final.pdf. Accessed 14 December 2009

[9] http://www.integrity-supplychain.eu/.

ECMT, European Conference of Ministers of Transport and OECD Maritime transport Committee Secretariats (2005), Container transport security across modes. Task Force in Security and Terrorism in Transport
Edmonson R (2005) Supply chain security, European style. J Commer, October 17
Eggers W (2004) Prospering in the secure economy. Deloitte research study, Deloitte Touche Tohmatsu, New York, NY, available at: www.deloitte.com
Grainger A (2007) Supply chain security: adding to a complex operational and institutional environment. World Customs Journal 1(2), September
Gutierrez X, Hintsa J (2006) Voluntary supply chain security programs: a systematic comparison. ILS 2006. The International Conference on Information Systems, Logistics and Supply Chain, Lyon, France, May 15–17
Gutierrez X, Hintsa J, Wieser P, Hameri A-P (2007) Voluntary supply chain security program impacts: an empirical study with BASC member companies. World Customs Journal 1(2), September
Hameri A-P, Hintsa J (2009) Assessing the drivers of change for cross-border supply chains. Int J Phys Distrib Logist 39(9):741–761
Helferich O, Cook R (2002) Securing the supply chain. White paper prepared for Council of Logistics Management. United States of America: 1–39
Hintsa J, Hameri A-P (2009) Security programs as part of efficient supply chain management. Supply Chain Forum: An International Journal 10(2)
Hintsa J, Wieser P, Gutierrez X, Hameri A-P (2009) Supply chain security management: an overview. IJLSM 5(3–4):344–355
Hintsa J, Ahokas J, Männistö T, Sahlstedt J (2010) Feasibility study on European supply chain security standards. The European Committee for Standardization (CEN)/TC 379 (forthcoming)
Kommerskollegium (2008) Supply chain security initiatives a trade facilitation perspective. Report is prepared for the Government of Sweden by the administrative body dealing with foreign trade and trade policy
Kwek K, Goswami N (2003) Cost and productivity implications of increased security in sea trade processes. Research paper, The Logistics Institute—Asia Pacific National University of Singapore
Lake J, Robinson W, Seghetti L (2005) Border and transportation security: the complexity of the challenge. Congressional research service report for Congress
Lee H, Wolfe M (2009) Supply chain security without tears. Supply Chain Management Review January/February: 12–20
Liem K (2009) The European security research programme. Inland Transport Security seminar, Geneva, 15 January
Miller M (2009) Supply chain security—practical experience. Inland Transport Security seminar, Geneva, 15 January
Peleg-Gillai B, Bhat G, Sept L (2006) Innovators in supply chain security: better security drives business value. Report, The Manufacturing Institute
Rice J, Caniato F (2003) Building a secure and resilient supply network. Supply Chain Manag Rev 7 (5):22–30
Rice J, Spayd P (2005) Investing in supply chain security: collateral benefits. IBM Center for the Business Government, May 2005: 1–30
Rucinski A (2009) Globally integrated security environment. Inland Transport Security seminar, Geneva, 15 January
Russell D, Saldanha J (2003) Five trends of security: aware logistics and supply chain operation. Transp J 42(4):44–54
Sarathy R (2006) Security and the global supply chain. Transp J 45(4):28–50
Sheu C, Lee L, Niehoff B (2006) A voluntary logistics security program and international supply chain partnership. Supply Chain Management: An International Journal 11(4):363–374
Skinner B, Kelly E, Tenney W (2008) Global supply chain security. NFR 2008 Loss Prevention Conference. Orlando, Florida, June 23–25
Solnik G (2009) Freight security standards, trucking security requirements, incident reporting. Inland Transport Security seminar, Geneva, 15 January
Thibault M, Brooks MR, Button KJ (2006) The response of the US maritime industry to the new container security initiatives. Transp J 45(1):5–15
UIRR (2007) UIRR risk analysis guidelines for combined transport terminals. International Union of Combined Road-Rail transport companies
WCO (2008) Customs in the 21st century—enhancing growth and development through trade facilitation and border security. Paper prepared for the WCO Council meeting

White C, Erera A, Savelsbergh M (2004) A research agenda for supply chain security and productivity. Working paper, School of Industrial and Systems Engineering, Georgia Institute of Technology
Williams Z, Lueg J, LeMay S (2008) Supply chain security: an overview and research agenda. IJLM 19 (2):254–281
Willis HH, Ortiz DS (2004) Evaluating the security of the global containerized supply chain. RAND Corporation
Wright G (2009) Progress on the mutual recognition agreement between the EU and US and business continuity planning in the EU. Inland Transport Security seminar, Geneva, 15 January
Wright PD, Liberatore MJ, Nydick RL (2006) A survey of operations research models and applications in Homeland Security. INTERFACES 36(6):514–529