CEN Supply Chain Security (SCS) Feasibility study

CEN/TC 379 Supply Chain Security

Final report

15.1.2010

Hintsa J., Ahokas J., Männistö T., Sahlstedt J.

Cross-border Research Association,

Lausanne, Switzerland

EXECUTIVE SUMMARY

This report presents the outcomes of a feasibility study on supply chain operator needs for a possible European standard in supply chain security (SCS). The study was commissioned by the European Committee for Standardization, CEN, and funded by European Commission Directorate-General Energy and Transport, DG TREN. The study was carried out by four researchers at a Lausanne, Switzerland, based research institute, Cross-border Research Association, CBRA. **The study process consisted of the following steps**:

(i) Literature review, where a large number of relevant publications were covered;
(ii) Expert interviews, with 21 experts in supply chain, security and/or standardization;
(iii) In-depth analysis of standards, covering four existing SCS standards and one regulation; and
(iv) Operator survey, where 86 European supply chain operators shared their views on various SCS aspects, including the feasibility of a set of standard ideas, derived from the expert interviews.

SCS is often considered to be a combination of crime prevention, security engineering, risk management, and operations management disciplines, i.e. part of social and engineering sciences. However, this study **explores SCS in a broader context**, covering some political and emotional factors, hypes and myths, some misconceptions and unrealistic expectations, and the interpretation of different schools of thought concerning priorities and most cost efficient ways to combat crime in supply chains. This study reveals relevant knowns and some unknowns about designing and implementing security in supply chains, including several concerns and complexities related to the development of SCS standards in Europe (and internationally). Aspects of anti-terrorism measures are considered and integrated into this study. Based on the outcome of the expert interviews, the research in particular focused on exploring the impact of crime (and terrorism) on European supply chains, and whether one or more new standards could help to mitigate such risks in a cost efficient manner.

In line with the mandate given, this study makes the following **three main recommendations** regarding the future of SCS standardization in Europe:

1. Develop a **CEN standard for crime incident reporting** in Europe. This standard can be exploited to harmonize the interaction between business and relevant authorities throughout Europe, in particular for reporting of crime incidents; and to streamline and speed up the process of collecting and sharing data on crime incidents, for the benefit of both supply chain operators and authorities.
2. Develop a **good practice guidebook on SCS**, sharing experiences between supply chain operators as to which security measures work (in which contexts), about the costs and benefits, and other relevant parameters, to be exploited in SCS design, implementation, monitoring and training.
3. Carry out a set of **detailed cost benefit case studies**. These focus on a **holistic SCS label**, targeted primarily for European small and medium sized enterprises (SMEs) in the logistics sector, especially for companies which are not eligible for customs SCS programs (like EU AEO). Based on the outcomes of 20-30 case studies, this additional study suggests the final decision as to whether a SCS label type of standard will or will not work.

Finally, the study presents a holistic SCS framework to be exploited in any future SCS standardization projects. This is concluded with **an emerging theory of ”Value Chain Security” (VCS)** which takes into consideration several broader and deeper aspects of real crime prevention and security management: the proposed **CEN standard for crime incident reporting** provides the first tangible building block towards the future VCS management - as part of the continuous fight against the ”dark side of supply chains”.

Foreword

Fast and reliable supply chains are crucial for today´s society and economy – "swift, even flow" being one of the key underlying theories for competitive supply chain management. Any type of disruptions or even abnormal variations in supply chain systems – in sourcing, transport, warehousing, production, distribution, data management etc. – can cause major costs to supply chain operators, in terms of extra administration, shipment replacement and expedited shipments, lost sales and lost customers etc. Crime in it´s various forms is not a new phenomenon as a source of disruptions in supply chains – there being a long history of sea piracy, and road and rail bandits, to mentin just a few obvious examples. Today, many additional forms of crime take place in supply chain systems, including violations of fiscal and non-fiscal customs regulations, intellectual property right violations, and human trafficking. Besides the direct cost of lost or damaged assets related to supply chain crime incidents, companies have to cover costs for supply chain disruptions, for higher insurance premiums, and for lost brand recognitition, amongst other possible costs. Regarding the risk of terrorism in global supply chains, the cost implications can also be twofold: first, the cost related directly to an attack and immediate recovery, and second, the costs related to getting the whole supply chain system back to normal: many experts anticipate the latter could be much higher than the former.

Before year 2001, supply chain security, SCS, was a prime concern of supply chain operators: manufacturers, shippers, warehouse keepers, freight forwarders, carriers, distributors and retail companies were designing and deciding on their own SCS measures fairly independently. After the terrorist attacks in 2001, and despite the attacks using domestic passenger transport, governments started to introduce a broad set of SCS programs and regulations consisting of advance cargo data requirements, non-intrusive inspections, physical security measures, operator certifications etc., to mitigate the risk of terrorism in supply chain systems, bringing possibly for the first time SCS standardization issues centre stage. It became a regular topic of debate between the public and private sectors as to the extent government designed and enforced SCS initiatives would really make sense in protecting our societies.

This SCS standardization feasibility study explores the needs for any further standardization and constraints on European supply chain operators to enhancing security in supply chains. The authors hope that they have been able to carry out an objective study on the topic, and have come up with the most pertenant findings, conclusions and recommendations. It is hoped also that this study can be used as a stepping stone for further insights to be made into SCS and to establish the EU at the forefront of developments in this field.

The authors wish to thank all parties which contributed to the study, institutions, stakeholder organisation and representatives which filled out the questionnaires. Without their help this study would not have been executed.

Any comments or questions regarding the report, please send us an email to: juha@cross-border.org

In Lausanne, 15.1.2010

CBRA Research team

Acknowledgements

Cross-border Research Association, CBRA, research team would like to first thank European Committee for Standardization, CEN, for granting the feasibility study contract, and European Commission Directorate-General Energy and Transport, DG TREN, for providing the funding for the study.

Second, we express our gratitude to the individuals, associations and companies providing the data for the study: 21 experts for the interviews, and 86 companies for the operator survey.

Third, CBRA team wants to thank following individuals for their inputs throughout the study process: Mr. Roeland van Bockel (Dutch Transport Administration), Mr. Arthur Carlebur (Netherlands Standardization Institute, NEN), Ms. Magda Noekee (Netherlands Standardization Institute, NEN), Ms. Maitane Olabarria (European Committee for Standardization, CEN), 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, Belgium), 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) and Mr. Wolfgang Elsner (European Commission DG TREN).

Fourth, we express our gratitude to our following three “home universities”, and their three Professors: Professor Ari-Pekka Hameri (Faculté des Hautes Etudes Commerciales, HEC, of University of Lausanne), Professor Matthias Finger (Ecole Polytechnique Fédérale de Lausanne, EPFL), and Professor Jan Holmström (Aalto University School of Science and Technology, former Helsinki University of Technology, Finland).

And fifth, CBRA team thanks the Ukrainian Academy of Customs, their Principal and following three individuals for good collaboration during the study: Dr. Olena Pavlenko, Ms. Tatyana Chika and Ms. Kseniia Kashcheieva.

Table of contents

List of figures

List of boxes

List of tables

1 Introduction

This opening chapter provides a framework for the whole supply chain security (SCS) feasibility study. Besides explaining the research questions, methodology, and study structure and flow, it provides some insights into the essence of SCS, including complexities and unknowns surrounding the topic; it explains some of the aspects of SCS interplay between a broad variety of parties; some philosophies regarding standardization; and finally, some limitations of the study. The format of the chapter is "question and answer", with a total of sixteen questions being answered in order to provide the reader with a sufficient background frame for the study.

Q1: What is supply chain security (SCS) all about?

A: A number of definitions for SCS exist in the literature, one by Closs et al. (2004)[1], and another by Hintsa et al (2009). In layman terminology, SCS aims at reducing the frequency and seriousness of the consequences of any crime- (and terrorism-) related incidents in supply chains, both from the point of view of a single actor, as well as that of a network of actors. This SCS aim can be reached via a variety of organizational, procedural and technological approaches. A particular company should invest in SCS management at a level that minimizes the total cost of security compliance, considering all prevention and recovery related costs. Since the terrorist attacks in 2001, governments are playing a big role in the overall management scheme of SCS by bringing into force policies, regulations, voluntary programs and enforcement agencies.[2]

Q2: What is the scope of SCS, in terms of crime types and security areas covered?

A: This is an evolving topic, and different schools of thought exist. Regarding crime types, businesses often focus on theft issues, while governments may consider terrorism as a more serious concern. Other typical concerns include intellectual property violations; violations of customs regulations; and illegal immigration. Security responses can be designed and implemented in a variety of ways, depending on the threats and vulnerabilities relevant for the supply chain in question. Security areas such as facility security, cargo security, human resource security, IT security and business network security each involve at least a dozen if not dozens of different security enhancement measures, either for crime prevention, detection/reaction and/or recovery purposes.

Q3: What is the history of supply chain crime?

A: Crime in supply chains – including sea piracy, smuggling, cargo theft and hijacking – has a long history, having existed from the early days of trade and transport. Some of the historically oldest forms of crime, such as sea piracy, have always been in governments' interest to combat, while protection against others, like theft, has primarily been solely the interest of businesses. The globalization of manufacturing, trade and logistics has broadened the scope of crime risks in supply chains, and many of them, including counterfeit products and other intellectual property violations, have become a truly joint concern of governments and businesses. However, only after the terrorist attacks in 2001 did governments worldwide step in to play a major role in SCS management by introducing a variety of SCS policies, regulations and voluntary programs.

[1] Closs et al (2004) define SCS as "Supply chain security management is the application of policies, procedures, and technology to protect supply chain assets (product, facilities, equipment, information, and personnel) from theft, damage, or terrorism, and to prevent the introduction of unauthorized contraband, people, or weapons of mass destruction into the supply chain."

[2] Many of the details in this answer to question Q1 will be covered in proper detail in the upcoming chapters – same goes with most of the 15 other questions.

Q4: Who are the main parties involved in the SCS interplay?

A: It goes without saying that the three main parties – businesses, governments and criminals – each have their own agendas and conflicting interests when it comes SCS policies, standards, single measures – and how to get around them: (i) businesses aiming to protect their assets and their reputation with cost-efficient security measures; (ii) governments aiming to protect the society and citizens against any harm or wrong-doing; and (iii) criminals aiming to maximize their profits, in terms of financial and/or publicity outcomes, while minimizing the risks of legal punishments. Limiting the discussion to business versus governmental interests, the former often sees the latter as introducing SCS requirements which are too costly in relation to the tangible benefits gained. Looking at the interplay of SCS between various business parties – manufacturers/shippers, trade/retail, logistics providers, SCS services and solutions, and the insurance sector – the question of costs and finance can become ever more complex.

Q5: What makes the SCS interplay between the various business actors complex?

A: Defining and agreeing what should be the ”right level” of SCS for various types of products moving around in logistics chains, understanding the real cost of security measures and activities, and agreeing on ”fair payment and financing principles” between the various actors are complex issues. Manufacturers and shippers, especially with high value and highly security-sensitive goods, may require their logistics service providers to invest in better security without being willing to pay premium for it. Global logistics companies may require their local small and medium size subcontractors to comply with new SCS programs, again without paying extra for it. SCS service and technology companies may be confusing the situation with offerings of new ”must-have” security solutions. All this may become quite confusing for example for a SME logistics company working on a local basis.

Q6: Why are objective analysis and design of SCS initiatives and measures difficult tasks to carry out?

A: It appears that many aspects of SCS knowledge such as security measure efficiency per crime type, costs and benefits of SCS initiatives, crime incident statistics and crime indicators, amongst others, are not well known by governmental policy makers nor by supply chain or by security managers. This is highly understandable, due to the nature of the “beast”: (i) measuring security efficiencies, costs and benefits is complex; and (ii) a large proportion of crime incidents go unreported – criminals do not write reports (or at least ones shared with a broader community) and companies hurt by crime typically want to minimize publicity. This all makes the ´optimum design´ of SCS programs difficult – like designing a quality management program without accurate failure rates and proper incident statistics, and without being able to measure how a new procedural investment improves the quality outcomes, etc. Furthermore, the ‘enemy’ of SCS is much more a moving target or dynamic phenomenon than that of quality management – criminal actors tend to learn about new security measures, instantly trying to find ways around them, or to move to new more accessible targets.

Q7: Why is working with SCS design and implementation not always well recognized?

A: The answer is quite straightforward: it is usually difficult to know whether the decrease in security incidents and damages (assuming they can be objectively measured in the first place) is thanks to a particular SCS investment or simply happens because the criminals shifted their focus to a more lucrative target or crime type. Especially if actual incidents are rare, it can even be questioned why problems that “didn’t exist” have to be fixed. This can especially be the case with regard to anti-terrorism SCS initiatives.

Indeed, when the ultimate success is that "nothing happened", it can certainly be a challenge to recognize the high achievers in the field of SCS management.

Q8: What is characteristic for existing SCS academic and practitioner publications?

A: In general terms, the current SCS literature is characterized by the existence of theoretical and conceptual studies on the academic side, and SCS initiative and solution descriptions on the practitioner side. There appears to be a lack of real empirical data on the efficiencies, benefits and costs of security measures and initiatives. This is understandable due to difficulties in accessing (sensitive) data, complexities of measurement, etc. Furthermore, the actual functioning and real dynamics underlying SCS management systems have until now been poorly covered by both academics and practitioners.

Q9: What are standards?

A standard is 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 to 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 of objections until a general agreement can be observed.

Q10: What is CEN doing regarding standardization?

CEN develops different kinds of documents for specific purposes: European Standards (ENs), Technical Specifications (TS), Technical Reports (TR) and CEN Workshop agreements (CVA). European Standards (EN) must be adopted as identical national standards and withdraw any conflicting national standards by National Standardization Bodies (NSBs). Technical specifications (TS) can be produced when there is no immediate need or not enough consensus for ENs, or where technology is not mature enough and the subject matter is still under technical development. Technical reports (TR) are documents containing informative material such as data from a survey, state of the art on a particular subject, information on work in other organizations. CEN Workshop agreements (CWA) can be drafted by CEN Workshops, which are open to any interested party. They enable the rapid exploitation of research results.

Q11: What are the questions this study aims to answer?

A: This is an empirical study, using data primarily from interviews, standards analysis and a survey, about business needs and constraints regarding a possible new CEN standard (or a set of standards) to enhance supply chain security (SCS) in Europe. In particular, this study aims to answer the following questions:

- Is crime an issue for supply chain operators in Europe?
- Are there any obvious gaps regarding existing SCS initiatives vs. crime issues in Europe?
- Can one or more possible new SCS standard(s) help to solve or reduce crime problems in Europe?
- What would be the high level content for a possible SCS standard (or a set of standards) in Europe[3]

Q12: Why is cost quantification not included in the study questions?

A: Quantification of costs of a possible new SCS standard (or a set of standards) cannot be carried out in this feasibility study, due to the fact that the scope (or content) of the possible new standard(s) has not been given. The research should first discover what type of (tangible) standard needs might exist in Europe. Once the scope is known, including possible cost components of a possible new standard, a sufficient

[3] Note: this feasibility study does not aim to design new standards in detail.

number of case companies must be examined to gain an understanding what an average company must do in order to reach the security level proposed in the possible standard. Thus, cost quantifications can only be done after this study.

Q13: Who is the primary audience and source of requirements and constraints for this feasibility study?

A: As discussed before, SCS is a ”3-party game” between business, government and criminal actors – without criminals, no crime to fight against, without governmental actors, no regulations, voluntary programs, and security inspections to prepare for, and without businesses, nothing to regulate for, and no crimes (in the supply chain) to carry out. This feasibility study, however, focuses on a sub-set of these actors – on security needs and constraints of supply chain operators, i.e. the companies directly involved in owning and moving the goods, illustrated with numbers 3, 4 and 5 in the Figure 1 below.

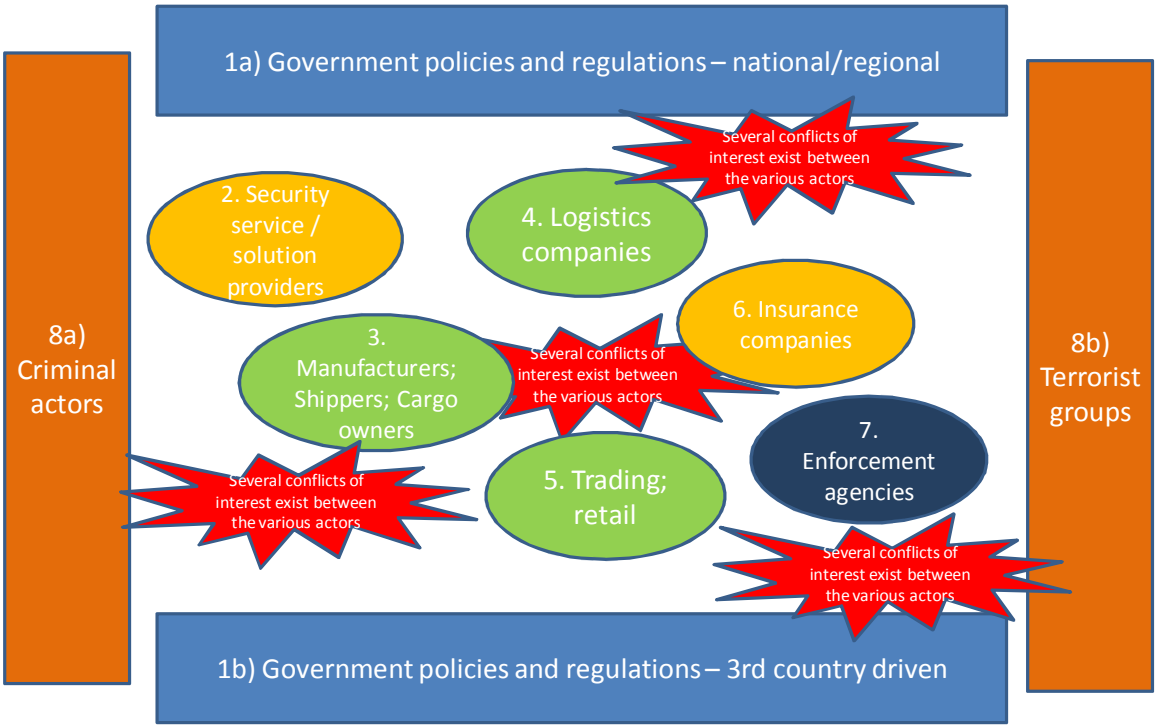

Figure 1 SCS interplay – high-level illustration of the main parties involved.

More specifically, this study covers the various illustrated ´eight SCS actors´ in the following way:

- Groups 3, 4 and 5 participate in all steps of the study, being the primary source on information via the expert interviews and operator survey for the whole study.
- Group 2 has a limited participation in the study, with some representation in the expert interviews.
- Group 6 has no actual representation in this study.
- Materials produced and/or enforced by groups 1a, 1b and 7 are considered as a source of information during the study process.
- Groups 8a and 8b are covered only via literature findings and perceptions shared by Groups 3, 4 and 5.

Q14: Which type of methodology is used in this study?

A: The methodology for this feasibility study has the following five steps:

1. Reviewing literature to reach an up-to-date view of the main components, dynamics and constraints of supply chain security management.
2. Interviewing a set of experts who represent the interests of European supply chain operators, regarding either security issues and/or standardization issues.
3. Analyzing a set of most relevant SCS initiatives in detail, as a desk exercise, in order to identify any possible gaps in security coverage, priorities, dynamics etc.
4. Surveying supply chain operators around Europe, representing different industrial sectors and company sizes.
5. Combining, structuring and prioritizing all the study outcomes, into final conclusions and recommendations regarding possible new SCS standards in Europe.

Q15: What is the structure and the flow of this report?

A: Following the study methodology description in the previous question, the structure and the flow of this report, including the links between the various chapters, is illustrated in Figure 2 below.

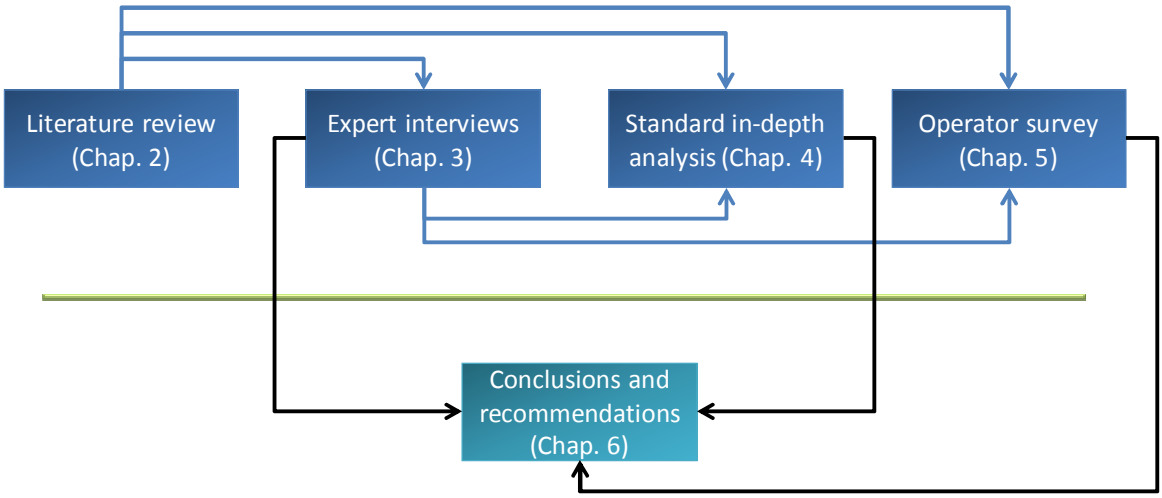

Figure 2 Report structure and links between various chapters

Q16: What are the study limitations and what remains out-of-scope for this study?

A: This project has a challenging goal to study the feasibility of a possible (one or more) SCS standard in Europe, while the scope of the possible standard is not fixed up front. In order to reach this goal, i.e. to study the feasibility and the content of possible standards in parallel, the following interesting aspects remain out of scope of the study: (i) any type of cost and benefit quantifications for any possible new SCS standards; (ii) process descriptions for any type of certification, auditing and/or monitoring schemes; and (iii) detailed analysis of the role of the insurance sector in relation to SCS standards. Limitations of the study include the fact that the main data sources for the study – i.e. the experts interviewed and the operators surveyed – contain a bias towards parties who chose to be pro-active. Thus they do not necessarily reflect the views of an 'average' European supply chain operator.

2 Literature review

2.1 Introduction

The goal of this chapter is to provide the reader with a set of findings in the literature, supporting the further development of this feasibility study, consisting of Expert interviews (Chapter 3), SCS initiative in-depth analysis (Chapter 4) and Operator survey (Chapter 5). We start by framing the study inside supply chain risk management (Chapter 2.2); followed by pointing out a set of typical vulnerabilities in supply chains / networks (Chapter 2.3). Next we look specifically at various crime risks in supply chains, both with a narrow practitioner view as well as with a broader academic view (Chapter 2.4); followed by a theoretical views on situational crime prevention (Chapter 2.5). Then, security approaches, measures and activities and SCS programs, standards, regulations (Chapter 2.6) are briefly reviewed. Next, examples of costs and benefit components of SCS are identified, followed by a basic illustration of total cost of SCS compliance – optimization (Chapter 2.7). Finally, some conclusions from the literature are drawn, and brought forward to the rest of the study (Chapter 2.8).

2.2 Risk management

Risk is often described as a measure of the probability and severity of adverse effects (Lowrance, 1980). Risk can be perceived in terms of the likelihood of an uncertain event or set of circumstances occurring which would have an adverse effect on the achievement of a project's objectives (Simon, P., Hillson, D. and Newland, K., 1997). Other authors stress that the perception of risk is interests group and context-depended (Moore, 1983):

> *. . . when terms like high risk or low risk are used, the meaning commonly depends on the starting asset base and the consequences that the occurrence of the risk would have for the asset base of the individual or organization concerned.*

Industrial corporations define supply chain risk for example in the following way:

> *Supply chain risk is any threat of an event that might disrupt normal flows of materials or stop things happening as planned (Waters, 2009).*

The definition encompass all supply chain glitches: parts shortages, production problems, ramp-up and roll-out problems, quality and testing problems, order changes by customer, development and engineering changes. Incidents and glitches can have impact on operational environment. They can decrease production and transportation capacity or the number of qualified suppliers, thus they increase uncertainty of supply, deliver and lead time. These changes are systematic and continuously monitored by the management in industrial supply chains (Zsidisin, 2003).

Accidents and intentional acts designed to cause harm or damage are part of the reasons for supply chain disruptions. The supply chain is a value chain, where the loss of final products destroys the possibility to pursue profit – property insurances cover only invested capital in products before the damage, but not anticipated business earnings or market share.

Stock markets severely penalizes firms that experience disruptions irrespective of which link in the supply chain is responsible for them (Hendricks, K.B. and Singhal, V.R., 2005). According Hendricks and Singhal an abnormal decrease in shareholder value should provide an incentive for various links in the supply chain to collaborate and co-operate to minimize disruptions in supply chains.

Government authorities emphasize the role of taxation, public health and environment when defining the supply chain risk. European Commission DG TAXUD defines: *"Risk" means the likelihood of an event occurring, in connection with the entry, exit, transit, transfer and end-use of goods moved between the customs territory of the Community and third countries and the presence of goods that do not have Community status, which prevents the correct application of Community or national measures, or compromises the financial interests of the Community and its Member States, or poses a threat to the Community's security and safety, to public health, to the environment or to consumers.*[4]

Different risk perception may have an impact on preferred security measures of supply chain operators; approach to risk reduction may be situation-dependent (Mitchell, 1995). Industrial supply chain operators may prefer supply chain planning and design as a security measure aiming at possible collateral benefits. Other operators may want to limit supply chain security measures to protection of their facilities. In addition, attempting to develop a risk assessment tool that can be used by managers in their own situation is very difficult (Harland, C., Brenchley, R. and Walker, H., 2003). One reason for this could be that little work has been done to relate risk-reduction strategies to the situations in which they are most effective (Mitchell, 1995). Additionally, there are a wide range of tools and techniques for managing risk, but they do not appear to have been adapted for use in managing supply chain risk (O. Khan and B. Burnes, 2007). In spite of a different emphasis and viewpoints relating to supply chain risk secure and predictable supply chain contribute interests of all stakeholders.

Networks of supply chains are vulnerable in front of a multitude of threats, hazards and catastrophes, which can be divided in three categories (Kesting, 2007):

- Natural threats, hazards and catastrophes
- Man-made threats, hazards and catastrophes
- Criminal activities and terrorism.[5]

Natural threats, hazards and catastrophes are caused by natural forces. These include flooding, storms, earthquakes, tidal waves, drought/bushfire/heat, cold/frost, hail or avalanches. The extent of the damage depends not only on the strength of the natural force. Both technical and organizational measures can help limit the consequences. The overall damage from a natural catastrophe always has a social dimension (Kesting, 2007).

[4] REGULATION (EC) No 648/2005 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 13 April 2005 amending Council Regulation (EEC) No 2913/92 establishing the Community Customs Code.

[5] This feasibility study naturally focuses on this last mentioned supply chain risk type, i.e. criminal activities and terrorism; simultaneously recognizing, that for supply chain managers this falls within the frame of supply chain risk management.

Man-made threats, hazards and catastrophes are events that are closely associated with human activity. Most of the time these involve a large object in a confined space. The category can include large fires, explosions, air crashes, or mine disasters. These can have very large impacts on supply chains.

Criminal activities and terrorism are a special category of risk. They are not due to chance but a result of premeditated human action. The probability of terrorist act cannot be assessed using the usual insurance processes (Kesting, 2007). This makes risk management in supply chains a challenging task.

2.3 Points of vulnerability in supply chains

Many factors in modern supply chains – the length of the (global) supply chains; the high number of actors involved; and dependencies between companies' business activities; amongst others – create vulnerabilities, of which some are there for criminals to exploit. Figure 3 below summarizes the various points of vulnerability in the supply chain, detailed with a set of concerns and security countermeasures (Sarathy, 2006):

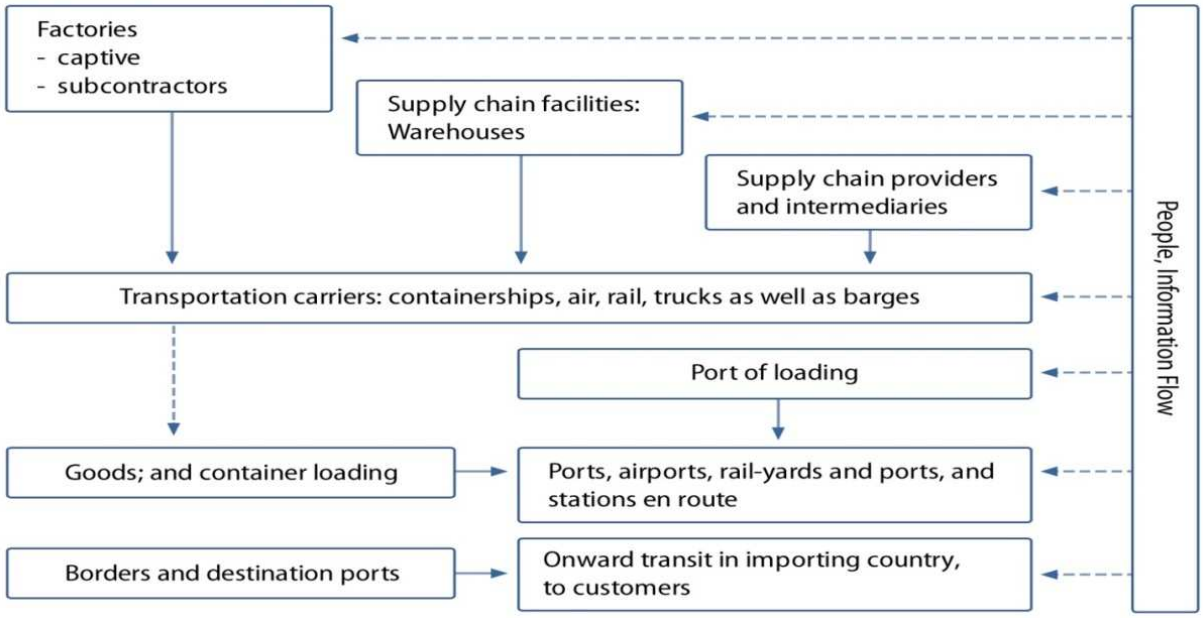

Figure 3 Points of vulnerability in supply chains

Security related sources of risk can occur at various points along the supply chain, including the following:

Manufacturing locations: security issues can take in product tampering and product substitution, which may render them dangerous to the users and the community; may affect firms' reputation and holding it liable for damages and losses; special challenges with manufacturing subcontractors, with whom security collaboration can pay off.

Goods: major security concerns include monitoring the loading of goods into containers; securing container integrity; monitoring attempts to tamper with the contents of containers while in transit; and verifying the integrity of the container on arrival.

Supply chain partners and intermediaries: firms such as trucking companies and freight forwarders form key elements in supply chains; one needs to insist and motivate the use of security practices, setting standards, checking compliance and offering incentives.

Transportation nodes and carriers: cargo security can be sought through container screening by using sensors, x-rays, gamma-rays, radiation monitoring, magnetic-field –based non-intrusive detection etc.; port security is attempted through controlled access, coupled with surveillance, based on intelligent vision etc.

People: since people are involved at every stage of the supply chain, security measures need to ensure that all such individuals can be trusted; measures include pre-shipment review of shippers and associates at the point of loading and departure, and monitoring people who have access to the containers; etc.

Information: supply chain reliability and performance depends heavily on the capture and processing of accurate supply chain information; hence, data security best practices such as virus and data access protection are widely deployed; the goal being to prevent unauthorized access to data, thus preventing alternation of cargo manifest data, etc.

Thus, the wide range of vulnerability across the entire supply chain underlines the difficulties to secure it. Compromised security at any link along the supply chain can prejudice the entire chain.

2.4 Crime[6] in supply chains

Nowadays, cargo crime, as a core form of supply chain crime, is increasingly transnational. Europol cargo theft study states that European transnational supply chain induces also truly transnational crime, while criminals may commit cargo crime in one country and sell stolen goods in another country. Europol alleges that expansion of EU is providing new criminal opportunities - especially the organized crime groups are acting more and more over the country borders. Eurowatch cargo crime bulletin 2008 expects growing cargo thefts in the next 12-14 months (i.e. in 2009). Increasing unemployment rate, which is mainly due to global economical downturn, will be according to Eurowatch one of the main triggers to increasing cargo crime. Eurowatch anticipates that vicious modus operandies such as deception operations and fake police frauds will increase during next years. Violence and use of fire arms will be also ascending. In the big picture, cargo thefts is highly costly to companies. Transported Asset Protection Association (TAPA) has estimated that cargo theft losses are 8.2 billion Euros across the whole of Europe. In the calculations TAPA has considered the full economic loss in terms of cost of replacement, re-shipping and reputational damage.

In addition to increasing cargo theft, other supply chain crime types appear to be also increasing. According to Europol The Threat of Organized Crime report (2006), several other supply chain crime areas such as drug smuggling and human trafficking are increasingly attracting the organized crime groups According to UNODC global report on trafficking in persons, number of human trafficking victims grew 27 % during 2003-2006. It should be, however, considered that calculations encompass wide variations among national and regional trends. Intellectual property right (IPR) violations are ever growing problem among the companies

[6] According to the Finnish Buro of Statistics, “crime is an act or negligence to which has been decreed penalty in law” (freely translated from the source: http://www.stat.fi/meta/kas/rikos.html)

which manufacture products with high brand value or novelty technology. Counterfeiting is a form of theft and it involves illicit production and sale of counterfeited products which are intended to pass for a real product. Counterfeited products are produced in down-stream supply chain and consequently transported through supply chain.

To summarize from the literature, typical forms of crimes with a supply chain link, i.e. "supply chain crime" include the following five[7]:

- Theft / cargo crime[8]
- Intellectual property right violence[9]
- Violations of customs fiscal regulations[10]
- Violations of customs non-fiscal regulations[11]
- Illegal immigration[12]

Outside the scope of this feasibility study, based on a working paper on "Value Chain Security (VCS)", under development by the CBRA research team, an even broader universe of "crime concerns" for companies operating in supply chains, particularly in the global environment, consist of:

- Cargo crime; including theft, larceny and robbery
- Counterfeiting and intellectual property violations
- Violations of any customs and/or international trade regulations
- Information and data theft; including industrial espionage
- Parallel trade; with various forms
- Document falsification and fraud
- Violations of environmental regulations: endangered species (CITES); dangerous waste materials
- Violations of safety, occupational health, labor law, and other possible regulations.
- Supplier crime regarding the outputs: product specification and/or raw material ingredient fraud
- Supplier crime regarding the processes: illicit working conditions; illegal labor, child labor etc.
- Distribution crime at physical locations: selling to unauthorized buyers
- Distribution crime in the internet
- Blackmailing, sabotage, vandalism and looting
- Hijacking of transportation vehicles: trucks, ships (sea piracy) etc.
- Human trafficking and illegal immigration
- Terrorism[13]; including exploiting the supply chain for delivery of illegal materials, and destruction of (parts of) the supply chain[14]

[7] These five items, together with terrorism, are explored further in this feasibility study.
[8] "Though not a statutory crime, cargo crime covers a number of criminal acts, including theft, larceny and robbery, associated with the stealing of otherwise legal products while passing through the transportation and supply function" (Possamai 2002)
[9] "An intellectual property infringement is the infringement or violation of an intellectual property right. There are several types of intellectual property rights, such as copyrights, patents, and trademarks. Therefore, an intellectual property infringement may for instance be a Copyright infringement, Patent infringement, Trademark infringement." Definition by Wikipedia.
[10] Including product value and quantity, HTS codes, country of origin, and other parameters aiming for illegal gains in paid duties.
[11] Consisting of violations of all other customs and trade regulations, including breaking trade quotas, smuggling of narcotics, weapons, endangered species etc.
[12] "Illegal immigration is immigration across national borders in a way that violates the immigration laws of the destination country." Definition by Wikipedia.
[13] One possible definition for terrorism is: ""The calculated use or threat of violence against civilians in order to attain goals that are political, religious or ideological" , from http://www.thefreedictionary.com/terrorism

2.5 Situational crime prevention

Crime prevention theories differ on the basis of how much they emphasize intrinsic crime propensity of human being, social factors and environmental aspects. Historically more attention has been drawn to psychological and social as root causes of crime (childhood experiences, genetic factors, social structures, demographic distributions, society as a control factor and changing position and needs of individuals in society). However these general crime theories give very limited amount of tools when analyzing very specific crime types under specific circumstances (Weisburd, 1993).

Crime opportunities and situational inducements or direct environmental factors play a significant role when making choices to start committing a crime (Cornish, Derek B. and Clarke Ronald V., 1986). This approach has later been elaborated to the rational choice theory, where security measures focus systematically on the reducing of crime opportunities. Rational choice theory and routine activity theory explain the dynamics of crime opportunities and choices in everyday life. They bring criminology down to the earth with measurable, tangible security measures.

Routine activity approach elucidates the chemistry for crime. It assumes that in order for a crime to occur there must be a convergence in time and space of three minimal elements: a likely offender, a suitable target, and the absence of capable guardian against crime (Felson Marcus and Clarke Ronald V., 1998). A capable guardian is not necessarily a police officer but rather anyone whose presence or proximity would discourage a crime from happening. Crimes can be deterred by altering how the elements of crime encounter in time and space.

To conclude, sixteen opportunity-reducing techniques, in four groups, of situational crime prevention are presented below:[15]

Increase the perceived effort of crime

1. Harden targets: security locks, burglar-resistance doors and windows
2. Control access to targets: access control systems, electronic locks
3. Deflect offenders from targets: fences, clear traffic signs
4. Control crime facilitators: keep keys in the safe place

Increase the perceived risks of crime

1. Screen entrances and exits: cargo screening, RFID –technology
2. Formal surveillance: security guards
3. Surveillance by tenants or employees: defensible space architecture, clear area layout
4. Natural surveillance: uniform adequate area lightning

Reduce the anticipated rewards of crime

[14] In order to thoroughly understand the nature of these various crimes, and how they link to supply chain management, following characterization is included in the CBRA working paper (2010) ”From Supply Chain Security (SCS) to Value Chain Security (VCS) Management”: (i) Definition(s) and trends for each crime type; (ii) Who has the primary concern: government vs. business; (iii) To what extent the crime is happening inside vs. outside the ”legitimate supply chain”; (iv) Which are the specific security measures to fight against the crime type; etc.

[15] The samples provided after each of the 16 crime prevention techniques are from the CBRA working paper (2010) ”From Supply Chain Security (SCS) to Value Chain Security (VCS) Management”

1. Remove targets: abandon cash money handling, minimize stocks
2. Identify property: property marking
3. Reduce temptation: rapid repair of vandalism, real time key management
4. Deny benefits: PIN –codes, anti-theft systems

Remove excuses for crime

1. Set rules: security policy and guidelines, industrial area map guides
2. Alert conscience: speedometers
3. Control disinhibitors: interfering for alcohol drinking
4. Assist compliance: handy access control sensors

2.6 Supply chain security measures and initiatives

There are virtually infinite number of ways to ´configure security´ in global supply chains, as a mixture of different processes and procedures, technologies, streams of information and data, etc. First a paper by Gutierrez et al (2006) groups security measures in five different security goal –groups, namely: (i) facility, (ii) cargo, (iii) human resources, (iv) information, and (v) business network and management system. Gutierrez provides five sample security measures per group, derived from ten voluntary SCS programs (per year 2005 situation). This ´SCS framework´-model, slightly updated with a (vi) crisis management and disaster recovery –group of measures, is visualized in Figure 4 below.

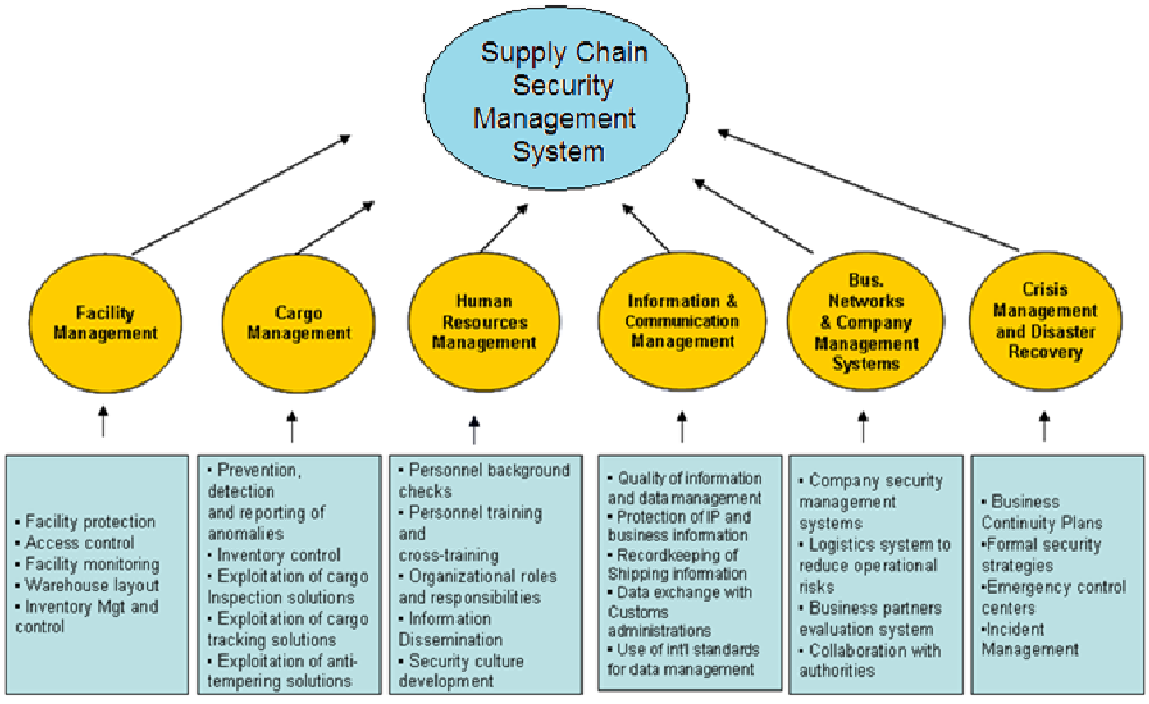

Figure 4 Supply chain security framework

Another way looking at grouping and listing of security measures has been created by an industry consortium in Asia (APEC 2005):

1. *Physical security* - includes security measures that monitor and control the facility's exterior and interior perimeters. This will include mail service security, lock and key control, and perimeter and interior alarms.
2. *Access controls* - prohibit unauthorized access to facilities, conveyances, vessels, aircraft, shipping, loading docks, and cargo areas. If access control is not possible, increased precautions in other security aspects may be needed.
3. *Personnel security* - is concerned with the screening of employees and prospective employees, as appropriate and as allowed for by law.
4. *Education, training and awareness* - encompass education and training of personnel regarding security policies, encouraging alertness for deviations from those policies and knowing what actions to take in response to security lapses.
5. *Procedural security* - assures recorded and verifiable location of goods in the supply chain. Procedures should provide for the security of goods throughout the supply chain and contingency procedures should be included within the scope of procedural security.
6. *Documentation processing security* - both electronic and manual, assures that information is legible and protected against the loss of data or introduction of erroneous information.
7. *Trading partner security* - extends SCS to suppliers and customers. Communication, assessment, training, and improvement are key components.
8. *Conveyance security* - provides protection against the introduction of unauthorized personnel and material into the supply chain, including the areas between the links of the supply chain.
9. *Crisis management and disaster recovery* - procedures include advance planning and process establishment to operate in extraordinary circumstances.

There are several ways to classify SCS initiatives, including programs, standards, regulations and pilot projects. A recent World Bank SCS guidebook (2009) divides SCS initiatives into following four groups:

- Compulsory SCS programs: e.g. 24 hour rule (US); and variations of it (in Mexico, Japan, China etc.)
- Major voluntary SCS programs: e.g .TAPA, C-TPAT, EU AEO, ISO 28000 series
- Major regional and national SCS programs: Frontline, BASC, Golden List program etc.
- Other significant SCS programs and projects: consisting of various technology pilot projects etc.

Hintsa et al. (2009) make a more detailed distinction on the primary goal, originating actor, transport mode, enforceability etc, of each SCS initiative. This is visualized in Table 1 below.

Table 1 Classification of various SCS initiatives

Action/ Response	*Originating actors*	*Transport modes*	*Enforceability*	*Examples*
Enhancing Customs Administrations security control capacity				
Adding the security layer to existing Customs compliance programs	Governmental agencies	All	Voluntary	PIP (Canada), StairSec (Sweden), ACP & Frontline (Australia), AEO (EU)
Designing and implementing supply chain security programs	Governmental agencies	All	Voluntary	C-TPAT(USA), Secure Export Partnership (New Zealand)
Preventing security problems at the source and exploiting advance cargo information	US government	Sea	Voluntary	CSI Container security initiative. US customs officers control cargo in foreign ports before they arrive at US borders.
		Sea	Mandatory (for exports to the US)	24 hour rule advance manifest rule and 96-hr notification of arrival vessel
Reducing specific industry/geography vulnerability				
Companies with high risk products or operating in risky regions designing security programs	Private sector	All	Voluntary	BASC (Latin America) against drug smuggling and TAPA (technology companies) against cargo theft.
Establishing specific regulations for vulnerable transport modes	International Organisations	Sea	Mandatory	ISPS by IMO
		Air	Mandatory	Aviation security plan of action by ICAO
Developing global security standards				
Establishing security standards that can be generalized for the entire Customs and trading community	International Organisations	All	Voluntary	WCO (World Customs Organization) Framework of Standards to Secure and Facilitate Global Trade.
Become the leading supply chain security management standard.	International Organisations	All	Voluntary	ISO (International organization for standardization), ISO28000
Technology development and deployment for security purposes				
Testing and evaluation of container scanning and tracking technology	Governmental agencies & private sector	Sea	Voluntary	OSC, Operation Safe Commerce.
Testing and evaluation of a complete tracking system along a secured trade lane	Private sector	All	Voluntary	SST, Smart and Secure Tradelane project.

2.7 Costs and benefits with SCS

Based on an exhaustive literature review, and previous research work carried out by the research team, one can present the following lists as typical cost and benefit components for SCS. [16]

[16] This sub-chapter originates to the CBRA working paper (2010) on "From Supply Chain Security (SCS) to Value Chain Security (VCS) Management" (to be published in 2010 as a journal paper: Hintsa J., Ahokas J., Männistö T., Sahlstedt J., Journal tbd.)

Typical SCS cost components consist of:

- Security technology, infrastructure and procedural investments for facility protection
- Security technology and procedural investments for cargo and conveyance protection
- Overall management of implementing and operating supply chain standards inside the company
- Overall management of implementing and operating supply chain standards in my business network, covering material and logistics suppliers
- Supply chain security training and awareness building
- Supply chain security standard certification and auditing fees
- Supply chain security consulting fees

Typical SCS benefit components consist of:

- Reduction in the number and/or value of actual crime incidents (theft; counterfeit; smuggling; illegal immigration; terrorism etc.)
- Reduction in insurance premiums, by being able to demonstrate compliance with one or more standards
- Operational benefits granted by government agencies (reduced data requirements; less physical inspections etc.)
- Promotion and protection of company brand name and reputation in the eyes of customers and other stakeholders (covering any kind of conditions, also post-incident situations, if they occur)
- Exploitation of a supply chain security standard as a core management tool (like standards in quality management, environmental management etc.)
- Gaining any kind of ”side benefits” (or collateral or dual benefits) regarding supply chain and logistics operations (better visibility to the supply chain; faster reactions in case of any type of disruptions etc.) [17]

Taking a more theoretical view on SCS costs and benefits, one can consider an optimization task to “minimize the total cost of security compliance”, illustrated in Figure 5 below[18]. The y-axis represents the cost of implementing and managing security, which increases from the origin along the (positive) y-axis. The x-axis represents the targeted or achieved security level, starting from “0-security” in the origin, and increasing along the (positive) x-axis.[19]

The curve I illustrates the cost for being non-compliant, i.e. not investing enough in security management regarding crime risks, government requirements, available benefits etc. – the lower the security level, the higher the potential cost for being non-compliant is (left part of curve I). The curve II illustrates the cost for security management itself, i.e. security products, technologies, services, certification costs etc. For this cost: the higher the spending, the higher the security level (right part of the curve).[20] Next, the curve III illustrates the total cost of security compliance, i.e. summing up the curves I (non-compliance and lost efficiency costs) and II (security product and service costs).

[17] The lists of typical SCS cost and benefit components are presented and tested in the Operator survey (Chap5).
[18] Original source for the diagram: Ahokas J., Hintsa J. Total Cost of Security Compliance. SCSM2006 Conference. Vevey, Sep.2006.
[19] There are no standard numeric scales for either y- or x-axis; theoretically, the maximum security level can be seen as “100% security”, which of course is both very difficult to define, and virtually impossible to achieve – without very serious security investments.
[20] This is of course assuming that the planned or implemented security measures are efficient (or even cost-efficient).

And, as in any management optimization task, the goal is to minimize the total cost security compliance, i.e. to aim for the lowest point of curve III. The last point made in the graph deals with curve II´, which highlights the importance of continuous seek for better targeted, more cost-efficient security measures, in order to lower the overall total cost of security compliance.

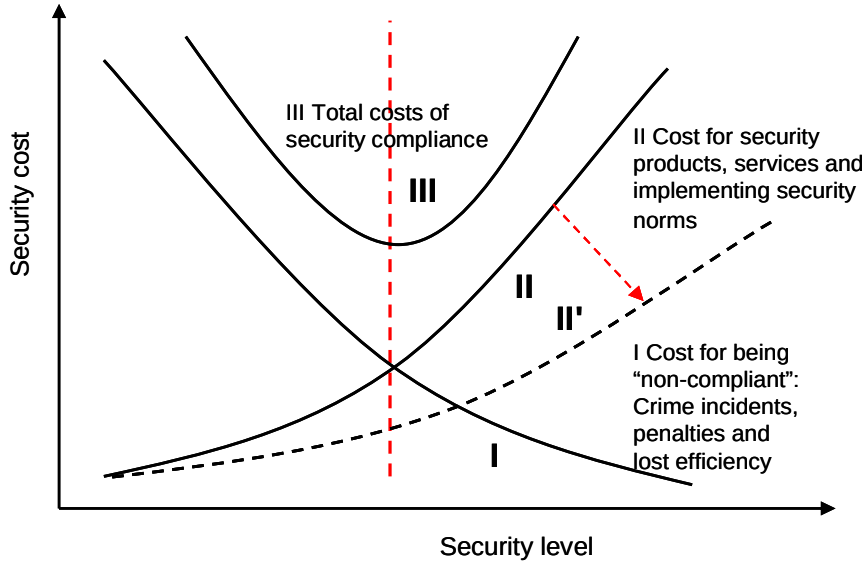

Figure 5 Minimizing the total cost of security compliance.

2.8 Conclusions

Based on this brief literature review on supply chain security (SCS) related literature, following conclusions can be drawn:

- Supply chains with their natural open structures and connections between manufacturing locations and other facilities, goods and carriers, supply chain partners, people and information, have vulnerabilities in front of criminal (intentional) acts.
- Crime in it´s various forms is often perceived as a growing concern in supply chains, as criminal organizations seek for lucrative "high profit, low risk" targets and operating models.
- SCS falls within the frame of risk management in supply chains, with the objective of reducing likelihoods and/or minimizing consequences of crime (and terrorism) related incidents in supply chains.
- Various approaches, techniques, methodologies and theories exist to fight against crime in supply chains, as well as outside supply chain environments.
- SCS programs often consist of packages of security measures to enhance facility, cargo, human resource, information system and business network security.
- Cost components for SCS are fairly straight forward to identify, still hard to measure; while the identification and measurement of SCS benefit components remains (even a harder task.

3 Expert interviews

3.1 Introduction

This Expert interview exercise has the following two goals regarding this feasibility study of possible SCS standards in Europe:

- To bring together SCS knowledge and views from top European experts, to support the further development of this feasibility study report.
- To provide an opportunity to all interested parties to state their ideas, opinions, expectations and concerns about the whole SCS initiative.

The outcomes of the interviews are used explicitly in the following chapters of the study:

- As a basis for in-depth SCS initiative analysis (Chapter 4)
- As factual points and statements tested in the Operator survey (Chapter 5)
- As some of the final conclusions and recommendations (Chapter 6).

The rest of this chapter has the following structure:

- Chapter 3.2 Interview process
- Chapter 3.3 Findings with high consensus
- Chapter 3.4 Non-consensus findings
- Chapter 3.5 Explicit concerns about developing new SCS standards
- Chapter 3.6 Collection of all standard ideas shared during the interviews
- Chapter 3.7 Standard development framework and ideas for possible standards
- Chapter 3.8 Conclusions

3.2 Interview process

A total of 21 interviews were carried out between March and May 2009. 17 interviews were carried out by phone, one was a personal interview, and three replies were provided in writing. The interviews lasted between 15 minutes to one hour. The association /company[21] and country of each expert is listed below:[22]

- Association des Utilisateurs de Transport de Fret, FR
- Confederation of European Security Services (CoESS), BE
- EuroCommerce (the retail, wholesale and international trade representative to EU), BE
- Europe Container Terminals, NL
- European Association for Forwarding, Transport, Logistic and Customs Services (CLECAT), BE
- European Express Association (EEA), BE
- European Office of Crafts, Trades and SMEs for Standardisation (normapme), BE

[21] In case of single companies, the expert in question was representing the views of a national standards association.
[22] This list is in alphabetical order, while the list of expert references, E1 to E21, is in random order.

- European Shippers Council (ESC), BE
- European Small Business Alliance (ESBA), BE
- Integrated Safety and Security, University of Applied Sciences Campus Vienna, AT
- International Union of Combined Road-Rail Transport Companies (UIRR), BE
- Maersk Group, DK
- Outokumpu, FI
- Road Haulage Association, UK
- Se Klapeida State Seaport Authority, LT
- SIS, SE
- Temi Group, IT
- The Association of European Chambers of Commerce and Industry (Eurochambers), BE
- The Community of European Railway and Infrastructure Companies (CER), BE
- Transported Asset Protection Association (TAPA), UK
- World Shipping Council, BE

A list of eight questions was drafted by the research team, based on the study mandate and findings in the literature review. The questions were the following:

1. Please describe briefly your organization, and your role in it (you are welcome to email in advance any materials on your organization)?
2. Please share your overall views on how SCS has evolved since year 2001, and which trends you see happening in the future?
3. Please give your overall comments on the draft Table of contents for the study report?
4. Which SCS materials (on other projects, studies, reports etc.) would you recommend to include in the study review?
5. Which existing SCS standard(s), on your opinion, should be part of the in-depth analysis?
6. Would you have contacts to supply chain operators (shippers, carriers, warehouse keepers etc.) we could survey in April 2009?
7. Who do you foresee as other stakeholders, experts etc. to invite for interviews in this feasibility study?
8. Do you have any other views or opinions regarding the SCS scope, operators etc. as it relates to this SCS feasibility study?

3.3 Findings with high consensus

F1 (Finding-1): Crime appears to be of growing concern in Europe

The first high consensus finding links to question number 2 on overall views and trends of SCS and crime since the year 2001. Keeping in mind that trends in crime patterns are at best perceptions and 'educated guesses' due to the reasons explained in Chapters 1 and 2, five experts shared the view that crime appears to be on growing trajectory in Europe.

E6: "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..."

E2: "Awareness of SCS problems has been increasing (since 2001)... Cargo crime is recognized as a problem today, while earlier it was thought of as a victimless problem... Also sensitivity of terrorist groups exploiting the supply chains..."

E5: "Crime has become much more organized (since 2001), instead of opportunity incidents... Internalization of offenders is also happening... Bigger incidents today are mostly carried out by well prepared international organizations..."

E15: "Crime in supply chains has increased (since 2001), including smuggling, counterfeiting, parallel trade and theft... This has been happening while the media attention has been focusing on terrorism..."

E10: "Growing crime trends (since 2001) is a problem especially in the new member states...more theft in trucks... and the areas where the train has to stop..."

F2: There have been no witnessed occurrences of terrorism in European supply chains

The second consensus finding was on the topic of terrorism in supply chains. None of the experts quoted any concrete examples of how terrorists would have e.g. attacked (European) supply chains, or used it as a delivery vehicle for serious weapons. Instead, three expert quotes, shared below, attest to the contrary:[23]

E5: "We have to pay millions for supply chain (security), even though there has been no incident of terrorism…"

E19: "… where is the terrorist threat for a lorry who moves tomatoes from one place to another… I am not aware that terrorists are going after individual trucks…"

E14: "…terrorism we have not seen…"

Closely related to this, one expert (E20) also made the following statement: *"…now we see that the fear of terrorism is going down… and focus shifting to financial crisis…"*. Another expert (E12), said that:*"…the opinion of carriers, trucking companies etc. is that they will not put resources (in SCS standard implementation) if it is just against terrorism…"*

F3: Lots of SCS initiatives have been introduced since 2001

The third consensus finding deals with SCS programs, standards, regulations and other possible initiatives introduced since 2001. Several experts see an overwhelming number of new initiatives being rolled out, with lots of abbreviations, many similarities (but still some differences), and focusing often on anti-terrorism. Three quotes:

[23] We are dealing again with perceptions, as none of the experts are likely to be aware of any "close by incidents", where some attack was either planned or partially executed – but failed due to government intervention or some other reason.

E4: " After 2001, there was ... a panic reaction, to fear of major chemical, biological, nuclear attack…the idea was to secure the US border from outside...even though in 2001 airplanes came from inside..."

E20: "Regulations in air transport; dangerous goods, ADR...EU legislative measures, based on ISPS code...C-TPAT...CSI...100% scanning...TAPA FRS...WCO SAFE FoS...European Chemicals Council, transport of dangerous goods.. prevention of terrorist getting into possession on dangerous goods... ISO).

E12: " Most of the (SCS) programs are similar... they come from same origin... they deal with security of premises, training of people, control of sub-contractors..."

F4: Criticism of the existing SCS initiatives

The forth consensus finding, mainly related to the question number 2 on SCS trends, points out a variety of shortcomings of the existing SCS initiatives, including lack of benefits for businesses, lack of coordination between various programs and agencies, temporary and superficial characteristics of some of the initiatives, and so on. To illustrate the skeptical attitudes, five expert quotes are shared below:

E20: "Our members have really noticed an explosion in national, bilateral and international SCS initiatives... We have a feeling that more is coming...(at the same time), mostly we see a lot of new burdens, while we don't see any gain in extra security".

E12: "There are lots of different SCS programs, without coordination... Every program adds a layer, without coordination..."

E5: "Now you get all different agencies involved in terrorism... too many programs, too difficult... no one-stop-shop.."

E10: "It is confusing as there are so many (SCS) initiatives... Emphasis on word ´initiatives´, as especially SCS technology oriented initiatives tend to come and go..."

E9: "EU AEO is for the time being more of a paper desk exercise, rather than an actual security improvement... likewise, why would 100% scanning be real security?"

Box 1 Illusions with SCS benefits

Companies often complain that the lack of tangible benefits regarding SCS standards is the main reason not to implement them. This argument seems reasonable and difficult to argue against: unless benefits exceed costs, one should not implement any standard (or make any kind of investment). Many government-developed and enforced SCS programs are perceived to fall into this category, e.g. the AEO programs, where customs administrations are struggling to deliver on their promises about lower inspection rates, priority cross-border treatment etc.

In order to objectively estimate, analyze and measure any potential SCS benefits, the CBRA research team suggests grouping benefits into the following three groups:

- Direct security benefits: reduction in crime incidents (and possibly trials); lower security related administration costs (including investigation and claims); and lower insurance premiums (in the long run).
- Being part of a "SCS / AEO club": satisfying customer requests; brand promotion and protection; enjoying government recognitions (also 3rd country, via mutual recognition schemes); and faster cross-border lead times (with less inspections).
- Any other side benefits / collateral benefits / spill-over benefits: improved supply chain visibility; lower safety stock levels; improved job satisfaction etc.

Finally, the research team makes the following recommendations regarding the three groups of SCS benefit listed above: (i) Direct

security benefits should be the main driver to justify (or decline) any SCS investments; (ii) Before justifying any SCS investments with the "SCS / AEO club" arguments, one should spend some time investigating whether the SCS programs will be fully implemented as intended - e.g. customers will not accept any other way of demonstrating adequate security standards in the supply chain (than e.g. a specific AEO standard); and (iii) Non-security-oriented benefits are typically very difficult to identify, deliver and measure – thus one should take a realistic view before including them in any investment calculation.

F5: Risk management should be a core component of any SCS initiative

The fifth consensus finding relates to the relevance of risk management as a core component of any SCS standardization or other initiative. Here the experts took a broad view on the meaning of 'risk management', varying from SCS standard design to identifying high-risk containers in the supply chain. Below four quotes are shared to illustrate their views:

> *E4: " The main change now (compared to previous SCS initiatives): instead of securing the whole supply chain, we must do risk assessment first..."*
>
> *E5: "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"*
>
> *E13: "If you don't have credible risk assessment in place (for containers), you should open every box… this is not feasible"*
>
> *E2: "Must be risk based, no one-size-fits-all approach works..."*

Box 2 Risk management shortcomings

The central role of risk management, or risk assessment, is often quoted by business practitioners as a key part of the efficient implementation of SCS standards and other management systems. This can imply either that the actual SCS requirements are determined based on a priori risk assessments, with (perceived) threats, vulnerabilities, risk likelihoods and consequences; and/or that risk management becomes part of the SCS standard requirements.

While no-one normally questions the overall relevance of risk assessment as part of efficient supply chain security management, including setting priorities for crime prevention and/or recovery investments, many challenges and obstacles exist in the process, such as:

- Who is capable in an objective way to recognize all crime and terrorism related threats and vulnerabilities in supply chains?
- Who has the knowledge of the numeric likelihoods and consequences of various risks?
- Especially for "low likelihood – high consequence" events (e.g. terrorism), who can assign any realistic numbers to these?
- Even for "high likelihood – low consequence" events (e.g. theft), who can forecast changes in crime patterns, including discontinuity points?

Due to these types of challenges with the "traditional" risk management approach, the CBRA research team suggests complementary approaches be considered by supply chain operators in the future. New approaches are emerging based on human factors and experiences in high-reliability organizations. They emphasize expertise, acceptance of complexity in operations, awareness and commitment to react to early warning signs – often hardly trying to quantify the risks, and possibly not even mentioning the word "risk" per se.

3.4 Non-consensus findings

N1 (Non-consensus finding -1): Is SCS standardization primarily a public policy versus a private sector matter

The first non-consensus finding deals with the question of whether design, implementation and control of SCS initiatives are primarily a public sector or a private sector concern. Examples exist today of both approaches: (i) public sector examples include US initiatives C-TPAT, CSI and 24-hour rule, and (ii) private sector initiatives include TAPA and BASC. Even though there are only two experts quoted here – with opposing opinions – this is a crucial topic for this feasibility study.

The first expert (E13), who sees SCS as a public sector concern and is very much a believer in public regulation, worrying about vulnerabilities created by voluntary measures, said that: *"SCS is a public policy issue, which must be addressed by the governments... we don't think it is up to standards organization (such as CEN or ISO) to define SCS needs in a vacuum... we want law, uniformity, level playing field...voluntary measures create vulnerabilities..."*

The second expert (E2) was of the opposite opinion, stating that: *"The approach that everything should be regulated does not work".* Related to this issue, several of the other interviewed experts made the point clear up front that: *"there should be no new regulation for SCS in Europe".*

N2: Is SCS standardization primarily a national, a regional or a global issue?

This second non-consensus finding deals with the question of whether SCS standards should be of national, regional or global nature. Examples exist for each category, on a world-wide basis: (i) national: e.g. several British standards for technical aspects of SCS, including CCTV management and operation, and Jordan's' Golden List –program; (ii) regional: the EU's AEO, Latin America's BASC; and (iii) global: ISO28000 series; and WCO SAFE, as a global framework for customs.

Experts who were in favor of global approaches were using following types of arguments:

> *E13: "Trade is global by nature, and thus only global standards for SCS are necessary...We fear like a plague, that EU goes ahead with its own SCS requirements, while this would be followed by the Chinese, US etc..."*
>
> *E11: " Trade is global, why have a special European standard... the big logistics want to have a common ground, global standard ; having worked hard on the ISO standard..."*
>
> *E20: "...if a standard, then a global one...otherwise there will be a disconnect with supply chains."*

Experts who saw relevance of the regional, i.e. European approach, shared their political views regarding where SCS initiatives originate from, as well as practical reasoning regarding the possible cross-border implications of a possible ´large-scale incident':

> *E12: " Europeans have to comply with SCS regulations, all focusing on international trade... This initiative concerns intra-EU supply chains..."*

E15: "… supply chain operators (in our country) would be pleased if there was a European standard for SCS (as they are facing difficulties in implementing some current initiatives.."

E6: " If you take the example of airport security, which used to be a national competence...now 2320 regulation, the EU imposes countries a minimum way to secure the airports...with measures that have to be taken… this could be a way to go forward… that countries should have a national plan... critical infrastructure protection, CIP, Sep.2008 directive, similar approach as 2320 – defines European critical infrastructure...in one country or multiple... it can be purely national, but if there is a terrorist attack, it would have major impact on other countries too..."

Finally, one expert (E11) also emphasized the national aspects of supply chains in Europe: *"Cross-European haulage is small, involving some countries like Ireland and Scandinavia, mostly national movements..."*

N3: Is SCS standardization primarily about anti-crime or anti-terrorism?

The third non-consensus finding deals with the goal of SCS initiatives: is it to fight against terrorism, or to fight against one or more crime types? Again, existing SCS initiatives cover both aspects: (i) US C-TPAT, CSI and 24-hour rule have been established clearly for anti-terrorism purposes, whereas (ii) TAPA was established as anti-theft program of high value goods, and BASC as an anti-smuggling program against narcotics smuggling.

The views varied from "nothing in common" to "killing two birds with one stone" types of observations:

E12: "Nothing in common, as the consequences and responses are so different".

E11: "In smuggling, we can accept that some amount of (illegal) drugs get through to our country... With nuclear weapons, we cannot afford one failure".

E14: "Even if some preventative measures are the same or comparable, the physical handling is still different... The actors are very different... In ordinary crime, the companies get more involved and follow up is different... While terrorism would typically be a one-time incident, never to be repeated (the same way)"

E9: " 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..."[24]

One of the experts (E12) also emphasized the different approaches required for different types of crime risks: *"Smuggling of tobacco and alcohol has different actors and different problems as other crimes – if one tries the catch-all, or one-size –fits-all approach, nothing will be achieved…".*

Box 3 Security measures: terrorism versus theft

A common debate amongst government officers, supply chain practitioners, and security professionals – also in this feasibility study – is whether the same security standards and measures can help in the fight against "ordinary crime", primarily cargo theft, in addition to the fight against terrorism, i.e. is it possible to kill two birds with one stone, or, do they risk becoming a "jack of all trades, and master of none"?

Conceptually, the same security measures may assist with both missions. If one considers container integrity as an example, the

procedural, electronic, mechanical or other security measures (or their combinations) designed to prevent unauthorized access to a container in-transit, can simultaneously prevent criminals, terrorists and smugglers from stealing anything from or placing anything to inside the container. Also background checks with personnel and suppliers can help to avoid hiring individuals likely to commit a criminal or terrorist act. There is no guarantee of success, however, as demonstrated in the previous example of a recent theft of cash in transit in Lyon, France.

The main difference between terrorism and theft lies in the motives of the perpetrators. Terrorists aim at getting publicity for their ideological goals. They create fear and terror among people so that they could coerce policy makers into making decisions the terrorists want. Thieves base their targets on economic reward. The other differences relate to the risk components of impact and probability. Terrorism attack scenarios generally anticipate wide-scale devastation and disruption to society and the economy, such as might arise from the explosion of a "dirty bomb in a container". In contrast, a theft is usually a minor or intermediate event. In addition the occurrence of cargo theft is more frequent whereas terrorist attacks are comparatively rare.

In the name of cost-efficiencies, or "security economies of scale", the CBRA research team recommends maintaining an open mind when designing new SCS standards and technologies etc. to tackle criminal and terrorist threats together. One should remain mindful also that single security measures (the 'silver bullets') able to deal with all potential threats are rare and, in many cases, the successful standards and measures taken are likely to be many and varied.

N4: Is SCS standardization truly voluntary, or can ´voluntary standards become mandatory´?

The next non-consensus finding deals with whether voluntary standards actually really are voluntary – or whether they are likely to become market-driven, mandatory initiatives? One could argue here that if a standard provides enough value to the supply chain – or supply network – then a snowball effect will follow, and it might become a practical requirement to stay in business. The concern here might be that by introducing a new standard, even if it doesn't provide real value (or is not really needed), big companies may require SMEs to comply with it, just for the principle.

One expert (E19) worried about the mandatory aspects stated that *"Standards are not voluntary... the customers, especially large companies and public administrations ask SMEs to comply with standards..."*

Another expert (E12) didn't see this as a risk, drawing an analogy from other standardization domain: *"Make comparison with ISO9000 in the middle of 1990s... big companies would refer to ISO9000 processes ... but, it did not become a means of segregation"*

Another related debate was raised as to whether security is – or should become – a competitiveness factor, i.e. can one win more business, and/or better margins, by active implementation of various SCS initiatives? Expert E5 sees security as a selling point for the logistics sector: *"Transport companies have started to place more importance in security (since year 2001)... Security is used as a selling point...".* While expert E13 felt the opposite: *"(In our sector), security should not become a competitive edge, but we want law, uniformity and a level playing field..."*

N5: Other non-consensus findings

Two interesting points were raised as to whether the whole scheme of authorized versus non-authorized businesses can work. Two logistics sector experts challenged this, with the following arguments:

> *E4: " Trains, we have problems: like on road all types of operators… in trains, we have units from authorized, and non- authorized operators..."*
>
> *E13: "There can be up to 10.000 containers on a ship.. no way that we can operate only AEO containers. ..what good does it do, if one container is AEO, and another not?"*

And lastly, one expert (E11) challenged the concept of layered security, by stating that: *"If you are implying that a European standard is needed, you are saying that customs, port authority, 3rd country checks etc. do not work..."*

Box 4 Layered security

One of the interviewed experts in this feasibility study made an implicit note against the relevance of "layered security" in supply chains, thus motivating a brief analysis on what layered security can mean in a supply chain context.

Layered security has a long tradition in the military. A medieval stronghold can be used to illustrate this: The first security layer of the stronghold is a moat. If attackers manage to overcome this obstacle, they encounter high walls which resemble the second layer of security. In addition to these two security layers, the addition of castle guards cannot be ignored in the defense of the stronghold. In theory, physical security layers can be added to security systems indefinitely. However, physical obstacles only slow criminals. Without proper surveillance and the intervention of a human actor, criminals can break through security layers sooner or later.

The same principles can be applied in the context of supply chain security? Criminals are a miscellaneous group which has different motives, skills and levels of intent to commit a crime. Effective security measures depend on time, place and the "criminal on duty". Natural surveillance of workers may prove to be an effective crime prevention method during the day time but ineffective at night. Burglar resistant doors are effective until a skillful thief breaks it. In order to establish an effective security system various layered security systems could be deployed. An illustrative example consists of three layers of security for trucks:

1. A secure parking lot scheme can prevent criminals from gaining access to a truck.
2. Doors of the truck can be locked with burglar resistant locks.
3. The truck can be under surveillance by a security service provider company, with potential links to a local enforcement agency.

By layering security measures valuable targets can be shielded with higher confidence of successfully deterring, preventing or identifying a crime taking place. If every security layer can stop 80 % of criminals trying to steal consignments, this suggests that a three layer system deflects 99,2% of attacks.[25] The same reliability level is quite hard to achieve with just one security measure in place. Consequently, sole spearhead security measure with an outstanding 95 % deflection rate is still less reliable when compared with a set of layered security measures with an 80 % deflection rate. As a conclusion, the CBRA research team suggests layered security measures be used because there is no single silver-bullet security measure which would stop all crime in the supply chains for good.

3.5 Explicit concerns about developing new SCS standards

In this sub-chapter around one dozen different concerns raised by the experts, concerns closely related to this feasibility study and/or possible new standard on SCS, are shared – and briefly commented on by the research team.

C1 (Concern-1): A new SCS standard may become a European regulation

This concern was expressed by ten experts, who see that (i) a new European SCS regulation is absolutely not required, and who have the concern that (ii) a CEN SCS standard could (later) lead to a regulation. One expert (E11) stated that: *"We know the background to this study... this will be converted into legislation..."*. This point is taken directly to the final conclusions of the study (Chapter 6) – without the need for much further exploration or analysis.

C2: This study has a risk of starting with the conclusions

[25] P(system deflects criminal) = 1 – (1. layer fails) * (2. layer fails) * (3. layer fails) = 1- (1-0,8)^3 = 0,992

Another expert *E2* stated that*: "This study needs to check if a standard is needed, not to set the end results and just trying to confirm it".* Expert E4 continued that*: "... a previous study started in a situation of high threat – try to avoid this".* In response to these concerns, it should be stressed that this study does not start with any preconceived conclusions, as it explores, in parallel, the market needs and constraints for any type of new SCS standard, without a fixed standard scope or other result in mind.

C3: The scope for the possible new SCS standard may not be clear enough

Expert E12 made the point that at the time of the expert interviews the scope of the possible standard(s) was not clear, which might lead to problems: "*The scope of this norm should be defined, is it only dedicated to the fight against terrorism, or does it include other tasks like fighting illegal immigration ... we don't think that the response is same….neither is it for theft and pilferage...".* It is true that identifying the possible scope(s) was part of the research work, thus the detailed scope(s) were not shared at the time of the interviews (as they were not known to anyone, including the research team – as mentioned in the previous concern C2).

C4: SCS standards may not work at all in fight against crime

One expert (E19) raised the concern that standards may have no role in the fight against actual crime, thus implicating that they are just paper exercises, the exact quote being: *"Crime exists, lorries get stolen, and reported to the police... I can't see how standards prevent crime".* This point is referred to both explicitly and implicitly throughout the study, e.g. while looking at the possible benefits of SCS standard implementations.

Box 5 Challenges with image-based SCS

One of the most debated security measures is that of the "image-based surveillance and inspection". This normally involves surveillance with closed circuit television (CCTV) systems and x-ray scanning equipment, especially the scanning of maritime containers. Several questions have been raised by practitioners in recent years regarding the accuracy, efficiency, costs and a number of other parameters relating to the image-based approaches. Research analyzing the links between CCTV investments and crime trends especially in city environments (hooliganism, theft etc.) have indicated some controversial results. Regarding the x-ray scanning of sea containers, the CBRA research team could not identify any empirical studies on the efficiencies, or (realized) operational costs etc.; only conceptual papers were found.

Image-based SCS has recently been a fiercely debated topic due to the introduction of the US Secure Freight Initiative (SFI) legislation. This legislation requires 100% scanning for all US-bound containers at foreign ports by year 2012.[26] The new legislation may complicate trading and induce substantial operational costs. Moreover, 100% scanning is sometimes argued to undermine security by diverting scarce resources from other more effective security measures.[27] The Secure Freight Initiative is also criticized by many for being more concerned over the amount of security in place rather than the quality of it. This initiative appears to run counter to the contemporary risk based scanning approach where high-risk containers are scanned more frequently than low-risk ones. It is still unknown how much real security 100% scanning will ultimately deliver.

What is lacking in the public debates on "security efficiencies" of image-based SCS solutions, is a structured approach to the identification and analysis of key cost components, bottlenecks, pitfalls, trade-offs etc. Therefore the CBRA research team suggests the following issues to be covered in future debates and research:

- How much does the equipment (CCTV or x-ray scanner or other image-based device) cost?
- Who covers the costs in the first place? Are the costs passed later to other actors?
- What are the space requirements needed to install and operate the equipment? Is this space available already, or does it need to be procured? If procured, how much does it cost, and who pays?
- What are the normal operational and maintenance costs of the equipment? Who pays?
- What is the overall quality of the images?
- How well can the images be used for crime prevention (e.g. x-ray to detect dirty bombs inside a container)?
- How well can the images be used for recovery (e.g. CCTV images to prosecute thieves)?

[26] Report to Congress on Integrated Scanning System Pilots (Security and Accountability for Every Port Act of 2006, Section 231)
[27] EC DG TAXUD (TAXATION AND CUSTOMS UNION) comments on 100% scanning

- What is the false-positive rate with the images, i.e. what is the percentage of false alarms (triggering e.g. physical inspection actions)?
- Who is analyzing the images, either in real-time (for prevention) or for recovery (identifying the suspects and/or prosecution)? What is the job motivation like? What are the educational requirements?
- How much storage and communication capacity do the images require? Is it available? Who pays?
- How does the image-taking process impact the supply chain? Does it slow down the flows?
- Are there any legal (e.g. privacy), safety (e.g. radiation) or other "side concerns" with the technology? How are they tackled?
- Are the financial and/or human resources required for the image-based SCS solution(s) separate from other SCS efforts (which may be perceived more security efficient)?
- Is there a risk that an image-based SCS solution would contribute somehow to a "false sense of security" being created?
- Is there a risk that an image-based SCS solution would increase barriers for trade (e.g. in developing countries)?
- How likely is it that an image-based SCS solution would deter criminals from committing crime and consequently prevent the crime from happening in the first place?

The list above is not intended to be complete; instead, many other crucial questions are likely to emerge, once experts are put together for an objective analysis session: this is proposed by the CBRA research team, in order to minimize overly political and/or emotional debates in the future.

C5: SCS standard may not fit to all actors

Expert E12 highlighted the point that some of the existing SCS initiatives are designed more for large multinational companies, instead of small and medium sized enterprises (SMEs): *"When we consider various programs... C-TPAT is the mother… then WCO SAFE… and then EU AEO… these are prescriptions, almost norms for a specific category of actors: big multinationals and carriers…they have the resources. These are very different from intra-EU actors, small carriers – the vast majority of trucking companies are one-truck companies..."*. In light of this concern, particular attention was paid to the realities and constraints of SMEs during this study.

C6: SCS standards may reveal security secrets to the 'bad guys'

This is the classical question, well-known at least in the information and data security environment: should security be kept secret, or " Security Through Obscurity (STO)", i.e. should security knowledge be kept in the hands of a minimum number of highly trustworthy individuals, thus preventing the development and implementation of any open SCS standards? Expert E21 formulated this concern in the following way: *"Security is not an issue to talk about openly, it is supposed to be secret... Companies in our industry share information between each other, and with the police..."*. This aspect is tested in the Operator survey, as one of the possible dilemmas regarding SCS standards and other initiatives.

Box 6 Security through secrecy?

One of the interviewed experts in this feasibility study raised the point that "security should be kept secret", otherwise criminals and terrorists can (too) easily exploit loopholes in the measures in order to commit their crimes. Could the requirement for "secrecy of security" result in an end to any and all publicly available SCS standards?

Looking at security traditions in a broader context, two extreme paradigms can be identified: a Military phrase "loose lips sink ships" suggests a strict nondisclosure approach. The phrase means that in some circumstances disclosure of information by unwitting or unscrupulous people – i.e. so called "loose lips", can lead to unfavorable results, metaphorically described as the "sinking of ships". The premise is therefore, that it is safer not to share details on security procedures, or even on the existence of something worth securing. The other paradigm states that there is "no security through obscurity". IT experts representing this approach think that criminals inevitably figure out the vulnerabilities in a system one way or another. Therefore, they would suggest, instead of hiding the security vulnerabilities from a broader audience, one should focus on fixing them.[28]

[28] Swire, P, 2004. *A Model for When Disclosure Helps Security: What Is Different About Computer and Network Security?*

A fully secretive approach would mean that only a hand full of authorized security experts would know the big picture as well as the details of SCS initiatives. Only those few security experts would be able to develop and discuss security improvements, ultimately putting an end to public SCS discussions and knowledge sharing. This could quickly lead to dilemmas such as "who is guarding the guards" etc.

A fully, open information disclosure approach, on the other hand, is likely to reveal the most vulnerable links of supply chains, logistics routes, schedules and procedures, evidently also to criminals. Using this information the criminals can plan their illicit operations well in advance and strike on the most valuable consignments.

Nevertheless, it is arguable that a policy of disclosure puts pressure on supply chain operators to improve the weakest links by deploying new crime prevention techniques and re-structuring supply chains etc. The improvement of the weakest links is facilitated by the public which is able to criticize security measures and argue their effectiveness, thus revealing security gaps which might otherwise be ignored. Information disclosure also prevents security service providers from hiding their security weaknesses. Transparency of security information allows security service buyers to assess the capabilities of the security service providers and purchase service from the companies which provide the best security.[29]

To conclude, there is no easy answer as is so often the case with SCS design and optimization matters. Instead, one must continuously seek a balance between secrecy versus openness in security management and standardization.

C7: SCS standards may become counterproductive for security

Besides revealing security secrets to the 'bad guys', two experts raised a few other concerns where SCS standards may become counterproductive for actual security. Expert E11 shared his concern about the ultimate shortcomings of any type of personnel screening, background checking and vetting processes: *"... a guy would become most trustworthy on paper, and hit afterwards..."*. Expert E13 explained how a technology meant to enhance security (via maritime awareness), actually became a tool for the criminals to choose the target (ship) of their attack: *"There is also a constant debate...you have technical devices that can assist cargo or vessel security... e.g. ships have to carry satellite devices, now it is 2000 miles from the coast, for maritime awareness, like in aviation...in a case at the coast of Yemen, bad guys intercepted ship signals..."*. Some of these concerns are tested further in the Operator survey (Chapter 5).

Box 7 Counterproductive SCS

As one of the interviewed experts pointed out – using the case of terrorists exploiting ship arrival (early) signals to plan their attacks on the ships – standards and solutions meant to enhance supply chain security may sometimes turn out to be counterproductive, i.e. to decrease the real level of security in supply chains.

Another example of counterproductive SCS comes from the news archives, known as the "plata-or-plomo" –dilemma (taking a bribe or a bullet): in Mexico truck drivers of the security certificated companies have been coerced to convey marijuana shipments across the border into the US. Criminals exploit ruthlessly the fact that the trucks of the certificated companies are inspected / scanned less frequently than the trucks of non-certificated companies.[30] In addition to coercion, the criminals are painting logos of the certificated credible companies on their fake trucks which are then loaded with drugs or other contraband.[31]

It goes without saying that any kind of security measure which facilitates criminal efforts damages the credibility of the SCS programs and provides plenty of ammunition for the critics of the SCS standards. Being closely linked with the concepts of "secrecy of security", the "false sense of security" and the "weakest link in security", the CBRA research team recommends consideration of these pitfalls in greater detail and avoidance of them when designing any new SCS standards.

C8:The standards development process may be over-influenced by security businesses

[29] Schneier, B, 2004. *The Non-Security of Secrecy*
[30] http://www.washingtontimes.com/news/2009/nov/24/smugglers-set-eyes-on-us-truck-program/
[31] http://abcnews.go.com/Blotter/story?id=4156618&page=1

A common concern among the supply chain operators, regarding both this feasibility study, and the possible development of one or more SCS standards, is that security service and/or technology companies may have too big an influence and guide the process towards ´high threat scenarios´, proprietary solutions, expensive auditing and other schemes. Expert E20 made the following point:*"... one should not include people (in this feasibility study) who are only interested in making money (on security)...",* and expert E5 continued by stating: *"You don't want auditors and security system suppliers for the development phase...you need people from industry with strong experience on security, but not as their core business...don't make a measure mandatory...".* This is a topic where a working balance should be reachable, i.e. not to become over-influenced by the security business sector, while not losing the opportunity to exploit the knowledge of security professionals during the process.

Box 8 Who is guarding the guards?

The Latin phrase "Quis custodiet ipsos custodes?" has been puzzling people since the ancient times. It was Plato who introduced first this philosophical dilemma which can be translated as "Who will guard the guardians themselves?".

Cases exist where the guard has committed the crime – e.g. a cash transport company in Lyon, France, fell victim recently to one of its security guards with "an exemplary work record" who managed to steal 10 million Euros in cash from a customer (bank) delivery.[32] In view of such example, it is clear that background checks, training, and internal security procedures do not always work: it begs the question "who is guarding the guards of the supply chain"?

A related aspect, touching daily supply chain operations and security, is: how can one ensure that a security service provider is really delivering the service and/or performance level agreed in the contract – assuming that such service or performance levels are defined and agreed in the first place? Maybe a combination of audits, tracking of realized crime incident rates, pricing (or discounts or penalties) based on realized crime incident rates, joint security drills, even word-of-mouth, and some other means can be helpful in ensuring that the guards are performing their tasks properly – as hiring "a guard to guard the guards" may not be seen to be economically feasible.

Another SCS guard-related issue concerns the government agencies, including police, customs, transportation, and some other inspection agencies: who ensures, and how, that all of these agencies have deep enough expertise, perform their work to the highest standards, and without any links to criminal organizations or are not open to corruption etc.? (this could actually be closer to the original concerns of Plato cited earlier.).

CBRA research recommends both business and governmental communities consider carefully this issue whenever creating new SCS policies, standards, regulations and investments, in order to minimize the risk of guards becoming the enemy of SCS.

C9: Unnecessary gaps might be created with non-SCS standards

Two experts shared their views on the necessity to link any possible SCS standard development with other security standards and other management systems, in order to make the implementation and maintenance as fluent as possible. Expert E15 discussed learning from other security standards: *"You should look at not just transport and supply chain, but any security standard...we need to get to a point where all security standards are written same way...".* Expert E9 proposed to position any SCS standard development within a broader context of management standards and systems: *" Companies in the future have ten different management systems – we have to bring them together... you have to make specific systems, to meet specific needs... but when we establish specific systems, we have to see how these specific systems connect."* These views are considered at the report recommendations (Chapter 6).

C10: The enforcement and monitoring of a possible new SCS standard may become costly

[32] http://news.sky.com/skynews/Home/World-News/Bank-Heist-In-France-Security-Guard-At-Loomis-In-Lyon-Vanishes-With-10m-In-Armoured-Van/Article/200911115441624

Even though the auditing, certification, enforcement and monitoring procedures of a possible new SCS standard are out of the scope for this feasibility study, one expert (E11) shared his worries on this dimension of the whole standardization process: "*How are you going to enforce it? Is it going to be voluntary? ...problem with the AEO program, accreditation, on a 3-year cycle… who is going to pay, and to whom? ...Lloyds study tells us that accreditation cost, in Germany, is 14.000 Euros per company... What about tactical monitoring and strategic monitoring…. under existing CEN monitoring system…who says yes or no…quite a big task…"*. This concern is being partially addressed at the recommendations part (Chapter 6) of this report.

C11: Other arguments why a new European SCS standard might not be feasible

Finally, a handful of other arguments were shared by some experts to illustrate that no new European SCS standard might be feasible. First, expert E13 drew an analogy between the criminal legal system and SCS in Europe *"Every country has laws to make theft illegal, why would standards be better... and, criminal law has not been standardized – who thinks that SCS standard is more doable, when laws have not been harmonized..."*. Second, expert E11 was worried about jeopardizing the Treaty of Rome: *"We can't support a single market, Article 30, Treaty of Rome, free movements of goods and people and services...this (CEN SCS initiative) would imply that free movements of goods is not possible..."* And third, expert E1 had concerns about Vienna Convention between ISO and CEN: "*What I miss: you have lot of work going on in ISO – the interesting thing is the relation between ISO and CEN standard..."*. These are somewhat tricky arguments to deal with, but: (i) Maybe the lack of legal harmonization in Europe does not automatically lead to difficulties with "non-legal SCS standardization"? (ii) Maybe a business-driven SCS standard could support the 'spirit' of the Treaty of Rome (or future EU Treaties)? (iii) Maybe ISO and CEN could be complimentary when it comes to SCS standards?

Box 9 Dynamic behavior of the enemy

Security management in supply chains shares conceptual similarities with other support functions such as safety management, quality management, environmental management and even the management of corporate social responsibility. The conceptual similarities exist, in terms of problem prevention versus recovery (cost) optimization objectives – conceptually one should minimize the sum of the costs of incident prevention and recovery with any of these disciplines, while avoiding any over investments in these important – but, nevertheless, support functions.

How then does supply chain security (SCS) management differ from safety management and quality management etc.? In SCS the "enemy" – single criminals, criminal organizations, terrorist groups etc. – is a learning and (sometimes) an intelligent entity, which can adjust to the changing environment, looking for new crime opportunities, security obstacles, grey market demand and/or prices, criminal law updates etc. (Such "dynamic behavior" is obviously not the case with safety incidents/accidents and quality problems.)

Furthermore, this can have the following types of sample implications, making SCS standard development and SCS measurement even more challenging tasks:

- Once criminals learn about a new SCS standard established to protect certain entities in the supply chain (e.g. port facilities), they may shift their focus to another part of the supply chain (e.g. inland terminals).
- Whenever demand patterns and/or grey market prices e.g. for stolen goods change, criminals may shift their commodity focus (e.g. from cigarettes to mobile phones)
- If a criminal law changes by introducing harder punishments with one type of crime in supply chains (e.g. cargo theft), criminals may swap the crime type to one with more lenient punishments in case they are caught (e.g. IPR violations).

Based on the obvious dynamic nature of crime as the "enemy" of supply chains, the CBRA research team recommends more research focus in the future on criminology and criminal behavior, as well as frequent reviews of existing SCS standards and measures, on their strengths and weaknesses, in relation to actual crime patterns and risks.

3.6 Collection of all standard ideas shared during the interviews

The research team kept a very open mind when identifying and collecting ideas for possible SCS standards, during the expert interviews. The observed ideas are presented on two levels: first the actual standard ideas (S1 to S10 below) and second the relevant characteristics for one or more possible SCS standards. These ideas are to be tested further in the Operator survey (Chapter 5).

S1 (Standard-idea-1): SCS risk management and risk assessment

The first idea for a possible standard was proposed by expert E5, who stated: *"How to conduct a risk management...how to make the process of assessing and evaluating risks... what measures to accept, what to move etc... it would add value to existing programs...and become a basis for the whole exercise..."*

S2: SCS standard for companies who are not eligible for EU AEO, but still may need a "SCS label" for their business

The second idea was formulated by expert E12: *"... to help SMEs, who are not in position to become EU AEO or C-TPAT. SMEs which are sometimes dealing with the export market... this norm could be a minimum norm, to provide minimum standard, that they could show their customers, e.g. in the US... limited to pre-carriage to international port or airport, where goods are taken into charge by the big players... this segment is a weak point and could be covered by this norm... this analysis was done two years ago… the idea is still considered by many stakeholders... the minimum norm could help: e.g. asking for background checks; closed parking lots, etc..."*

S3: Security standard for "non –supply chain" companies

The third idea was presented by expert E10, who saw the issue of non-supply chain companies possibly becoming requested to have some "SCS label" in place in the future: *"3rd parties in supply chains – cleaning companies, security companies etc. – personnel screening is an issue..."*

S4: Standard for secure parking lots

The fourth idea on developing a standard around secure parking lots, a major topic in cargo crime, was hinted by a couple of experts, including E11: *"Secure parking lots is the major issue for us in fight against theft".*

S5: Standard for being able to operate during "high threat / high security" situations

The idea on having a "SCS label" which enables companies to operate supply chains during high threat / post incident situations – if they decide to invest up-front on such qualifications, was brought up by expert E5: *"...if you design a standard on mutual levels of threats; then whenever government changes the level, you have your equivalent security level... you need police and justice to work with you. CASE: one EU country increases threat level; company can react with higher security in that country; or a group of countries move for higher security..."*

S6: Good practices guidebook

A couple of experts were thinking about a need for a "SCS good practice" –guidebook, either as a standalone document, or linked to an existing SCS initiative. On the former, expert E5 shared the following note: *"When you do your comparison of existing programs...training and pre-screening in every program; but no one program how to do conduct pre-screening... make a standard on best practices on existing things".* And, on the latter aspect, expert E15 said that *"..there is already 28000, why rewrite, why not help ISO to improve... with a European implementation guidebook...".*

S7: A standard to verify whether companies in the supply chain are "legitimate"

This standard idea was stimulated by E11, who talked about following approach with the trucking sector in one EU country: *"...in our country, for truck drives you need a full license; (i) professional competence, (ii) good financial stand; (iii) and no court cases..."*

S8: A standard for crime incident reporting

This standard idea was hinted by expert E11, who explained about an existing commercial service for: *"...truck theft monitoring..."* – as this service also includes a component for the incident reporting. A second expert (E2) also shared views on existing crime incident reporting services.

S9: A standard for SCS service procurement

This standard idea was hinted by expert E6, who explained that: *"... there is a manual, which gives a buyer of security services some 60 security criteria, helping to make RFP and to evaluate bids..".*

S10: A standard for SCS training and awareness building

The relevance of training and awareness building with SCS was mentioned by couple of experts; and thus brought to as the tenth idea on the table for a possible new European SCS standard.

Other SCS standard characteristics brought up by the experts

Expert E9 saw targeting "normal crime" with a possible new SCS standard of high relevance: "... f*rom our point of view, interesting added value...if also delivers more security against normal crime.. it would become much more relevant for our members in daily work."*

Expert E12 highlighted toolbox dimension of the exercise: *"... the problem is: people consider norm as a regulation – instead of a toolbox..."*

Expert E5 emphasized the importance of mutual recognition between various SCS initiatives: *"Regarding SCS, the one-stop-shop, mutual recognition of programs is crucial... with EU AEO and regulated agent status..."*

Simplicity of any possible new SCS standard was a key for expert E10, who said that: *"... if a standard happens, we should keep it simple, minimum standard, this is the basic, if you want do business in supply chain, you can get stamp... we are dealing with small and big enterprises..."*

Linking with relevant non- SCS standards was pointed out by expert E1, using the new ISO standard for risk management as a sample: *"ISO31000 not published yet; coming on risk management, will be published*

after summer 2009 (the working group has finished)... this is a generic standard, risk management, will touch any standard with risk component..."

Creating a step-wise SCS standard system, like was done in the Swedish STAIRSEC-system, was shared by expert E6: "*One can think of different levels of security: level A = 5 measures; B = 7 measures etc... once you have complied with measures, you get an official stamp.. and everyone knows it is a secure part of the supply chain..."*

Finally, expert E9 considered the public-private-partnership –mentality relevant: *"...earlier we got engaged with police on normal criminal activities – which would have impact on security, focus on theft..."*

3.7 Summary and conclusions[33]

In this last sub-chapter of the Expert interviews section, the following two conclusions are made:

1. Any new SCS standard development should be considered within the framework presented here (See Figure 6 below).
2. The list of SCS standard ideas should be tested with a group of manufacturing, logistics and trade/retail companies, who actually operate the supply chains in Europe.

First, let's look at the SCS standards development framework, derived from the expert interviews, illustrated in Figure 6 below. The framework level choices to be explored in the upcoming parts of this feasibility study, and the conclusions to be drawn and reported (in Chapter 6), are the following nine:

1. Should a possible new SCS standard / family of standards (in the rest of the list: "new SCS standard" be rather risk based, or a level playing field based?
2. Should a new SCS standard have rather a regional focus or a global focus?
3. Should a new SCS standard rather focus on anti-crime activities or anti-terrorism activities?
4. Should a new SCS standard development be rather driven by the business community or by the governmental community?
5. On the business side, should a SCS standard development be rather driven by the supply chain operators themselves or by the security services and solutions sector?
6. Should a new SCS standard focus more on multi-modal and interconnectivity aspects of SCS, or more on single mode / single sector / single actor type aspects of SCS?
7. Should a new SCS standard focus on specific security and crime issues in supply chains or should it have a generic management system type of focus?
8. Should a new SCS standard have rather an inland focus in SCS, or rather a cross-border focus in SCS?
9. Should a new SCS standard rather go for a single level of security recognitions, or should it contain multiple levels?

[33] At this point, one additional standard idea was introduced by the research team: S11: A standard for crime indicators and forecasting. This idea is based on the preliminary work done for a European security research proposal, by the CBRA research team. The content for such a standard would consist of indicators one can observe and measure while anticipating future crime trends – one sample is a survey template to survey citizens how willing they are to buy stolen, counterfeit and/or smuggled goods (e.g. cigarettes).

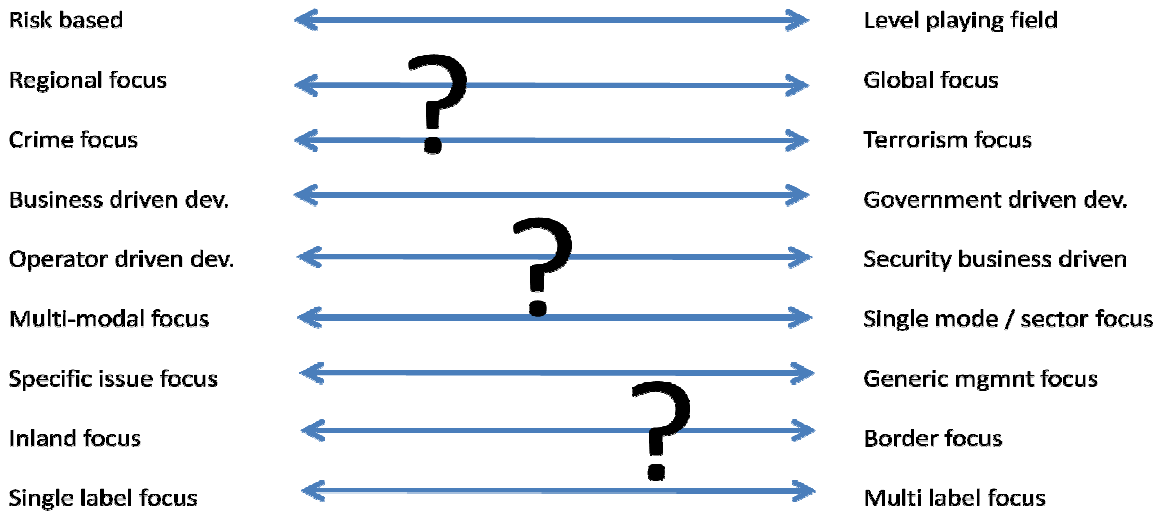

Figure 6 Framework for development of new SCS standards

And second, we list the ideas for possible new SCS standards shared by the experts, now as intuitively structured list, based on the type of business actors (logistics; all supply chain operators; non operators involved; and the criminal context targeted (”normal crime” vs. terrorism).

1. Supply chain security for any actors; covering all types of crime and terrorism
    - Risk management and risk assessment regarding crime and terrorism threats / hazards in supply chains
    - Supply chain security training and awareness building processes
    - Supply chain security – services procurement and/or services contract templates, with vocabulary
2. Supply chain security, focus on crime (mainly anti-theft), first two covering all actors, third specific for road carriers
    - Crime incident reporting standard, with reporting data model, process model etc.
    - Crime forecasting and crime indicators, with forecasting data model, process model etc.
    - Secure parking lot standards (only for road carriers)
3. Supply chain security, focus on anti-terrorism, first two one covering logistics actors, third one ”non-supply chain companies”
    - Supply chain security standard targeted from small and medium sized logistics companies who might be required to have some ”SCS label” to do business.
    - Supply chain security standard targeted for such logistics companies which aim to operate as soon as possible after a major incident and/or during a high alert situation.
    - Security standard targeted for other services (= non-logistics) companies – like office services; office supplies etc.
4. Supply chain security guidebooks
    - Supply chain security good practices guidebook
    - European implementation annex for ISO28000 Supply chain security series of standards

4 SCS initiative analysis

4.1 Introduction

The goal of this chapter is to take an in-depth look at a select set of supply chain security (SCS) initiatives, in order to understand how they are really meant to work. Previous analysis presented in the literature typically focuses on security measure check list -reviews, including statistics on which programs make references to fences, CCTVs, guards etc., thus lacking deeper understanding on the actual design and dynamics of these programs.

This in-depth SCS initiative analysis, the first of its kind[34], aims to provide answers to the following types of questions regarding supply chain security coverage, design, dynamics, theoretical grounds etc.:

- Which supply chain actor types are linked to which SCS initiatives?
- Which security areas such as facility, cargo and human resource security, are covered, and to which degree, by the SCS initiatives?
- Which phases in security management – crime prevention, crime detection; recovery from incidents of crime – are covered, and to which extent, by the SCS initiatives?
- How are the continuous improvement cycle steps – plan, do, check, act – taken into consideration by the SCS initiatives?
- How are the principles of situational crime prevention theories covered by the SCS initiatives?
- How are the existing national and European level security norms taken into consideration with the SCS initiatives?

The rest of this chapter has the following structure:

- Chapter 4.2 presents and justifies the five chosen SCS initiatives;
- Chapter 4.3 introduces the six chosen analysis methods;
- Chapter 4.4 – Chapter 4.9 present the actual analysis done, with some conclusions; and
- Chapter 4.10 draws the final conclusions for this exercise.

4.2 Overview of the five SCS initiatives

Based on the priorities expressed during the expert interviews (Chapter 3), five SCS initiatives with high European relevance were chosen for this in-depth analysis:

- EU AEO, EU Authorized Economic Operator
- ISO 28000 series, International Standards Organization, Security Management Systems for the Supply Chain
- TAPA, Transported Asset Protection Association, Freight Suppliers Minimum Security Requirements
- IRU, International Road Union, Road Transport Security Guidelines
- EU Port security directive.

In the coming five boxes, the following four details are presented per organization and initiative:

[34] CBRA research team is not aware of any previous study which would have taken a similar approach.

- Organization behind the initiative
- Mission / vision of the organization
- Purpose of the initiative, and
- Scope of the initiative.

The information provided is based on one or more websites per initiative, as indicated in the footnotes.

4.2.1 European Union Authorized Economic Operator (EU AEO)

Box 10 EU AEO [35]

Organization behind the initiative:
European parliament and European Council establishing legislation based on which the European Commission (Directorate General for European Commission Taxation and Customs Union, DG TAXUD) in cooperation with EU Member States have developed Guidelines for AEO in 2007.

Mission / vision of the organization:
Mission of EC DG TAXUD is to develop and manage the EU Customs Union, a foundation of the European Union, and to develop and implement tax policy across the EU for the benefit of citizens, businesses and the EU Member States. Particular attention is given to the Internal Market, by making sure it functions smoothly and efficiently.

Purpose of the initiative:
Provide a voluntary priority custom handling status for business (AEO status) when fulfilling the requirements of the so-called security amendment to the Community Customs Code, i.e. providing amongst other for the creation of an Authorized Economic Operator (AEO). The legislation stipulates that customs authorities shall grant to reliable traders that are established in the European Community the status of AEO. EU AEO guidelines should be drawn up for both customs authorities and economic operators to ensure common understanding and uniform application of the new customs legislation related to the AEO concept, and to guarantee transparency and an equal treatment of economic operators.

Scope of the initiative:
A legal person who, in the course of his business, is involved in activities covered by customs legislation can apply for status of AEO.

4.2.2 ISO 28000 series, International Standards Organization, Security Management Systems for the Supply Chain

Box 11 ISO 28000 series[36]

Organization behind the initiative:
The International Organization for Standardization (ISO) is a worldwide federation of national standards bodies.

Mission / vision of the organization:
ISO's international standards and deliverables support: facilitation of global trade, improvement of quality, safety and security, environmental and customer protection, as well as the rational use of natural resources, global dissemination of technologies and good practices, all of which contribute to economic and social progress.

[35] Following web sites were used as main sources:
http://ec.europa.eu/taxation_customs/resources/documents/common/about/welcome/mission_statement_en.pdf, and
http://ec.europa.eu/taxation_customs/customs/policy_issues/customs_security/aeo/index_en.htm
[36] http://www.iso.org/iso/pressrelease.htm?refid=Ref1086

Purpose of the initiative:
The **ISO 28000 series** of standards on supply chain security management systems aim to help to reduce risks to people and cargo within the supply chain. The standards address potential security issues at all stages of the supply process, thus targeting threats such as terrorism, fraud and piracy.

The following standards have been recently published:

- ISO 28000:2007, Specification for security management systems for the supply chain;
- ISO 28001:2007, Security management systems for the supply chain – Best practices for implementing supply chain security – Assessments and plans – Requirements and guidance;
- ISO 28003:2007, Security management systems for the supply chain – Requirements for bodies providing audit and certification of supply chain security management systems;
- ISO 28004:2007, Security management systems for the supply chain – Guidelines for the implementation of ISO 28000.

Scope of the initiative:
ISO 28000 series standards can be applied by organizations of all sizes involved in manufacturing, service, storage or transportation by air, rail, road and sea at any stage of the production or supply process.

4.2.3 TAPA, Transported Asset Protection Association, Freight Suppliers Minimum Security Requirements (FSR 2009)

Box 12 TAPA[37]

Organization behind initiative:
The Transported Asset Protection Association (TAPA) is a forum that unites global manufacturers, logistics providers, freight carriers, law enforcement agencies, and other stakeholders with the common aim of reducing losses from international supply chains.

Mission / vision of the organization:
To establish and maintain best practice asset protection for industry and related logistics and freight service providers. TAPA effects the reduction of losses in the manufacture, transportation and distribution of high value products.

Purpose of the initiative:
Provide workable solutions for issues that are experienced industry-wide by member companies. This includes sharing experience and processes that are not proprietary to member companies, improving overall security effectiveness in targeted areas and incorporating these processes across the industry to reduce losses due to theft. TSR are a set of industry standards for Truck Security. FSR 2009 is a qualitative standard of best practices that enable different levels of classification according to threat levels. They were established to ensure the safe and secure in-transit storage and warehousing of any TAPA members' assets throughout the world. The standard outlines the process and specification for suppliers to attain TAPA certification for their facilities and transit operations.

Scope of the initiative:
The TAPA TSR and FSR 2009 shall apply to all geographical areas, and all relevant logistics services provided.

4.2.4 IRU, International Road Union, Road Transport Security Guidelines

Box 13 IRU[38]

Organization behind initiative:
The IRU (International Road Union), through its national associations, represents the entire road transport industry world-wide.

[37] The primary source for the information is the website of TAPA , http://www.tapaemea.com/public/
[38] The primary source for the information is the website of IRU , http://www.iru.org/

Mission / vision of the organization:
By working for the highest professional standards, the IRU improves the safety record and environmental performance of road transport and ensures the mobility of people and goods.

Purpose of the initiative:
The IRU Road Transport Security Guidelines (2004/2005) are a set of detailed recommendations for Managers of road transport companies, Drivers, Shippers/Consignors and Companies transporting Dangerous Goods by Road on improving security in day-to-day operations. They contain practical tips to strengthen security against terrorist and other criminal threats. The objective is to raise security awareness and suggest preventive measures to minimize risk of theft or misuse of goods or vehicles for terrorist purposes.

Scope of the initiative:
Road transport operators.

4.2.5 EU Port security directive

Box 14 EU Port Directive[39]

Organization behind initiative:
The European Parliament and Council of the European Union.

Mission / vision of the organization:
The European Parliament and Council are the two only deciding institutions for EU wide legislation. They represent a major impetus in defining the general political guidelines of the European Union.

Purpose of the initiative:
The main objective of the Directive is to introduce a security system in all port areas. With a view to realizing this objective, the Directive is aimed at establishing a port area based EU framework to guarantee a high and comparable level of security in all European ports. This Directive thus complements the EC regulation on enhancing vessel and port facility security of 31 March 2004, establishing am EU ship and port facility security system in line with the amendments of the SOLAS (Safety of Life at Sea) Convention and the ISPS (International Ship and Port facility Security) Code. Taken together, therefore, the Directive on port security and the Regulation on ship and port facility security provide the necessary framework for protecting the whole chain of maritime transport logistics (from the ship to the port via the ship/port interface and the whole port area) against the risk of attacks on Community territory.

Scope of the initiative:
The Directive applies to people, infrastructure and equipment (including means of transport) in ports and adjacent areas.

Regarding these five SCS initiatives, the following specific documents and sections were used throughout the analysis:

1. EU AEO: based on Regulation EC No 648/2005 of 13 April 2005 amending Council Regulation No 2913/92 establishing the Community Customs Code. Based on the EU legislation non binding EU AEO Guidelines were established containing Section 5 Safety and Security (dated 1.7.2007, pages 20-40) Authorized Economic Operators Guidelines (29.6.2007, 82 pages) Part 2, I.2.5 Section V Safety and security requirements (pages 58 – 74) with 64 requirements, is to be covered in the analysis.

[39] The primary sources for the information are the website of http://europa.eu/legislation_summaries/transport/waterborne_transport/l24162_en.htm and http://www.parliament.uk/commons/lib/research/briefings/snbt-03106.pdf

2. ISO 28000 series: ISO28001 - Security management systems for the supply chain — Best practices for implementing supply chain security, assessments and plans — Requirements and guidance (10.15.2007, 28 pages). Table A, Performance review list (pages 12-14) with 31 requirements, is to be scrutinized in the study.
3. TAPA: Freight Suppliers Minimum Security Requirements (1.1.2009, 19 pages). Section 2 – Specifications (pages 11 – 18), with 79 requirements, is to be included in the analysis.
4. IRU: Road Transport Security Guidelines (2005, 45 pages) Chapter 3: Recommendations for shippers/consignors (pages 22–25), with 53 requirements, is to be covered in the study.
5. EU Port security directive, Directive 2005/65/EC of 26 October 2005 on enhancing port security (OJ 25.11.2005, 12 pages). Annex II Port Security Plan (pages 9 - 10) with 16 requirements, is scrutinized in the study.

4.3 Overview of the six step analysis -approach

In order to produce a comprehensive analysis of the security approaches of the five SCS initiatives, the research team developed a six-step analysis method. Each step of the analysis is explained and motivated below; and the whole approach is visualized in Figure 8 at the end of this sub-chapter.

Analysis-1: Supply chain actor types

The first analysis looks simply at the supply chain actor type –coverage of each of the five SCS initiatives. The three main groups for the supply chain actors are: (i) trade / retail / wholesale; (ii) shippers / manufacturers; and (iii) logistics companies: freight forwarders, carriers, warehouse keepers etc. (see the detailed list of logistics actors in Figure 8 below, six pages after this one). This list of supply chain actors has been derived from the literature, and is being used also in the supply chain operator survey (Chapter 5).

This analysis is done on SCS initiative level, instead of requirement level analysis (as is the case for the following three analysis steps). The mapping between the supply chain actors and the initiatives is primarily based on SCS initiative documentations, i.e. how they explain the target group for each initiative. In unclear cases details are verified with external experts.

By carrying out this analysis we gain understanding which actors are most covered by these five SCS initiatives, and whether any actor-specific gaps exist within these five SCS initiatives.

Analysis-2. Supply chain security framework

The second analysis approach has been derived from the study by Gutierrez and Hintsa (2006), which developed a five group model of supply chain security measures introduced in ten different voluntary supply chain security programs[40] .

[40] The paper by Gutierrez and Hintsa (2006) is based on ten voluntary SCS program documentation of summer 2005.

For this study, the first four groups are used as originally defined by Gutierrez and Hintsa (2006):

1. Facility management: Guaranteeing the security of the facilities where cargo is stored and handled or cargo related information handled.
2. Cargo management: Protecting cargo during all steps of shipping and transport processes.
3. Human resources management: Guaranteeing trustworthiness and security awareness of all personnel in direct and indirect contact with cargo and other company assets.
4. Information management: Protecting critical business data and exploiting information as tool for detecting illegal activities and preventing security breaches.

Regarding the fifth area, the reference to ”Management systems” was dropped, shifting the focus purely on ”Business network”:

5. Business network: Managing security upstream and/or downstream in the supply chain, with suppliers, service providers, and/or customers.

To be complete, the CBRA research team also added two more security areas, as part of a holistic SCS framework analysis:

6. Risk management: Recognizing and analyzing crime threats, vulnerabilities in the supply chain, security incident likelihoods and consequences, reducing risks to an acceptable level.
7. Disaster recovery: Preparing oneself for a fast (and cost efficient) recovery after security related incidents, getting the supply chain back to normal level in a minimum time.

This analysis is done on security requirement level for each of the five SCS initiatives, i.e. each requirement / question / sentence or paragraph is analyzed separately. Many security requirements fall into multiple areas, which is addressed during the analysis.[41]

By carrying out this analysis we gain a good understanding of how well (or poorly) these seven security areas in this SCS framework are covered by the five SCS initiatives – and if any gaps exist.

Analysis-3: Security phase

The third analysis step called Security phase, has a somewhat less explicit backing in the literature – however, the CBRA research team finds it a highly relevant dimension of analyzing and/or designing supply chain security standards. The research team fixed the following three-phase scheme for this analysis:

1. Prevent: Security measures and activities which have the primary goal of preventing crime incidents from happening.
2. Detect / react: Security measures and activities which have the primary goal of helping to identify, even in real time, or near real time, when crime incidents have taken place, in order to support solving the situation, as fast and at as low a cost as possible.
3. Recover: Security measures and activities which have the primary goal of helping businesses to get back to normal operations.

[41] The mapping is based purely on the CBRA research team understanding of the security requirements.

One related presentation was given recently by a EC DG Enterprise officer Mr. Khoen Liem (2009), who talked about "building up capabilities related to the phases of a security incident", with following six phases: (i) Identify (incident related); (ii) Prevent (threat related); (iii) Protect (target related); (iv) Prepare (operation related); (v) Respond (crisis related); and (vi) Recover (consequence related).[42] However, this format is very much prepared for "major incidents" such as terrorism, which form only a limited part of this feasibility study – thus, the simplified three-phase scheme makes sense here.

The analysis is done again on security requirement level, i.e. "row-level".[43] In case a requirement covers more than one of the phases, they are all identified during the analysis.[44]

By carrying out this analysis we gain a good understanding on how well (or poorly) these three security phases are covered by the five SCS initiatives – and if any gaps exist.

Analysis-4: Continuous improvement cycle

The fourth analysis step is the cycle of continuous improvement which is also known as the Deming cycle. This analysis step has strong basis especially in quality control literature. In the Deming cycle improvements are achieved by carrying out Planning, Doing, Checking and Acting tasks consecutively in an infinite cycle (PDCA). These sequential steps create basis for the continuous improvement cycle. As the continuous improvement cycle has been successfully established, performance is likely to improve constantly. On the other hand, if there is a lack of continuous improvement the performance stagnates or even decays. Deployment of the cycle of continuous improvement is crucial when company's security system must be up-dated constantly.

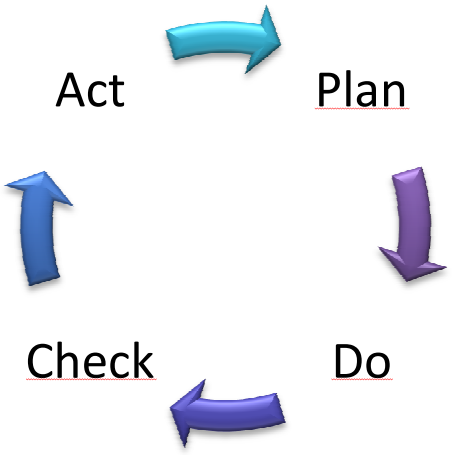

Figure 7 The PDCA-cycle

In in-depth analysis all five selected standards are scrutinized in order to evaluate how continuous improvement has been taken into consideration. Definitions for each cycle steps:

1. Plan: Design or revise procedures to improve results. Arrange proper measurement methods.

[42] Speech at the UNECE Inland Transport Security seminar, Geneva, 15 January 2009.
[43] The mapping is based purely on the CBRA research team understanding of the security requirements.
[44] One could of course argue that any security measure and activity, if made known to the potential criminals, could always contribute in the Prevent phase

2. Do: Execute the plan and measure performance
3. Check: Evaluate the measurements and transmit the result information to organization
4. Act: Evaluate measurement system and implement required improvements

This analysis is done on security requirement level for each of the five SCS initiatives, i.e. each requirement / question / sentence or paragraph is analyzed separately. One requirement can fall only in one cycle step category.

Continuous improvement analysis gives us a good understanding of how well (or poorly) four cycle steps are covered by the five SCS initiatives.

Analysis-5: Situational crime prevention

The fifth step in this in-depth analysis process in based on situational crime prevention theories, applied to supply chain environment. The prerequisite for all supply chain crime is the opportunity to affect material, information or people flows. In dynamic supply chains material, product and people flows change rapidly, thus crime opportunities emerge and change in time and space. Compared to the many other processes in society there is a fundamental difference - supply chains are substantially more predictable and controllable. Supply chain management brings new prevention methods alongside traditional physical security to protect supply chains: supply chain planning and design, product planning and design and extended information security. All these methods are based on practicable situational crime prevention theories*, which enable systematic mitigation of crime opportunities in the supply chain.*

This analysis consists of following four steps, derived from crime prevention literature – briefly explained after the list:

1. Supply chain (re)design: sourcing points, transport modes and routes, business partners etc.
2. Extended information protection: visible information on shipments, data system protection etc.
3. Physical security: prevent access to targets by guards, gates, alarm systems etc.
4. Crime reward decrease: product design and planning, postponement strategies, pin-codes etc.

1. Supply chain (re)design: Supply chain structure planning and design can affect the opportunities for crime. Management can decide for example to avoid dangerous supply routes and points of time; to work only with SCS certified suppliers and business partners, etc.

2. Extended information protection: Information related to the possible criminal targets, transport routes or warehouse facilities plays a key role in supply chain crime. If there is no exposure to transported products and related information is secured, there is no risk for theft, pilferage. Respectively if there is no information available of transport routes and schedules, there is no possibility to exploit the transportation system for illegal products. Furthermore, regularity and predictability of transportation routes and schedules increase the risk of crime. By making cargo related information 'invisible' through prevention of unauthorized access to both supply chain management systems and cargo handling areas, supply chain crimes can be undercut.

3. Physical security: A traditional way to prevent access to the targets. Access refers to physical barriers and surveillance. The easy access to targets can substantially increase crime rates without increase of

perpetrators or their motivation. The most valuable factor in the routine activity theory underlies in an insight - supply chain and logistics management has an influence on how possible offenders get access to targets without surveillance.

4. Crime reward decrease: An offender must assess the target to be valuable, thus there must be demand and market for the target objects. Demand takes into consideration the cost of the goods in question, the ease with which they can be resold, and the number of potential buyers (Factory mutual, 2000). By product planning and design, value and usability of transported products can be changed. Postponement strategies offer opportunity to add market dependent parts, programs or packages at the back-end of the supply chain. If operation applications or activation codes are not included until the points of sale, products stolen earlier in the chain are difficult to resell. By product design crime rewards can be decreased and offenders can be discouraged to commit a crime.

This analysis is done on security requirement level for each of the five SCS initiatives, i.e. each requirement / question / sentence or paragraph is analyzed separately. However, due to the novelty nature of this analysis approach (within supply chain context), only couple of sample findings are reported in this chapter.

Situational crime prevention analysis gives us a first understanding on how well (or poorly) crime prevention theories have been considered as part of SCS program design.

Analysis-6: Existing European security norms

This is the sixth and the last step of the in-depth SCS initiative analysis. Based on a working paper by the CBRA research team (Ahokas J. 2009)[45], the following five supply chain security-related areas have been pre-identified to contain possible explicit or implicit links with the existing SCS initiatives:

1. Physical security: building hardware, windows, doors, shutters, glass in building, secure storage units, guidelines for security of buildings against crime;
2. Access control and alarm systems: access control systems for use in security applications, intrusion and hold-up systems, intrusion systems - power supplies, intrusion systems - application guidelines;
3. CCTV systems: management and operation - code of practice, installation and remote monitoring of detector activated CCTV systems – code of practice, CCTV surveillance systems for use in security applications - system requirements & application guidelines, code of practice for digital CCTV recording systems for the purpose of image export to be used as evidence;
4. Security service providers: terminology, static site guarding and mobile patrol service – code of practice
5. Security screening: security screening of individuals employed in a security environment – code of practice

By carrying out this analysis we understand whether any explicit links exist between the variety of European security related norms, and the five SCS initiatives.

[45] Ahokas J. has a solid background in anti-crime activities in the insurance sector – thus he is intimately familiar with security related technical norms in Europe.

Finally, all the six analysis methods[46], with their essential content, are illustrated in Figure 8 below.[47]

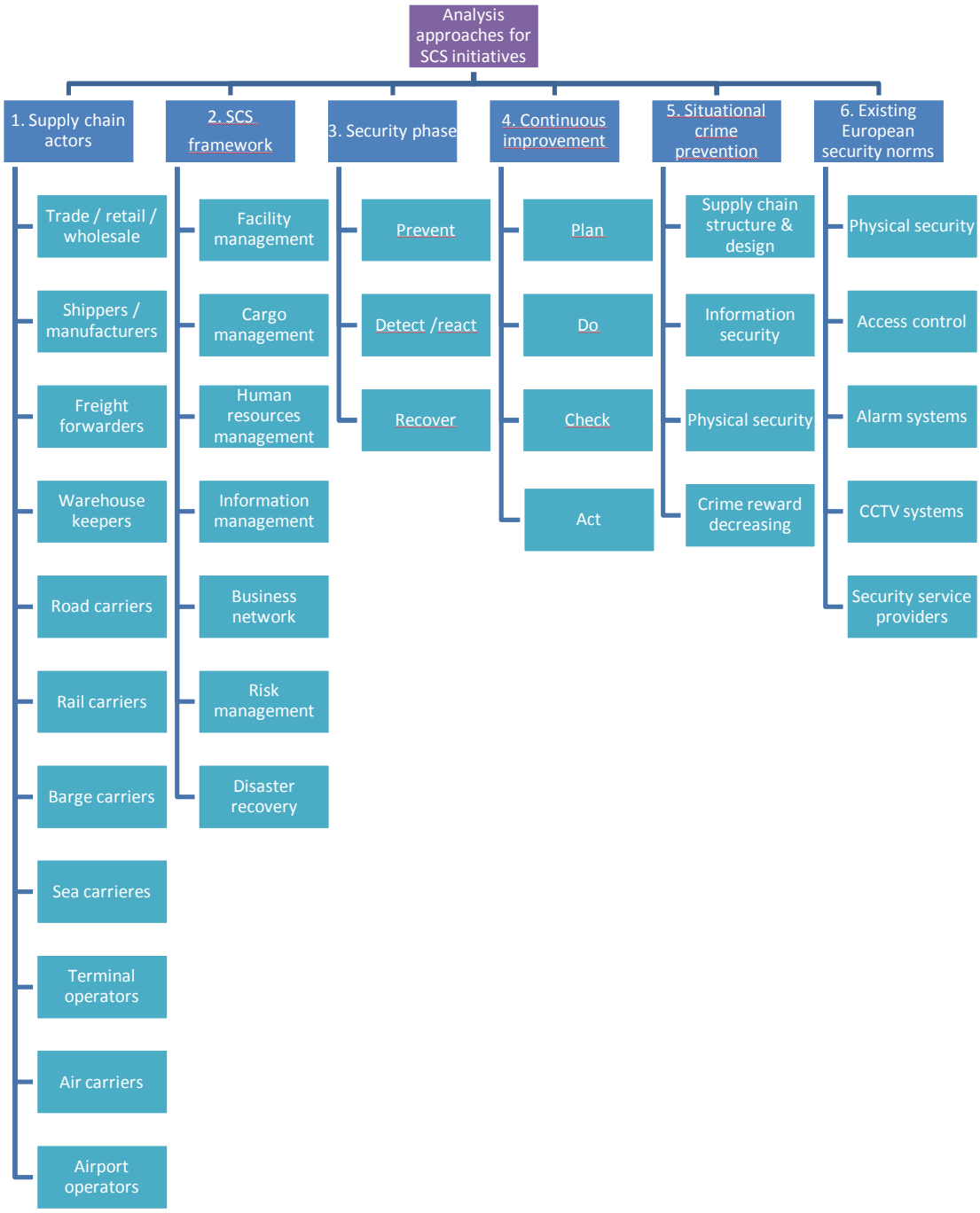

Figure 8 The six-step SCS initiative analysis methodology (copyright: CBRA 2009-2010)

[46]This 6-step analysis methodology is to be included in a planned journal paper: Hintsa J., Ahokas J., Männistö T., Sahlstedt J.(2010), Value Chain Security (VCS) Management, Journal tbd.

[47] Even though some of the details inside the six analysis approaches appear to be similar – e.g. Disaster recovery in SCS framework, and Recover in Security phase ; or Information management in SCS framework, and Information security in Situational crime prevention – they are all treated as independent steps in this study. (for future analysis purposes, the CBRA research team is working on an "integrated SCS analysis methodology", which will eliminate any possible overlapping steps – most likely placing Situational crime prevention in the center of the analysis methodology).

4.4 Supply chain actors involved per SCS initiative

First, the research team carried out an analysis looking at which supply chain actors typically can comply / do comply with the five SCS initiatives; the results are summarized in Table 2 below.

Initiatives can be roughly divided in two groups distinguished according supply chain or operator focus. EU AEO and ISO represent supply chain focus and IRU, TAPA and Port security represent operator focus.

The concept of EU AEO –Security and safety focuses closely on supply chain management and is not restricted to single transport modes. However, EU AEO has the requirement of ´customs transactions´, which can in practical terms leave whole actor types out of the program (e.g. sea barges) – and of course, individual companies in any of the sectors, who do not have these transactions would not be eligible.

ISO 28001 aspires to improve supply chain security processes independent of transport mode, and, the standard is meant to apply to all supply chain operators.

TAPA aims at ensuring safe and secure in-transit storage and warehousing, especially focusing on preventing loss of cargo for shippers and manufacturers. Currently, TAPA requirements focus mainly on security of road transport between warehouses and warehouse facilities itself (TSR, Truck Safety Requirements). TAPA is working on an air cargo security standard. From multimodal transport approach, the interconnectivity between trucks and other transport modes is covered.

The IRU Road Transport Security Guidelines are a set of recommendations to improve road security in day-to-day logistics operations, providing also security tips to other actors, including shippers.

The port security directive introduces a security management system in all EU port areas. The port security is focused on port operators and shipping companies. It also covers other operators when executing activities within the dedicated port areas.

Table 2 Matching various supply chain actors with the five SCS initiatives[48]

x = direct participation	EU AEO	ISO28001	IRU	TAPA	EU Port security directive
Notes	*Any actor with customs transactions can apply for EU AEO*	*Any company in the supply chain can implement*	*o = these actors can be involved / impacted*	*o = these actors can be involved / impacted*	*o = these actors can be involved / impacted*
Retail / wholesale	x	x		o	
Shippers / manufacturers	x	x	x	x	o
Warehouse keepers	x	x	x	x	o
Road carriers	x	x	x	x	o
Rail carriers	x	x	o	o	o
Multimodal carriers	x	x	o	o	o
Barge carriers	x	x	o	o	o
Sea carriers	x	x		o	x
Sea port operators	x	x		o	x
Air carriers	x	x		o	
Airport operator	x	x		o	

[48] The data on this table is based on estimates by the research team; it has not been validated by the parties behind the five initiatives.

4.5 Supply chain security framework

Secondly, the research team carried out an analysis looking at which relevant supply chain security aspects have been considered in these five SCS initiatives. The analysis is based on documents of the initiatives. In unclear situations details were verified with relevant experts. Next we show some illustrative examples of requirement categorization:

Facility management:

- ISO: "Are procedures in place to restrict, detect, and report unauthorized access to all shipping, loading dock areas and closed cargo transport unit storage?"
- EU Port Directive: "Access requirements. For some areas, requirements will only enter into force when security levels exceed minimal thresholds. All requirements and thresholds will be comprehensively included in the port security plan"

Cargo management:

- ISO: "Are procedures in place to ensure the integrity of the goods/cargo when the goods/cargo are delivered to another organization (transportation provider, consolidation centre, intermodal facility, etc.) in the supply chain?"
- IRU: "Seals should be placed by the shipper at departure, in the presence of the driver – never by the driver. Include the seal number in the transport documents and have the consignment note co-signed by both the shipper and the driver. Verify that seals, the load unit and packaging have not been interfered with at each load break. Companies should change their seals every three months - shape, color - to prevent counterfeit seals being made."
- EU AEO: "The integrity of cargo units should be ensured by placing them under permanent monitoring or keeping them in a safe, locked area."

Information management:

- EU AEO: "What security requirements have you placed on your trade partners and other contacts handling sensitive information provided by you?
- TAPA: "Destination to notify origin within 4 hours of receipt of shipment, reconciling pre-alert shipment details."
- ISO: "Is relevant data protected through use of storage systems not contingent on the operation of the primary data handling system (is there a data back up process in place)?"

Human resource management:

- TAPA: "Termination procedures in place for employees and contractors, ensuring return of IDs, access cards, keys and other sensitive information."
- EU Port Directive: "Based on those general aspects, the port security plan will attribute tasks and specify work plans in the following fields: […] Training and exercise requirements"

Business network management:

- EU AEO: "Does your insurance company impose security requirements on you? Have your customers imposed security arrangements on you?"
- IRU: "Share information and experience in preventive security measures with your regular transport providers."

Disaster management:

- TAPA: "Un-interrupted Power Supply (UPS) in place to ensure all electronic systems are able to function, even during power loss scenario."
- EU AEO: "Procedures should be in place when discrepancies and/or irregularities are discovered."

Risk management:

- IRU: "Carry out a detailed audit of company internal procedures, especially for threat/theft prevention."
- ISO: "Are processes in place to track changes in threat levels along transport routes?"

Next, we present the outcomes of the in-depth analysis, where each security requirement from the five SCS initiatives was analyzed and linked to one or more SCS framework groups. The results are presented in two diagrams below: the first one, Figure 9, shows inside each SCS initiative (on the x-axis) the percentage of each of the seven groups (on the y-axis); e.g. in ISO the human resource security requirements are present on around 45% of the requirements.[49]

[49] The total percentage when summing up all the seven bars per SCS initiative goes over 100%, as many of the SCS requirements can be linked to more than one of the SCS framework groups.

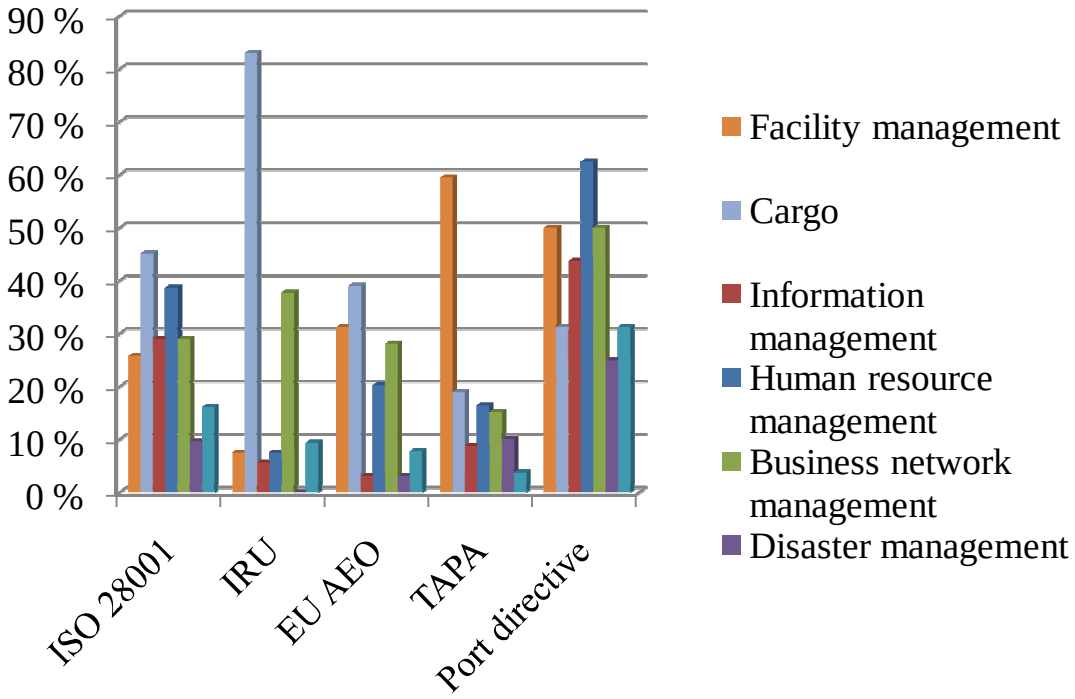

Figure 9 Percentage of SCS frame work groups

The second graph, Figure 10, shows per SCS framework group item (on x-axis) the total number of SCS requirements, broken down per SCS initiative (on y-axis); e.g. facility security has a total of around 100 references in these five SCS initiatives.[50]

[50] The total number of requirements, when summing up the numbers with the seven bars, goes much higher than the actual total number of requirements in the five SCS initiatives; this is due to the fact that one requirement often falls into two or even more SCS framework groups (just like in the previous graph, which is built on the same data as this one).

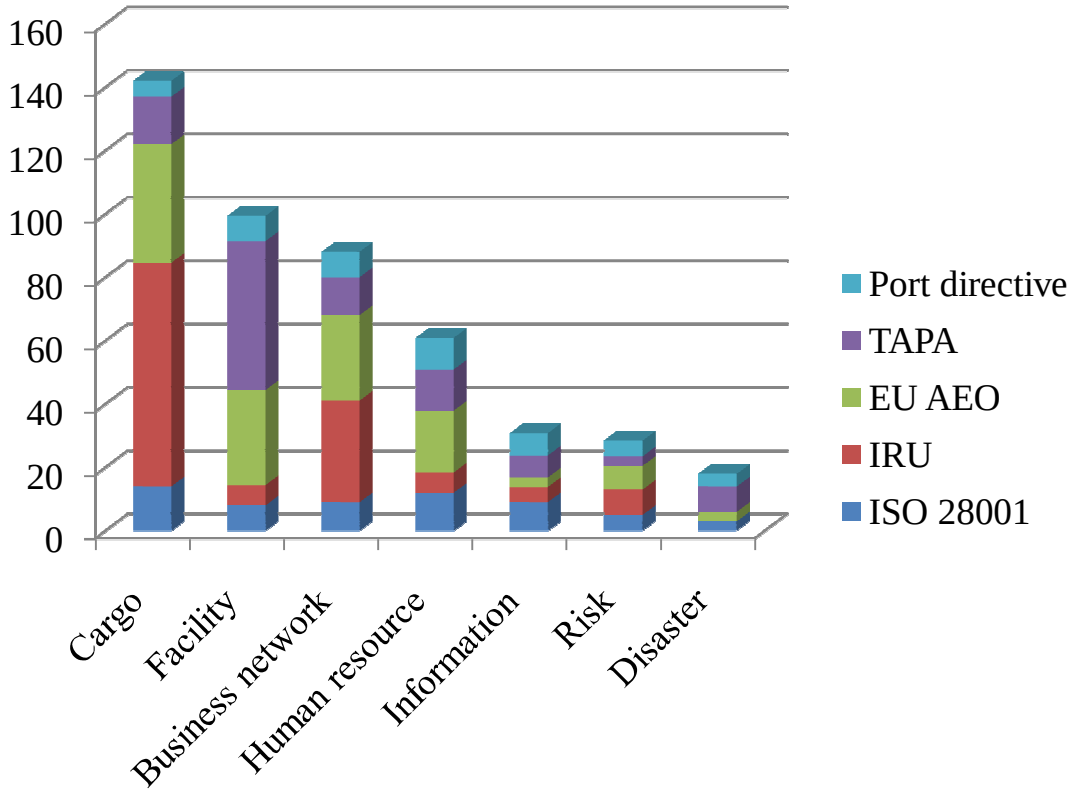

Figure 10 Number of requirements which can be categorized in certain SCS group

Based on the two diagrams above, the following immediate observations can be made:

- All five initiatives contain at least some measures from all seven groups[51]
- Two of the initiatives appear to have a bias towards one specific SCS measure – IRU to cargo, and TAPA to facility.[52]
- Cargo security requirements are most common with this set of the five SCS initiatives, followed by facility, business network and human resource security.
- The three least common security requirements are disaster recovery, risk management and information security.

[51] Just one exception, with IRU and disaster management.
[52] This is quite logical, taking into consideration the set-up of IRU and TAPA.

4.6 Security phase

Third, the research team carried out an analysis considering the security phase of requirements. Samples of requirement categorization include the following:

Prevent:

- IRU: "Limit access to loading areas and, if possible, provide several loading zones, each isolated from the others, and from the rest of the company premises."
- ISO: "Does the organization have procedures to evaluate the integrity of employees prior to employment and periodically relative to their security duties?"

Detect/react:

- EU AEO: "Where appropriate, the applicant should establish routines to weigh and tally outgoing goods."
- ISO: "Are procedures in place for notifying appropriate law enforcement in cases where anomalies or illegal activities are detected or suspected by the organization?"
- EU AEO: "At reception of the goods, the integrity of seals should be checked. Where relevant the applicant should have routines to seal incoming goods."

Recover:

- ISO: "Does organization have crisis management, business continuity, and security recovery plan?"
- EU AEO: "Procedures should be in place when discrepancies and/or irregularities are discovered."
- EU Port directive: "Based on those general aspects, the port security plan will attribute tasks and specify work plans in the following fields: […] The plan will detail interaction and coordination with other response and emergency plans. Where necessary conflicts and shortcomings will be resolved"

Next, we present the outcomes of the in-depth analysis, where each security requirement from the five SCS initiatives was analyzed and linked to one or more SCS of the three security phases. The results are presented in two diagrams below: the first one, Figure 11, shows inside each SCS initiative (on the x-axis) the percentage of each of the three phases (on the y-axis); e.g. in EU AEO almost 50% of the requirements have some kind of detect/react link.[53]

[53] The total percentage when summing up all the three bars per SCS initiative goes over 100%, as many of the SCS requirements can be linked to more than one of the security phases.

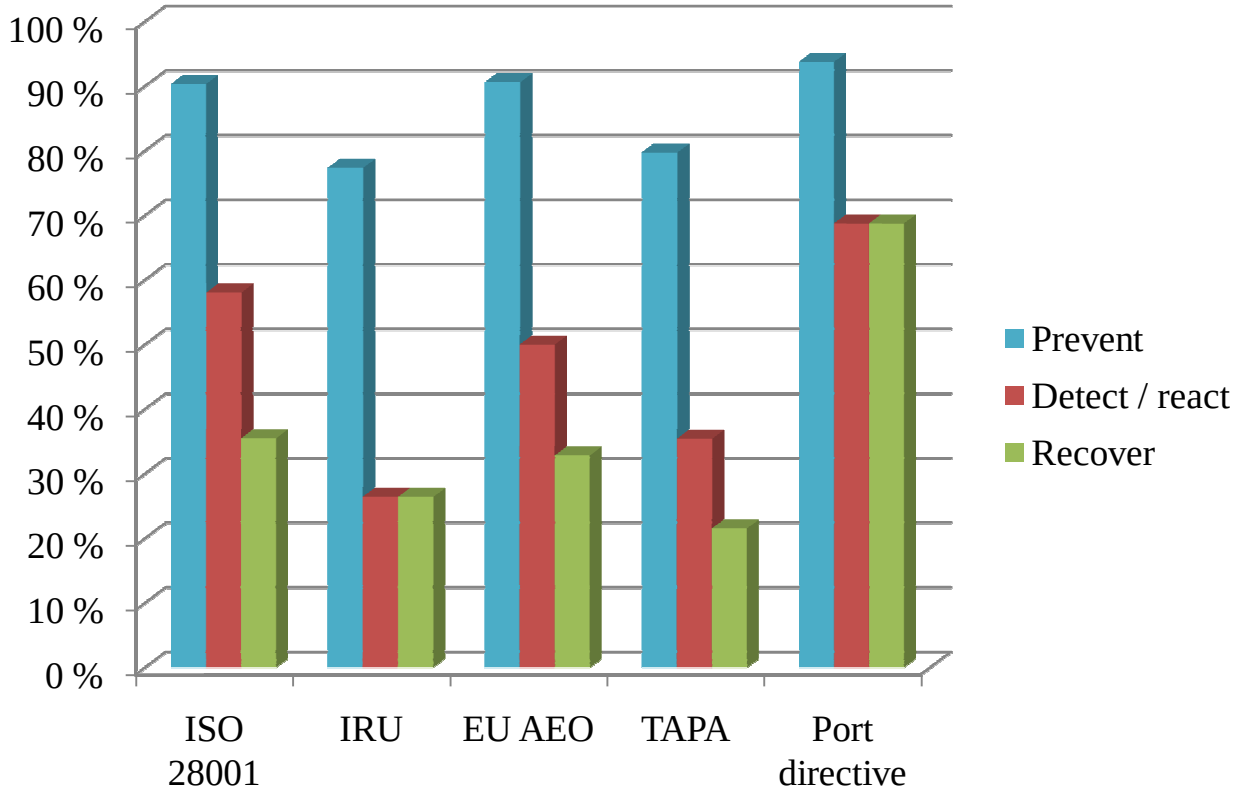

Figure 11 Percentage of security phase requirements

The second graph, Figure 12, shows per security phase (on x-axis) the total number of SCS requirements, broken down per SCS initiative (on y-axis); e.g. recover-phase has totally bit under 100 links with the SCS requirements.[54]

[54] The total number of requirements, when summing up the numbers with the three bars, goes higher than the actual total number of requirements in the five SCS initiatives; this is due to the fact that one requirement may fall into two or even three security phases (just like in the previous graph, which is built on the same data as this one).

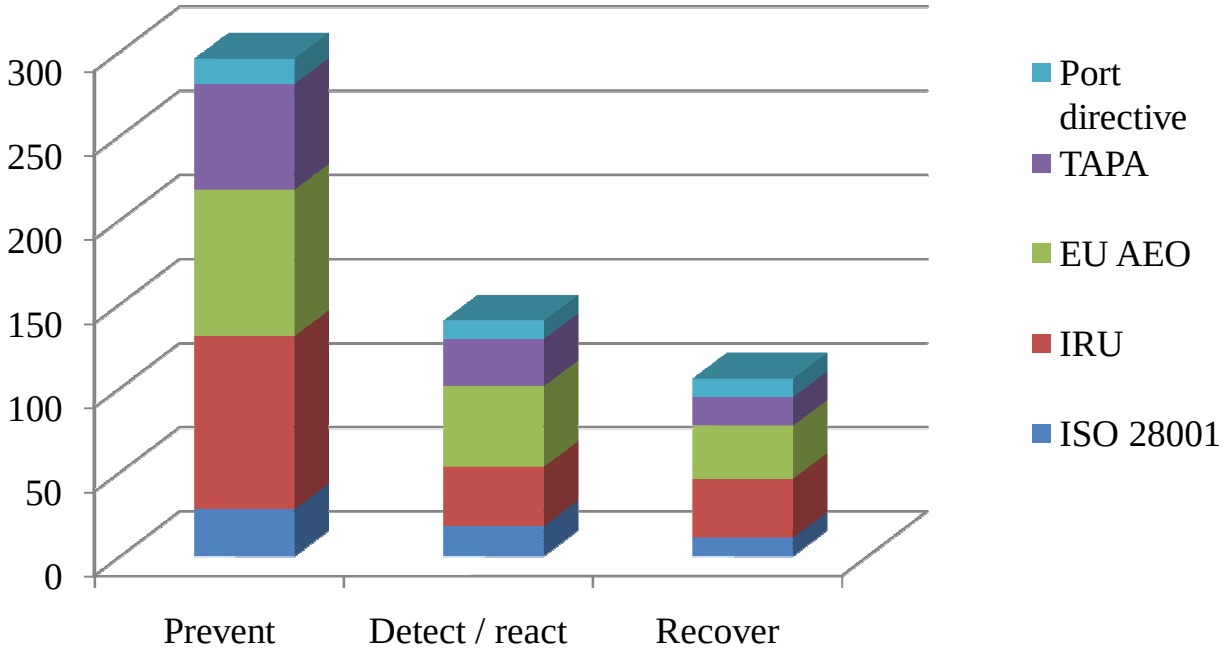

Figure 12 Number of requirements which can be categorized in a certain security phase

The following immediate observations can be made, based on the two diagrams above:

- Preventive measures are dominant in each SCS initiative.
- Detect/react and recover measures are still present in each initiative.
- ISO, EU AEO and TAPA have very similar overall profiles regarding their requirements and the three security phases.
- EU Port security directive has the most even spread between the three phases.[55]

4.7 Continuous improvement cycle

Fourth, the research team carried out an analysis whether the five SCS initiatives take account the concept of continuous improvement. Samples of the requirement categorization include:

Plan:

- EU Port Directive: "Based on those general aspects, the port security plan will attribute tasks and specify work plans in the following fields: […] Integration with other preventive plans or activities. The plan will specifically deal with integration with other preventive and control activities in force in the port."
- TAPA: "Risk assessments performed on Buyer-designated routes."

[55] This can be due to the fairly broad nature of security requirement descriptions in the EU Port security directive.

Do:

- EU AEO: "The applicant should have security requirements in place regarding the use of temporary personnel."
- IRU: "Establish a site management system covering identification, evaluation and management of security risks to people and information involved in dispatching goods."

Check:

- EU AEO: "Internal control procedures should be in place when discrepancies and/or irregularities are discovered. There should exist a separation of functions between the ordering of the goods (purchase), receipt (warehouse), the entering of the goods in the system (administration) and the payment of the invoice.

Act:

- EU AEO: "Have during the last year incidents occurred with regard to the arrangements as mentioned above? If yes, what types of measures have resulted as a consequence of the incidents which happened?"
- EU Port Directive: "Based on those general aspects, the port security plan will attribute tasks and specify work plans in the following fields: […] Procedures for adapting and updating the port security plan."

Next, we present the outcomes of the in-depth analysis, where each security requirement from the five SCS initiatives was analyzed and linked to one of the P/D/C/A -steps. The results are presented in two diagrams below: the first one, Figure 13, shows inside each SCS initiative (on the x-axis) the percentage of each of the three phases (on the y-axis); e.g. in EU Port security directive around 12% of the requirements have a link to the plan-step.[56]

[56] This time, the total percentage is maximum 100%, while each SCS requirement is linked to just one of the continuous improvement cycle steps; and, in few cases zero links are made, as they were not obvious enough – this is why some of the bars do not add up to quite 100%.

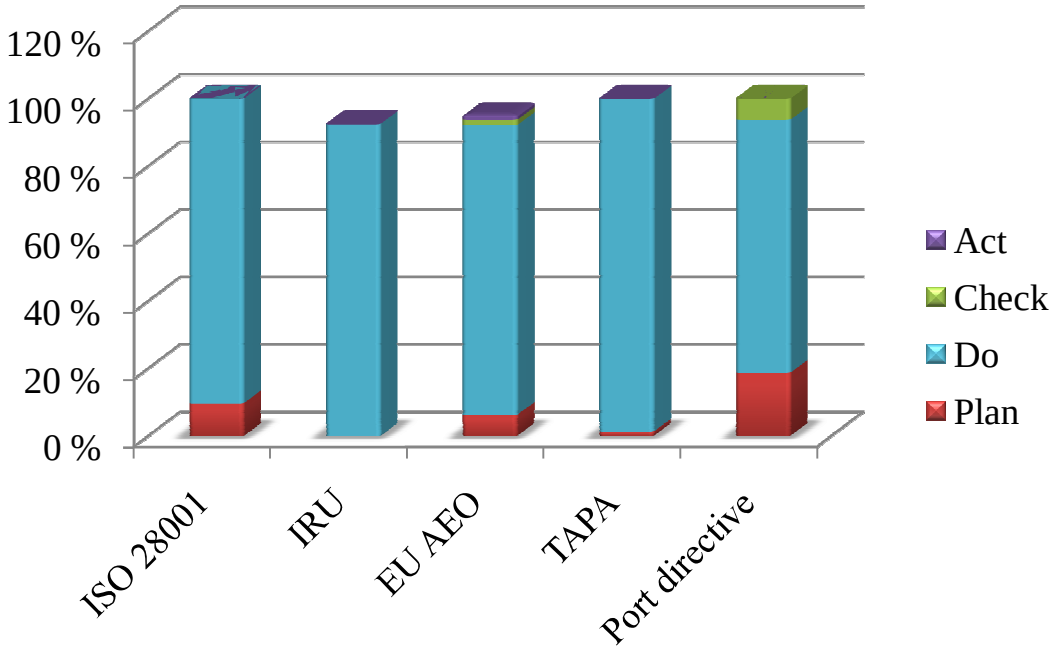

Figure 13 Percentage of PDCA-cycle steps

The second graph, Figure 14, shows per PDCA-step (on x-axis) the total number of SCS requirements, broken down per SCS initiative (on y-axis); e.g. do-step has in total over 300 requirements in the five SCS initiatives.

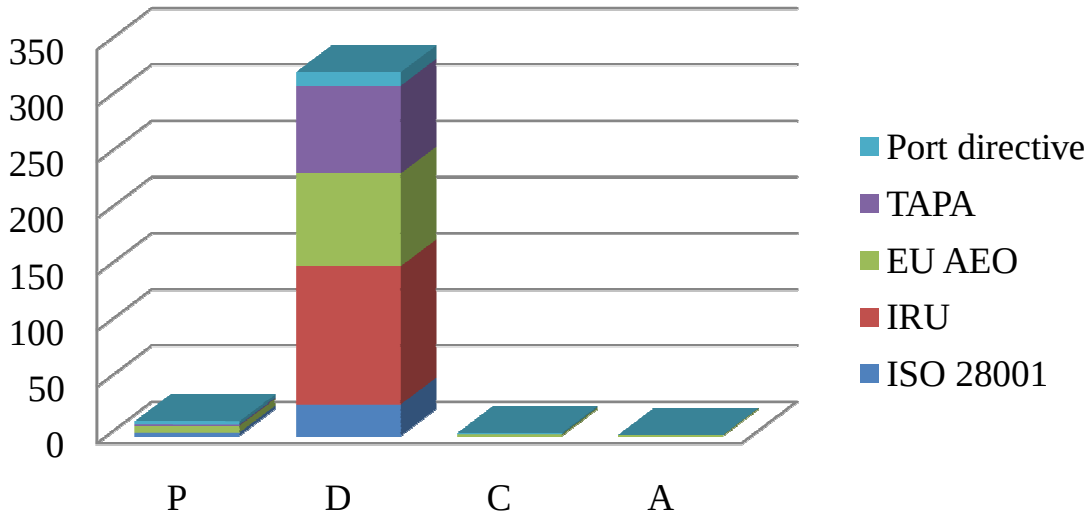

Figure 14 Number of requirements which can be categorized as a certain PDCA-cycle step

Based on these two diagrams, the following immediate observations can be made:

- Do-step is the dominant step in every SCS initiative.

- Plan-step plays some role in four of the five initiatives.
- Check–step is present only in EU AEO and EU Port security directive.
- Act-step is present only in EU AEO.

However, when one looks at the ISO28000 series at a whole, the PDCA-approach is fully highlighted there – even though it wasn't explicit in the document chosen for this in-depth analysis.

4.8 Situational crime prevention

As the second-to-last analysis method, the research team carried out a brief analysis based on situational crime prevention theories, applied to supply chain security.[57] This analysis is of anecdotal nature, more like testing its applicability in the SCS environment.

The logical sequence of situational crime prevention can be described as follows:

1. First, look at the whole supply chain, suppliers and sourcing countries, transport modes, routes and times, warehousing areas, etc. In the case of high threats and/or vulnerabilities, consider making changes in the supply chain design, in order to eliminate the sources of problems.

   *** However, if you cannot eliminate all threats and vulnerabilities, then:*

2. Second, protect information on your supply chain and shipments to the extent possible, without hurting the logistics efficiencies; e.g. hide company and product information on boxes, trucks etc.; invest in data system security; train your personnel on various aspects of information protection etc.

   *** However, if you cannot hide and protect all such information, and criminals know where they could strike, then:*

3. Third, prevent the access to your goods and supply chain assets by physical security; with "guards, guns and gates", amongst all other possible physical security means.

   *** However, if you cannot fully secure all the premises, and a crime actually happens, then:*

4. Fourth, minimize the crime rewards, by making the products as low value as possible; e.g. technical products will not work without a pin-code granted later from a centralized internet service, or a stolen truck cannot be driven more than one kilometer, etc.

   *** This is where the situational crime prevention theories applied to SCS stop.*

Observed samples for each of the four steps include the following:

[57] To the best knowledge of CBRA research team members, this is the first time someone is systematically working to apply situational crime prevention theories in the context of supply chain security, formulating one of the many building blocks for the new security management paradigm called Value Chain Security (VCS).

Supply chain (re)design:

- ISO: "Are there security rules, procedures or guidance provided to conveyance operators (for example, the avoidance of dangerous routes)?"
- IRU: "Only use transport operators of demonstrated good repute."

Information security:

- IRU: "Make the nomenclature neutral (remove special marks, references, codes - anything that enables the recognition of goods)."
- IRU: "Limit explicit information on the type of cargo and its itinerary."

Physical security:

- EU AEO: "How are the external boundaries of the premises secured? All buildings should be constructed of materials which resist unlawful entry and protect against external intrusion. All external and internal windows, gates and fences must be secured with locking devices or alternative access monitoring or control measures such as internal/external anti-burglar alarm systems or CCTV (close circuit TV systems)"
- TAPA: "Solid-top, hard-sided or reinforced soft-sided trailers with lockable cargo doors."

Crime reward decreasing:

- TAPA: "Vehicle immobilization devices utilized."

The brief conclusion at this point is that the opportunities of situational crime prevention theories are not widely exploited in these five SCS initiatives, and that they could be explored further in the future. For example the first and the last step of this analysis, i.e. supply chain (re)design, and crime reward decreasing are particularly interesting, possibly new approaches to reduce crime in supply chains.

4.9 Existing European security norms

The last analysis method in this six-method approach is reviewing any links between the five SCS initiatives and any existing European or national norms somehow related to supply chain security. The outcome of the norms review carried by the research team is presented below, listing several examples of existing security norms, under six groups. And this is followed by straightforward conclusions regarding the existence of links between these norms and the five SCS initiatives.

Physical Security:

- EN 12209: Building hardware - Locks and latches - Mechanically operated locks, latches and locking plates - Requirements and test methods
- EN 1303: Building hardware - Cylinders for locks - Requirements and test methods
- EN 12320: Building hardware - Padlocks and padlock fittings - Requirements and test methods
- ENV 1627: Windows, doors, shutters - Burglar resistance - Requirements and classification

- ENV 1628: Windows, doors, shutters. Burglar resistance. Test method for the determination of resistance under static loading
- ENV 1629: Windows, doors, shutters. Burglar resistance. Test method for the determination of resistance under dynamic loading
- ENV 1630: Windows, doors, shutters. Burglar resistance. Test method for the determination of resistance to manual burglary attempts
- EN 356: Glass in building - Security glazing - Testing and classification of resistance against manual attack
- EN 1063: Glass in building - Security glazing - Testing and classification of resistance against bullet attack
- EN 1143-1 Secure storage units - Requirements, classification and methods of test for resistance to burglary - Part 1: Safes, strongroom doors and strongrooms
- BS 8220-3:2004 Guide for security of buildings against crime – part 3: Storage, industrial and distribution premises

Access control:

- EN 50133-1: Alarm systems. Access control systems for use in security applications. Part 1: System requirements
- EN 50133-7: Alarm systems. Access control systems for use in security applications. Part 7: Application guidelines

Alarm systems:

- EN 50131-1 Alarm systems. Intrusion and hold-up systems. Part 1: System requirements
- EN 50131-6:1998 Alarm systems. Intrusion systems. Power supplies
- CLC/TS 50131-7 Alarm systems. Intrusion systems. Part 7: Application guidelines

CCTV –systems:

- BS 7958:2005 Closed-circuit television (CCTV). Management and operation. Code of practice
- BS 8418:2003 Installation and remote monitoring of detector activated CCTV systems – Code of practice
- prEN 50132-1 Alarm systems - CCTV surveillance systems for use in security applications - Part 1: System requirements
- EN 50132-7 Alarm systems. CCTV surveillance systems for use in Security applications. Part 7: Application guidelines
- BS 8495:2007 Code of practice for digital CCTV recording systems for the purpose of image export to be used as evidence

Security service providers:

- EN 15602 Security service providers. Terminology
- BS 7499: 2007 Static site guarding and mobile patrol service – Code of practice

Security screening:

- BS 7858:2006 Security screening of individuals employed in a security environment – Code of practice

The outcome of the this analysis-step is straight forward: the research team could not find one explicit link between the five SCS initiatives and these European and national security norms – even though several requirements existed talking about physical security, access control, alarm systems, CCTV etc.

4.10 Conclusions

The main findings of this SCS initiative chapter are as follows – addressing the original questions listed in the introduction (Chapter 4.1):

1. The five existing SCS initiatives, one way or another, cover all types of supply chain actors. Thus there are no urgent needs to fill any major gaps with new initiatives, in this sense.
2. Cargo and facility security measures are most common in these SCS initiatives, while a broad set of measures exists targeted also for business network, human resource, and information technology security.
3. Preventive security measures come up on top when analyzing the security phase, followed by detect/react measures, and finally followed by recovery-measures.
4. Regarding the continuous improvement cycle, do-step is the most dominant, by far, followed by a couple of plan-measures, and almost non-existing check- and act- measures.
5. The principles of crime prevention theories appear to be applied to some limited extent by the SCS initiatives: next to a large number of information and physical security measures, a couple of supply chain (re)design, and one crime reward decrease measure, were identified.
6. And finally, no link was found between the existing set of European (and national) security norms and these five SCS initiatives.

All these aspects, including differentiation, complementation and balancing between them – case by case basis - should be considered thoroughly, whenever analyzing and/or (re)designing any SCS initiatives.

5 Operator survey

5.1 Introduction

The goal of the Operator survey is to explore further a variety of SCS management and standards related aspects with the actual operators , i.e. trade/wholesale/retail; shippers/manufacturers; and various types of logistics companies. These are the companies which either own the goods at some point in the supply chain, or companies which participate in the logistics steps of handling, moving and/or storing the goods – the companies who face the damages when security incidents happen – one could call them also "the end-users of supply chain security".

First the survey process focused on creating the questionnaire; selecting the population; sending the invitations; schedule; and explanation of the tool (Chapter 5.2). Next, statistics on the survey participants, 86 companies in total, is presented, including company sector, size, geography, and person who replied (Chapter 5.3). This is followed by statistics on (perceived) crime trends and crime concerns (Chapter 5.4); security standards and procedures (Chapter 5.5); benefit and cost components with SCS standards (Chapter 5.6); and dilemmas with SCS standards (Chapter 5.7). Finally, the findings specific to possible new SCS standards are shared (Chapter 5.8); and the results of the whole operator survey are summarized and conclusions are made (Chapter 5.9).

5.2 Survey process

The survey questionnaire was created by the CBRA research team based on the outcomes of the literature review (Chapter 2) and expert interviews (Chapter 3).[58] The survey form has a total of 51 questions, in following four parts:[59]

- Part 1. Basic information: 14 questions on company sector; size; geography; import/export rates; person answering etc.
- Part 2. Supply chain security standards, costs and benefits: 9 questions on current security and other standards; security procedures in place; SCS cost and benefit components; etc.
- Part 3. Opinions by scale: 27 statements (agree / disagree) on various aspects of crime trends; needs and constraints for new standards; dilemmas with existing SCS initiatives; etc.
- Part 4. Any comments, notes or observations.

The survey was distributed to a large population of supply chain operators[60] in Europe[61], via following three main channels:

- CEN SCS group – with multiple emails, both by CBRA and by NEN
- Other trade associations – CBRA sent one round of emails to sectors specific associations

[58] The form was also tested and validated with the Study Project Steering group members, in August 2009.
[59] The complete questionnaire is presented in Annex 1 of this report.
[60] Shippers/manufacturers ; trade/retail/wholesale; and logistics sector.
[61] It is not possible to trace to how many companies the survey request went to.

- Other contacts – CBRA asked multiple persons to suggest additional contacts.

The technical platform was two-fold:

- Digium survey software – this was the main tool during the whole exercise.[62]
- Word-file – this was added as an option, as it appeared that some potential respondents preferred to answer this way.[63]

The survey was presented in three languages:

- English – this was the original language.
- German – was offered later during the survey.
- French – was offered later during the survey.

The schedule to reply in the survey was expanded once:

- Original deadline: 5.10.2009
- Final deadline: 23.10.2009

Total of 91 responses came on time, out of which 86 were valid for the study purposes.

5.3 Survey participants

First we look at statistics on the survey participants, with following eight questions and related parameters:

- What is the main business for the company: manufacturing vs. logistics vs. trade?
- What are the industry sectors, both main and side sectors for each company?
- What is the company turnover in Euros (in nine turnover groups)?
- How many people are employed by the company (in ten personnel number groups)?
- In which country is the business unit of the respondent located?
- How international (or "European") is the company (in five groups)?
- What is the value of import and export transactions, as a % of the sourcing (imports) and sales (exports) (in five groups)?
- In which function and on which organizational level does the person replying work (ten functions and eight organizational levels)?

Company business: manufacturing vs. logistics vs. trade

First, Figure 15 presents the distribution of respondents between the three main sectors. The transport and logistics sector is the biggest group in the study (63%), which reflects the bias of the survey sample towards the logistics sector, in particular via the logistics related trade associations active in the whole feasibility study. Manufacturers and shippers formed the second biggest group in the survey (29%), and finally trade,

[62] See www.digiumresearch.com for more details on this web-based survey tool.
[63] Before introducing the word-option, some participants printed the .pdf-version, replied by pen, scanned and emailed the scanned file back.

retail and wholesale came as the smallest group (8%); these two groups also reflecting the proportion of various associations active during this feasibility study process.

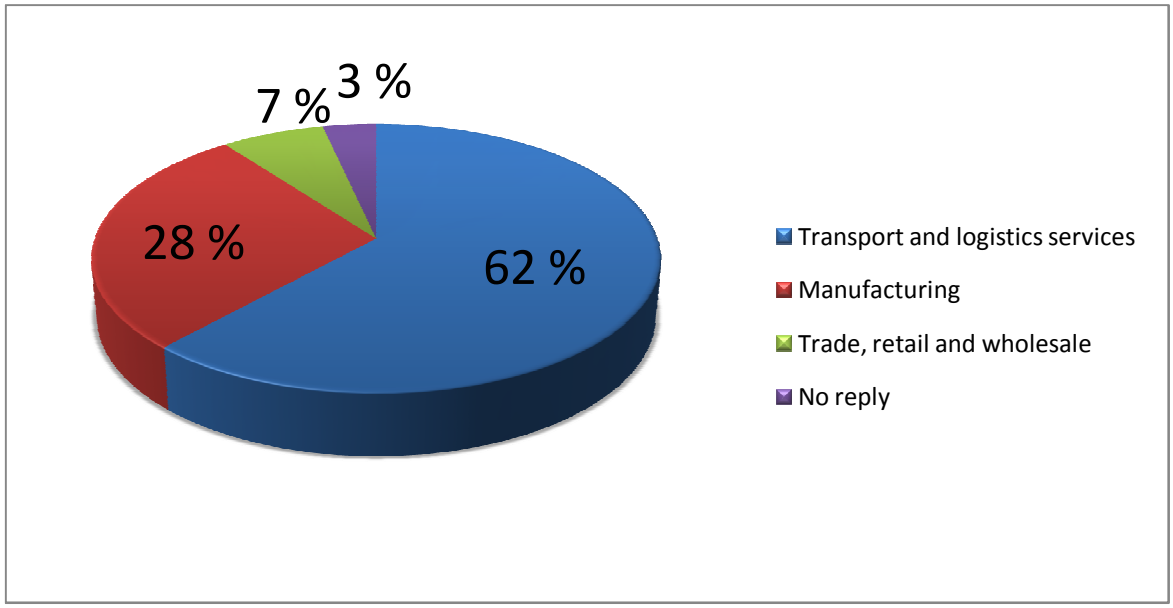

Figure 15 The distribution of respondents between the three main businesses.

Industry sectors, both main and side sectors for each company

Regarding the sectors for the companies participating in the survey, each company was asked first to identify their main sector, and – in the case of multi-sector companies – their side sectors.

First, regarding the manufacturing companies, there was a wide spread over 27 different sector, without any major dominating sector. This list includes both main and side sectors, as identified by participating companies:[64]

- Aerospace and Defense
- Apparel
- Beverages
- Building Materials, Glass
- Chemicals
- Computer Peripherals
- Computer Software
- Computers, Office Equipment
- Electronics, Electrical Equipment
- Energy
- Engineering, Construction
- Food Consumer Products
- Forest and Paper Products
- Furniture

[64] Here one company typically belongs to more than one sector; i.e. besides the main sector, most companies also identified one or more side sectors.

- Household and Personal Products
- Industrial and Farm Equipment
- Information Technology Services
- Medical Products and Equipment
- Metals
- Motor Vehicles and Parts
- Network and Other Communications Equipment
- Packaging, Containers
- Pharmaceuticals
- Publishing, Printing
- Semiconductors and Other Electronic Components
- Toys, Sporting Goods
- Transportation Equipment

Second, for the logistics companies, a graph is provided to illustrate the broad coverage of various types of logistics actors participating in the survey – all twelve proposed sectors are represented, at a minimum as a side sector (air port operators). The five biggest main sectors were road carriers; freight forwarders; sea carriers; rail carriers; and warehouse keepers. When including the side sectors, customs agent –services came also in the top five, dropping rail carriers to position six.

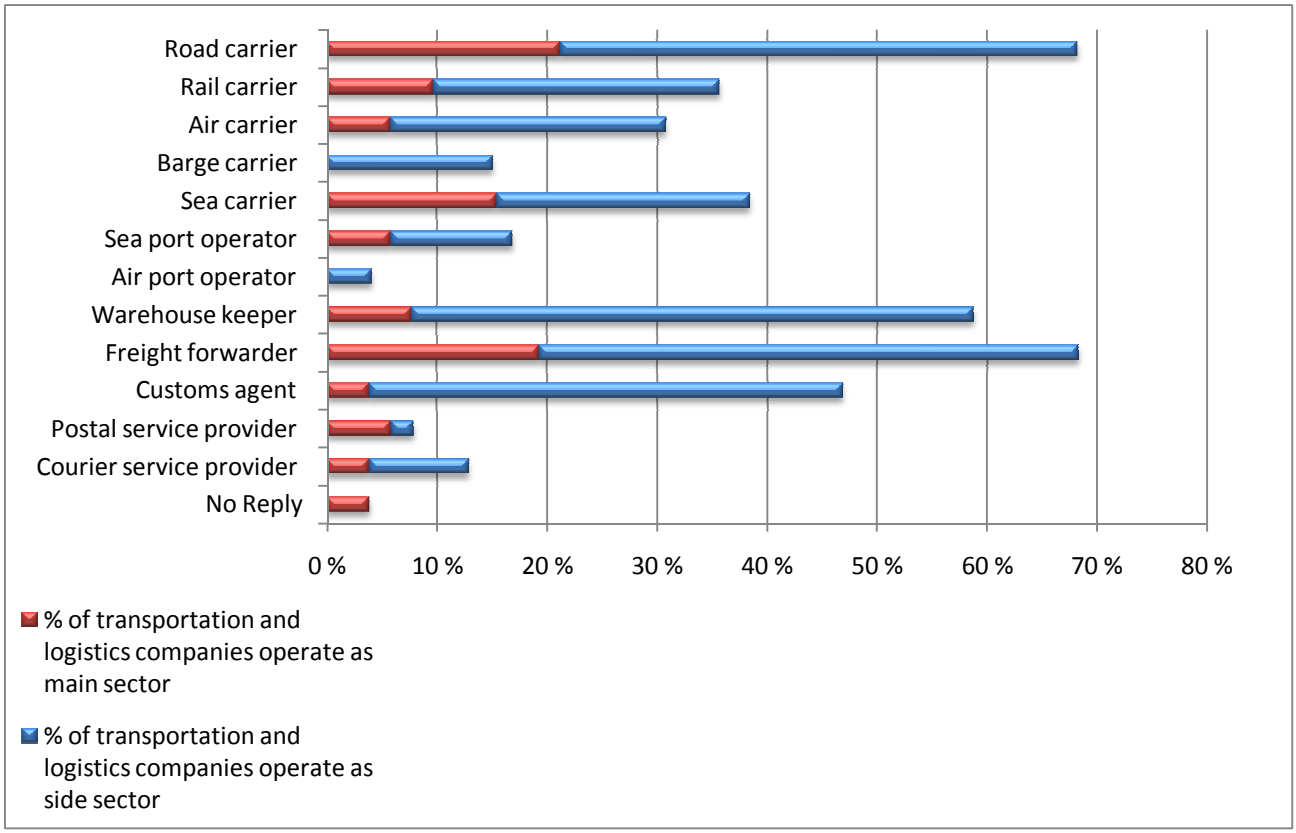

Figure 16 The distribution of the logistics sector respondents.

And third, regarding the trade, retail and wholesale companies, the following sectors were represented, either as a main sector and/or as a side sector:

- Commodities trading
- General Merchandisers
- Specialty Retailers
- Wholesalers: Diversified
- Wholesalers: Electronics and Office Equipment
- Wholesalers: Food and Grocery

Turnover in Euros and number of personnel employed

Next, we look at the size of the participating companies, both in terms of revenues and number of personnel. Companies from all size groups joined the survey, smallest ones having 250.000 to 1 million Euros in annual revenues, and just 1 to 5 employees. The biggest participants have over 10 billion Euros in revenues and over 100.000 employees working for the company. Looking at the number of employees, there are two peaks: 51-250 employees, and 5001-25000 employees, these two groups representing some 47% of the total population. For the revenues, the two main groups are 1-10 billion Euros and 10-50 million Euro, these two groups covering around 43% of the total population. In the total picture, there appears to be some bias towards larger companies, which is quite understandable regarding this type of survey.

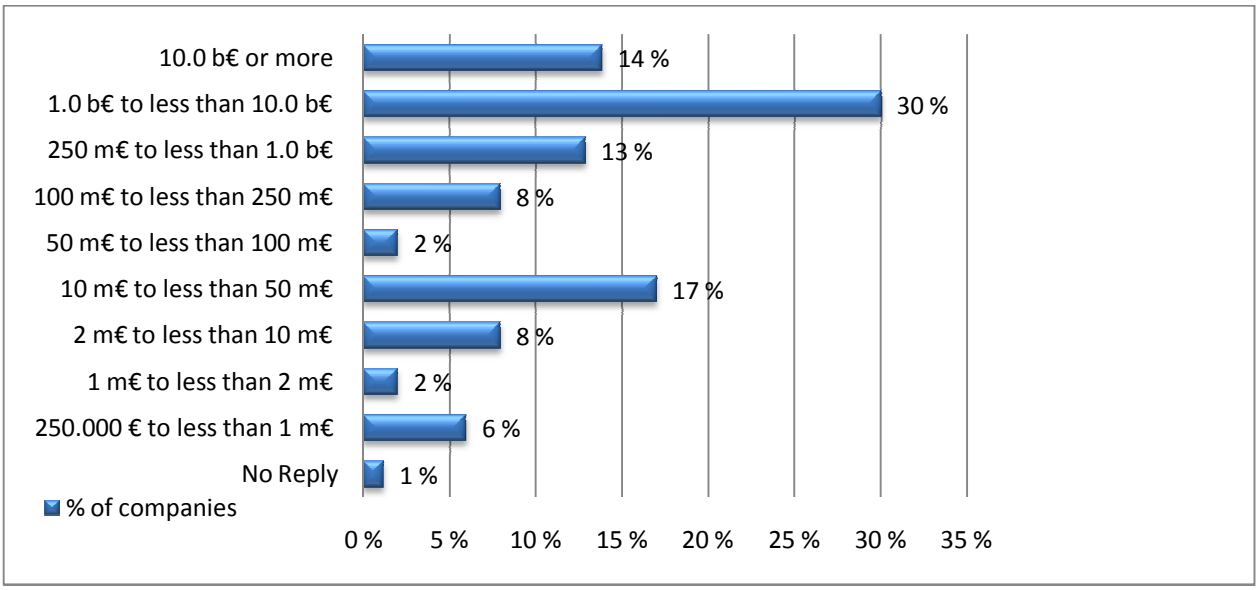

Figure 17 The distribution of turnover levels with the respondents

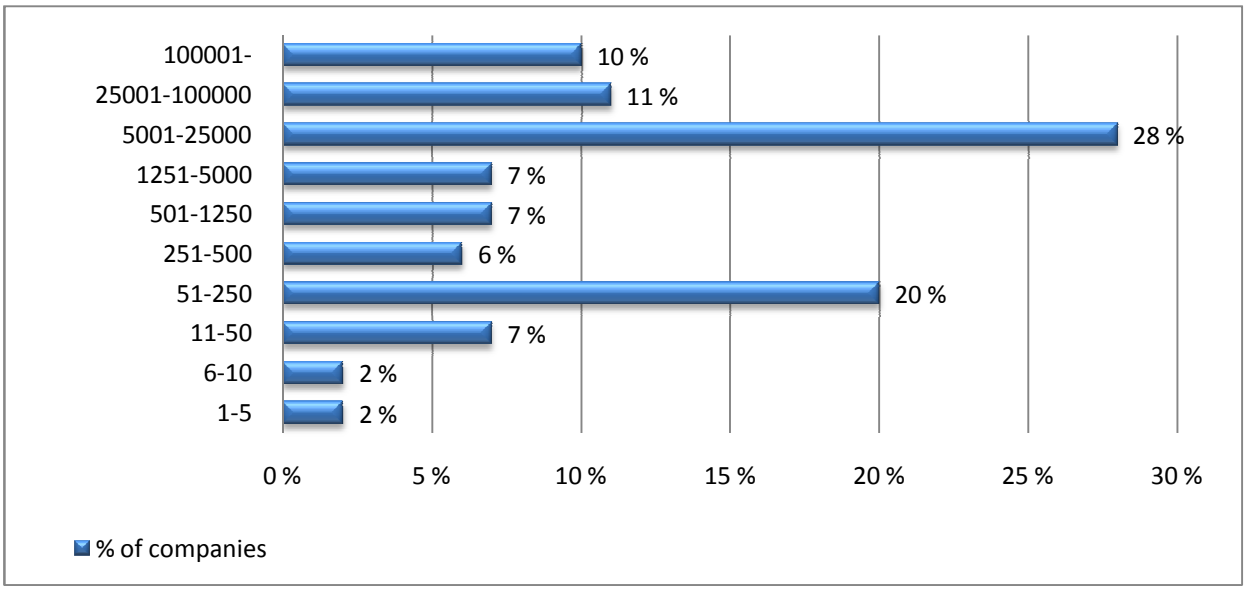

Figure 18 The distribution of number of employees with the respondents

Countries where the business unit of the respondent is located

Fourth, the home countries for the companies was asked – location determined where the responding person is working. The big EU countries Germany, France and UK, together with the Netherlands and Switzerland, cover over 70% of the responses, thus introducing some bias in the population. Around 4-5% of the replies came from Finland, Denmark, Belgium, Austria and Sweden each. The remaining 5-6% was covered for example by Spain, Bulgaria, Czech Republic, Hungary and Lithuania.

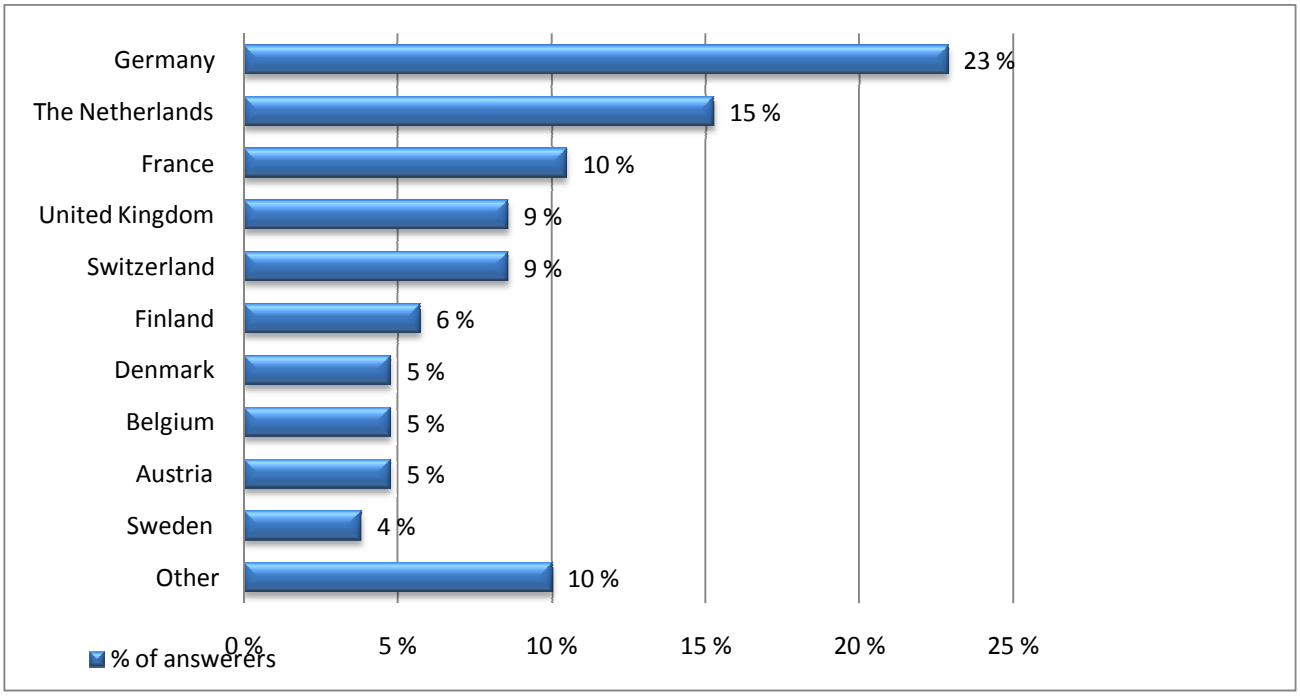

Figure 19 The distribution of home countries for the participating companies

International / European presence of the companies

Next, looking at the international / European presence of the responding companies, over 35% of them have multiple locations in multiple European countries (12 or less countries). Around 36% of the companies operate in more than 12 countries; and around 22% in just one country.

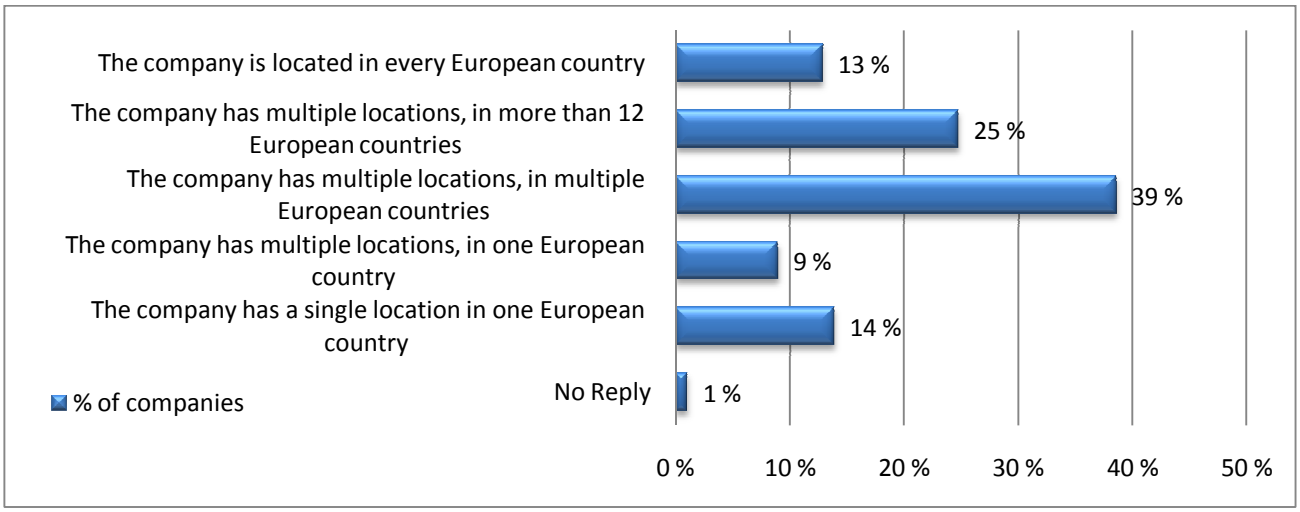

Figure 20 The degree of international (European) presence by the participating companies

Value of import and export transactions for the companies

Sixth, the share of international (non-EU) transactions was asked, both for imports (as sourcing) and for exports (as sales). Here the spread both for imports and for exports is fairly even in terms of the five-step scale used (0% ; 1-10% ; 11-25% ; 26-50% ; > 50%) – between 6-13 % for each of the groups. For the rest of the companies the question is either not relevant, or the answer is not known.

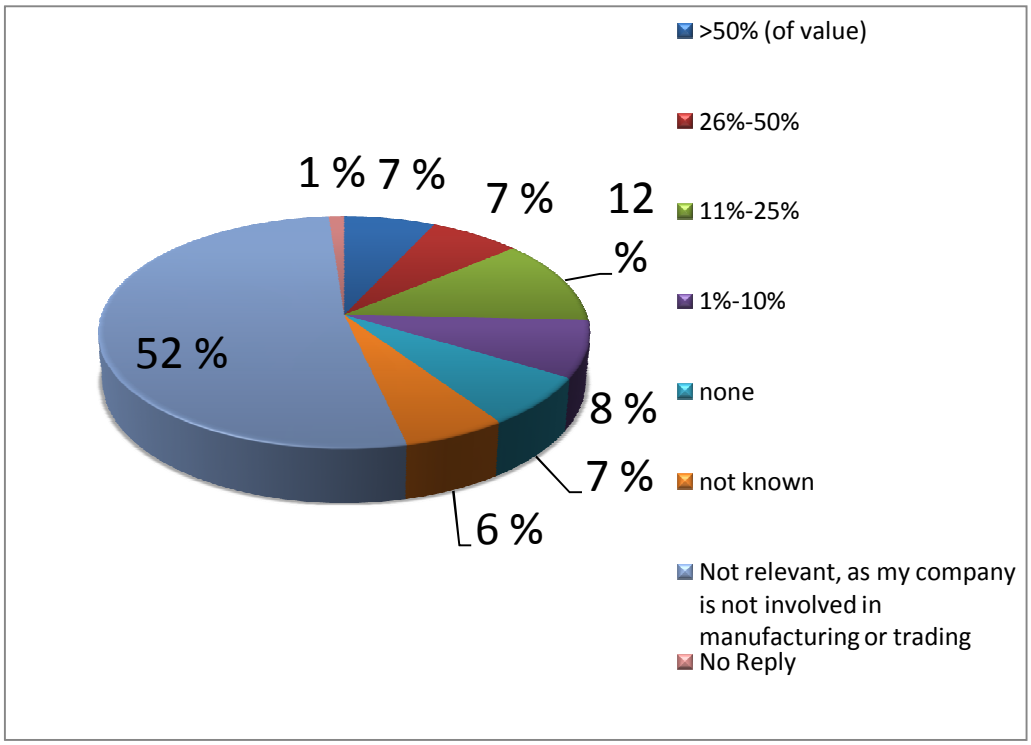

Figure 21 The level of imports, as % value of sourcing, with the participating companies

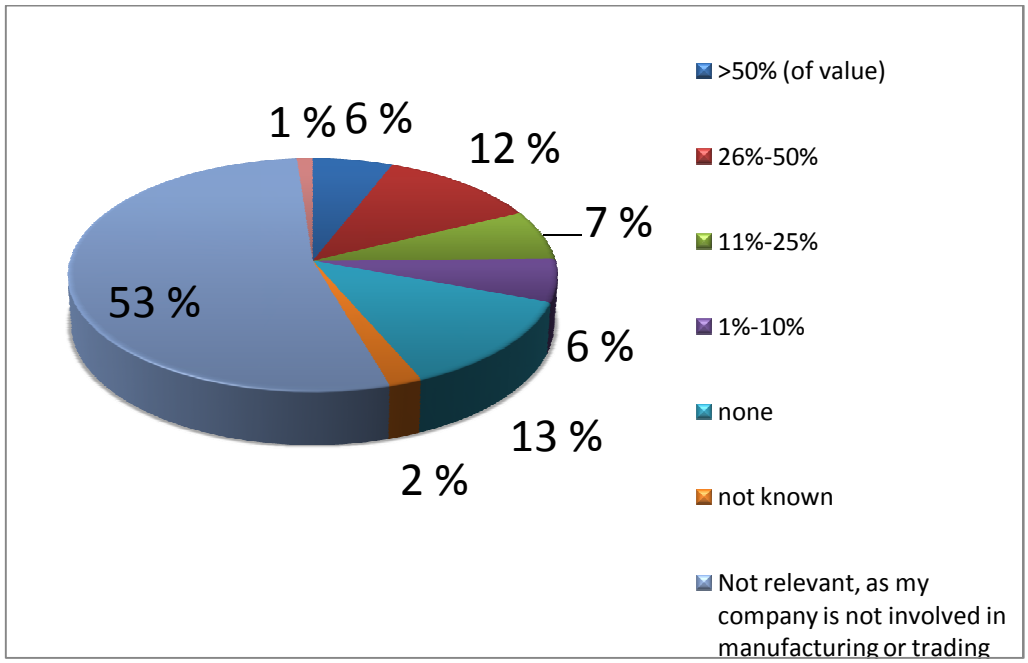

Figure 22 The level of exports, as % value of sales, with the participating companies

Organizational function and hierarchy level of the responding persons

Lastly, regarding factual data on the survey participants, the function and organizational hierarchy level of the responding persons were asked. As can be observed in Figure 23 below, around 35% of the responding

persons represent the security function; the rest working mainly for supply chain, transportation management, risk management, quality management and compliance functions.

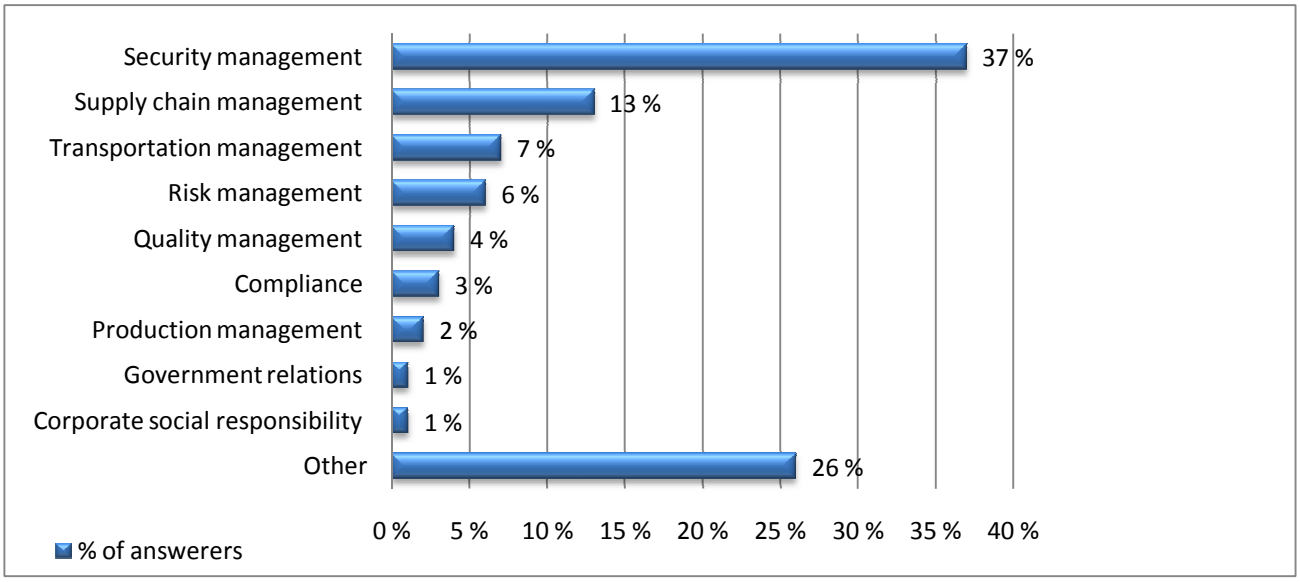

Figure 23 Business function of the person replying in the survey

On the organizational hierarchy question, the biggest individual group is on manager level (33%). The rest is fairly evenly distributed amongst another seven levels, from administrator and expert levels to management team and board of directors levels.

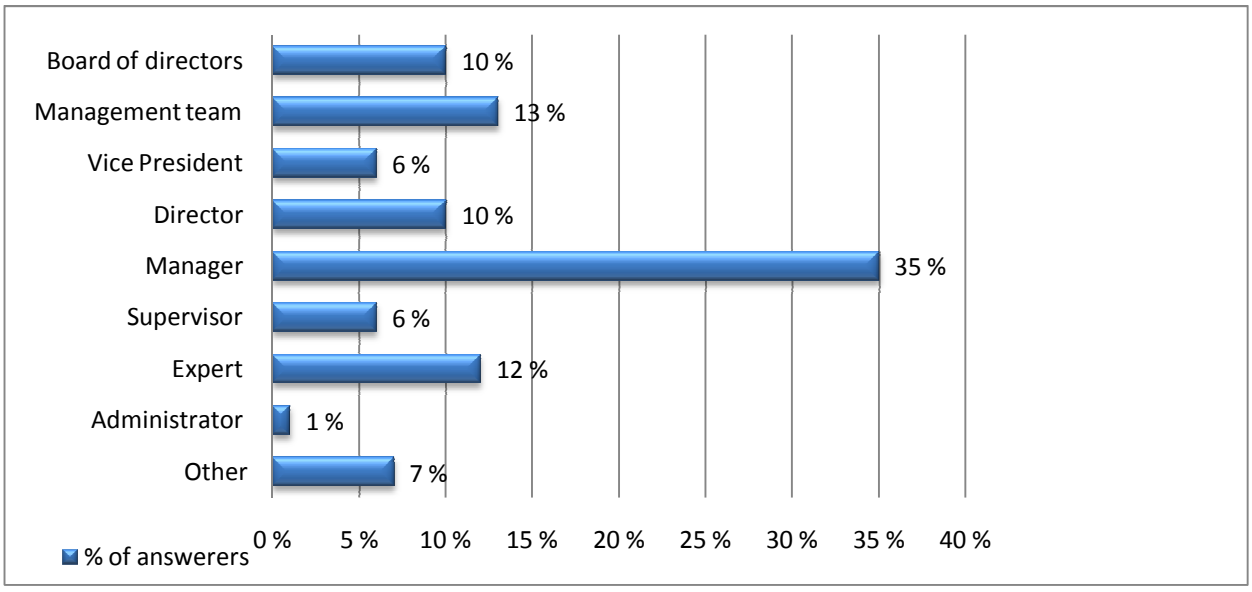

Figure 24 Hierarchical level of the person replying in the survey

5.4 Crime trends and concerns

In this sub-chapter two different angles on assessing the overall trends in crime and security; and the "seriousness" of various crime types are taken. First, in Figure 25 below, the assessments of four

statements (survey section 3) are reported, indicating partial agreement with "crime in supply chains is growingly a transnational problem"; "crime concerned have increased (during the past five years) in supply chains in Europe"; and "number of actual crime incidents have increased in European supply chains" – the third one with the highest variance, i.e. differing opinions.

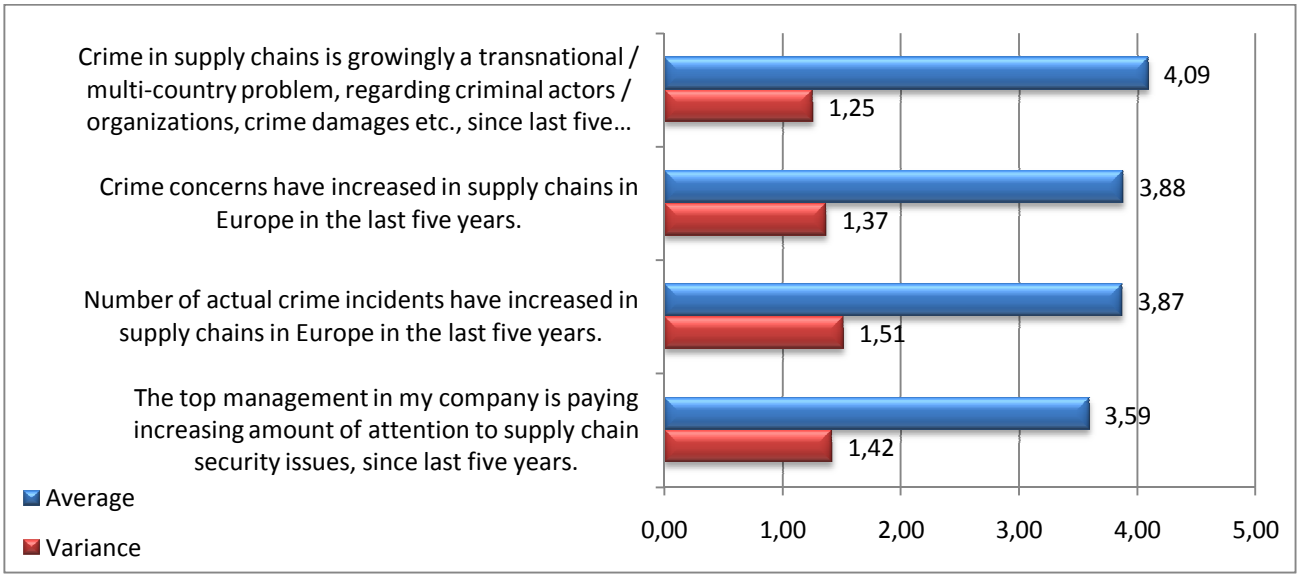

Figure 25 Views on crime and security trends in European supply chains[65]

Second, in Figure 26 below, the various crime concerns are assessed and prioritized by the respondents. Theft came on the highest position, also with the highest variation. The average of all crime concern is low to medium; thus indicating limited relevance of crime in overall supply chain management.

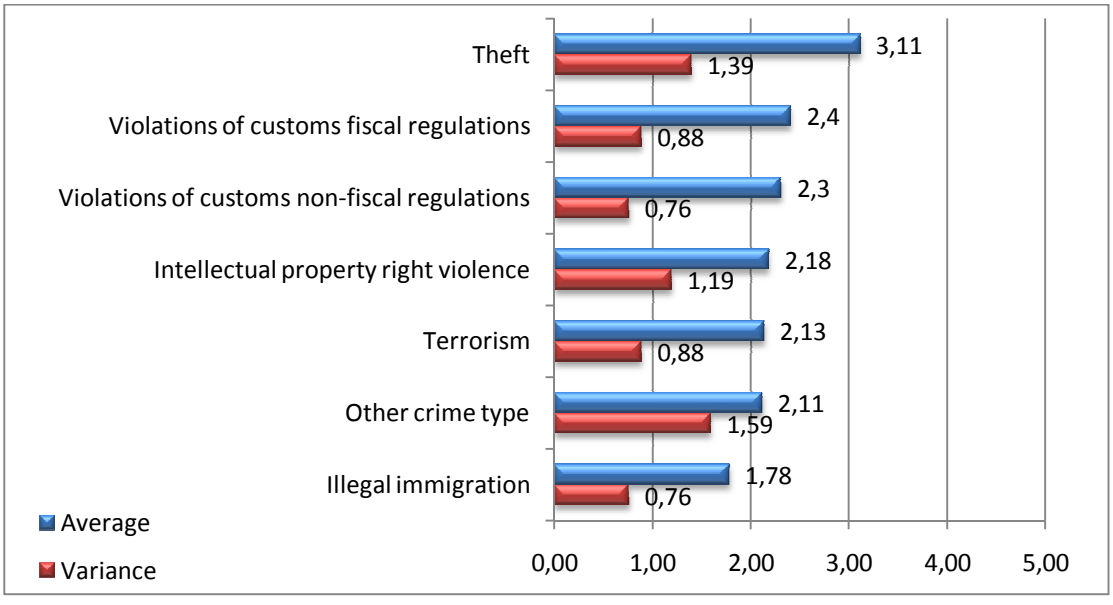

Figure 26 Priorities for crime concerns with the survey participants[66]

[65] A scale from 0 to 5 is used to show the answers accordingly: Fully agree(5) – Partially agree(4) – Neither agree or disagree(3) – Partially disagree(2) – Fully disagree(1). We start from 0 /include 0 to 1 in the scale because variances can be less than 1.

[66] A scale from 0 to 5 is used here: Very high (5) – High (4) – Medium (3) – Low (2) – None (1). We start from 0 /include 0 to 1 in the scale because variances can be less than 1.

5.5 Security standards and procedures

In this sub-chapter, the implemented SCS standards and guidelines are reviewed, together with the degree of contractual requirements to go together with these standards. This is followed by a yes/no type of analysis on specific security management procedures in place at the responding companies.

Regarding the implemented SCS standards question (Figure 27 below), the company internal policies / guidelines; EU AEO; TAPA; and other public administration created standards came out on top, with 28-43% implementation rate each. Regarding contractual requirements to have these standards in place, EU AEO and TAPA were the top two, both with around 18% of the survey population having such a requirement in place.

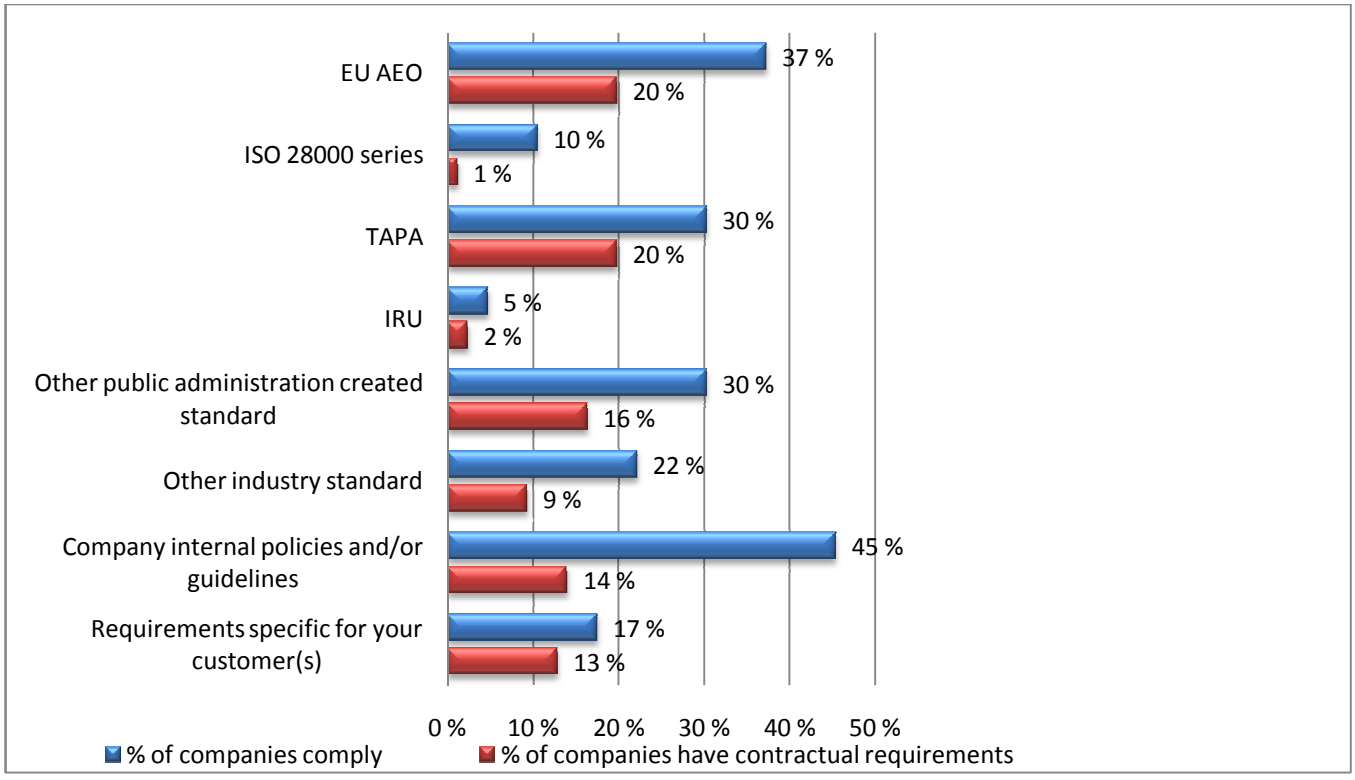

Figure 27 Percent-share of companies complying with various SCS standards

Regarding a set of five specific security management procedures (Figure 29 below), one can observe that documentation of all security measures and activities is a common practice (61% of the companies); followed by security efficiency reports, and defined accepted levels for crime risks (45% in both). Budgeting for annual SCS costs comes next (41%), while benefit-cost calculations come last (with 30% implementation rate).

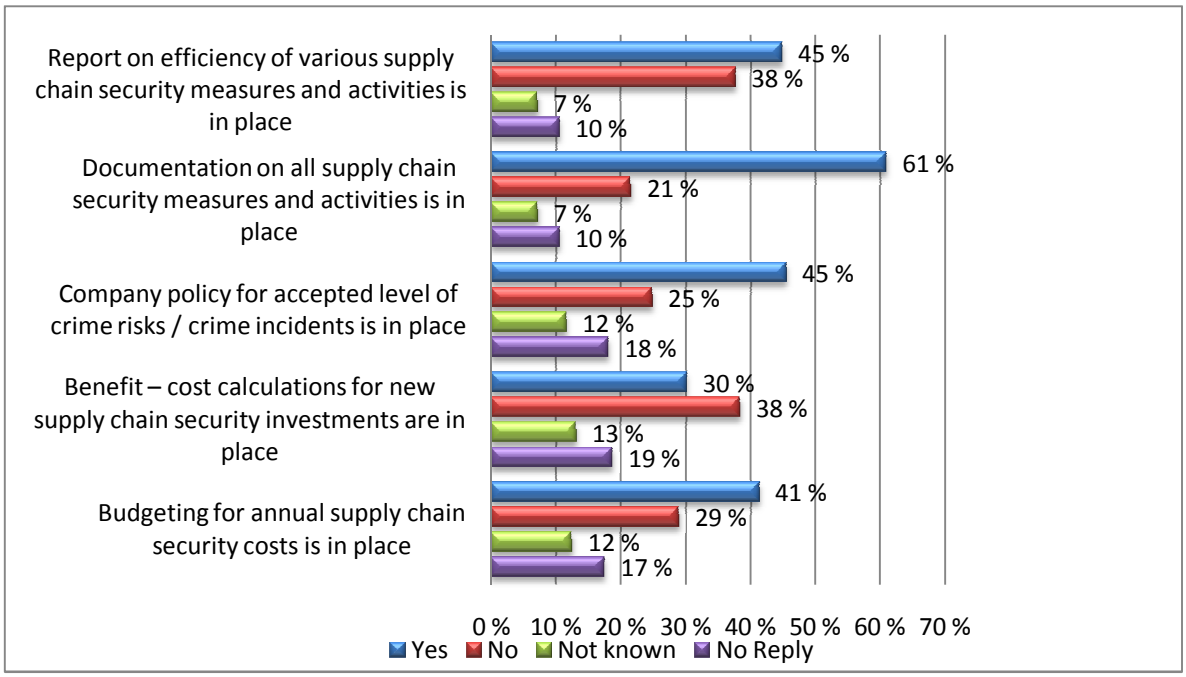

Figure 28 Various security management procedures in place (scale: yes / no / not known)

5.6 Benefits and costs with SCS standards

Regarding the benefits and costs of SCS standards, a qualitative assessment was carried out in the survey. On the benefit side, the two highest ranked benefit areas are “promotion and protection of company brand name and reputation” and “reduction in the number and/or value of actual crime incidents”. The lowest ranking was given to “operational benefits granted by government agencies” and “reduction in insurance premiums. In the overall scale, benefits are ranked between “low+ to medium+”, thus indicating limited overall benefit delivery of SCS standards, in general.

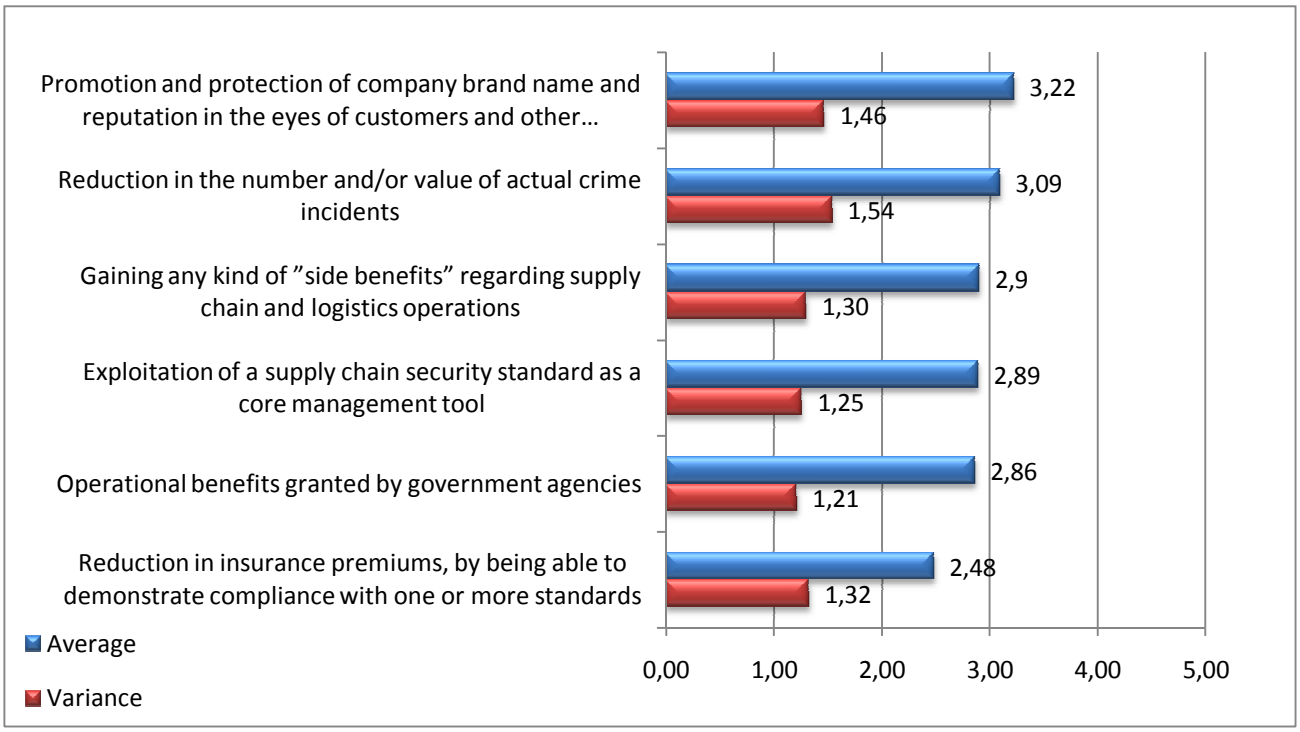

Figure 29 Ranking of a set of possible benefits with SCS standards[67]

Box 15 SCS standards and the insurance sector

Based on anecdotal evidence from the literature, as well as on the potential benefit ranking in the operator survey in this feasibility study, the links between SCS standardization and the insurance sector appear to be weak, even non-existent. Intuitively one might think that companies which comply with one or more SCS standards would enjoy lower insurance premiums; however, this does not appear to be the case.

An insurance system can be described as a mechanism reducing adverse financial impacts of random events. A company can sell its own financial risks to an insurance company; this insurance company then administrates this mechanism to help manage the risk. The insurance premium is a service fee, which covers the expected cost of losses in the long run, solvency capital costs and several administrative costs. Expected costs of losses are based on incident rates and expenses incurred in the past. An insurance company can use this information and apply statistical methods to assess its own risk portfolio and redistribute the resulting premium to the individual risks or risk market prices. In other words, the premium is not based on cumulative assessment of impacts of single security measures, but the administration of risk portfolios and "the law of large numbers". Insurance companies have effective tools to transfer and divide risk to competitive markets. Traditionally premium-cuts can be based on the insurance market situation, attractiveness of a customer, decreased liability or a willingness to lower the level of profit instead of loosing a customer - but normally not on declined probabilities of random events, such as security incidents.

Could there be any way in the future for an insurance company to reduce insurance premiums if a customer insisted they be based on compliance with SCS standards? The CBRA research team suggest this as a topic for further research as well as a topic for practitioner discussions and considerations; alternatively this could become an option for a forward looking insurance company (or even a start-up) to win new customers. This is clearly challenging, but an important topic to explore in more detail.

Looking next the two statements on "overall lack of tangible benefits regarding SCS standards", government and business developed / enforced standards, the straight forward observation is that the respondents see the lack of standards as a bigger problem with the government SCS initiatives.

[67] A scale from 0 to 5 is used here: Very high (5) – High (4) – Medium (3) – Low (2) – None (1). We start from 0 /include 0 to 1 in the scale because variances can be less than 1.

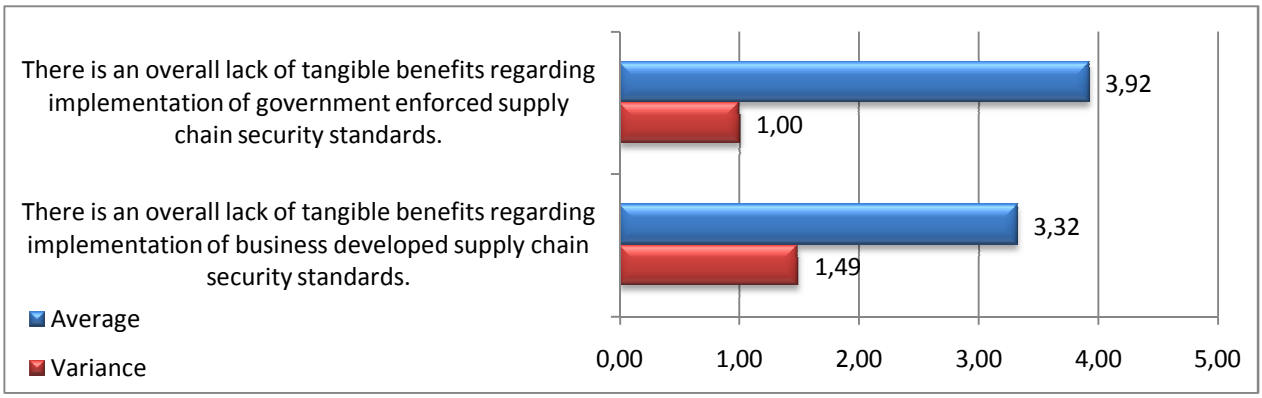

Figure 30 Opinions on benefits with government and business developed SCS standards[68]

Next, seven typical cost elements with SCS standard implementations are ranked by the respondents. Facility protection with technologies, infrastructure and procedural investments is seen as the main cost component; followed by cargo security solutions. Next comes the various "non-investment" type of costs, including business network management; certification and auditing; training and awareness building; and internal administration costs. The last cost item, i.e. consulting fees, is seen as of less relevance. When comparing the overall level of cost and benefit assessments, the former do get higher ranking than the latter.

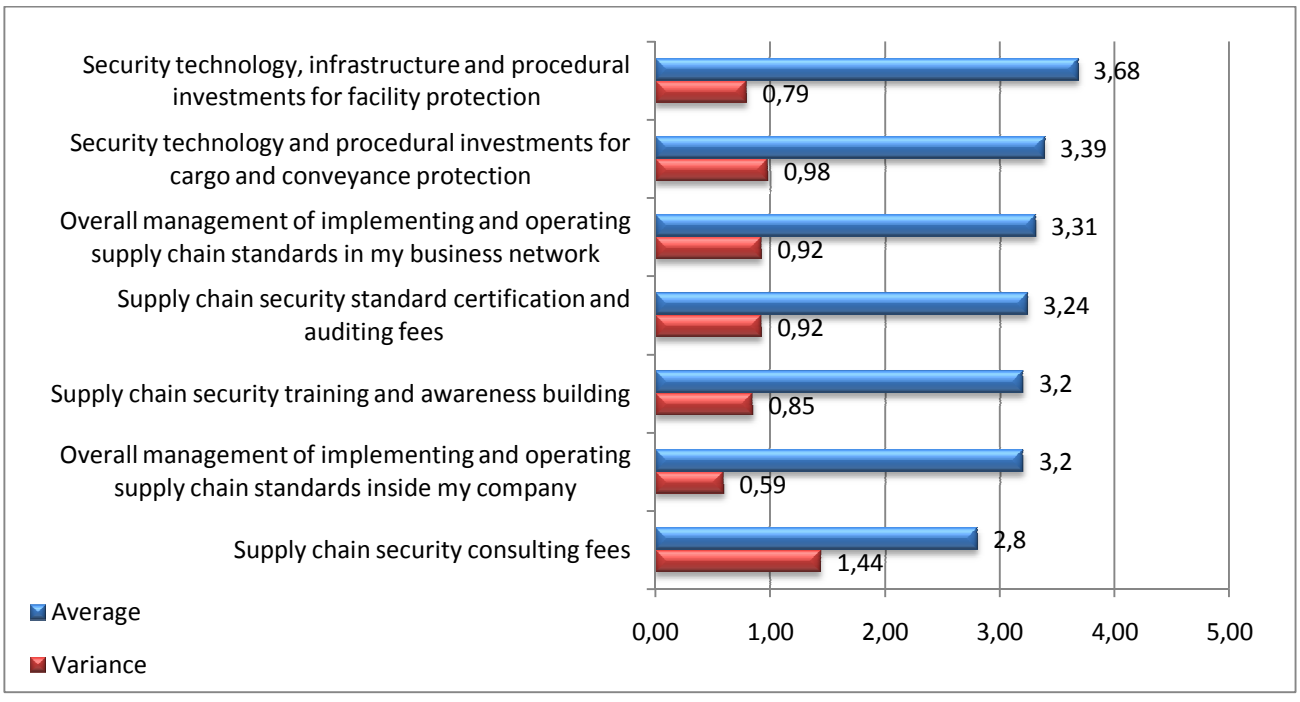

Figure 31 Ranking of a set of possible cost elements with SCS standards[69]

[68] A scale from 0 to 5 is used to show the answers accordingly: Fully agree(5) – Partially agree(4) – Neither agree or disagree(3) – Partially disagree(2) – Fully disagree(1). We start from 0 /include 0 to 1 in the scale because variances can be less than 1.

[69] A scale from 0 to 5 is used here: Very high (5) – High (4) – Medium (3) – Low (2) – None (1). We start from 0 /include 0 to 1 in the scale because variances can be less than 1.

Box 16 SCS costs in different industry sectors

Analyzing and budgeting costs of supply chain security (SCS) – especially in the context of ”post-2001 SCS” – depends strongly on the industry sector and type of products in question. Some commodities, with (perceived) high levels of crime and/or accident risks, have enjoyed relatively high security levels independently of post-2001 SCS programs, standards and regulations; while some commodities have traditionally had only very limited protection in place.

Based on anecdotal evidence from CBRA research, academic and trade journals – as well as using common sense – supply chains, at least in the following sectors, have had a long history of implementing specific security management practices and solutions:

- High value goods, with lucrative aftermarkets for stolen products: e.g. consumer electronics and some luxury goods (anti-theft).
- Highly taxed products in terms of customs and/or excise duties: e.g. fuel, alcohol, and cigarettes (anti-smuggling).
- Product / consumer safety issues: e.g. pharmaceutical products (anti-counterfeit and licensed sales channel issues)
- Dangerous materials, with a risk of explosion: various chemicals and petrochemical products (also anti-terrorism).

A number of other sectors do not, however, have any specific vulnerabilities regarding crime or terrorism in their supply chains, which therefore has led to a lower level of traditional security management being applied. These include: (low cost) clothing and furniture, basic metals,; and forest and paper products amongst others.

In order to comply with post-2001 SCS programs, especially those that apply equally to all, creating a ”level playing field” (such as AEO programs), companies in the first category are likely to require less investment in security than companies in the second category. This makes it difficult to estimate the total or even average SCS costs: the costs will depend heavily on the starting level of each company / supply chain in question. To shed some light onto the issue, the CBRA research team is actively looking at the security levels and investments for both ”high security” and ”low security” sectors and companies.

5.7 Dilemmas with security standards

The relevance of four possible dilemmas with SCS standards was investigated – and the results are presented in Figure 32 below. The main concern here is that “company or supply chain insiders can pass information and data to the criminals”; followed by “SCS standards easily create a false sense of security”. The degree of agreement is not particularly high there; while the variation in the opinions is relatively high.

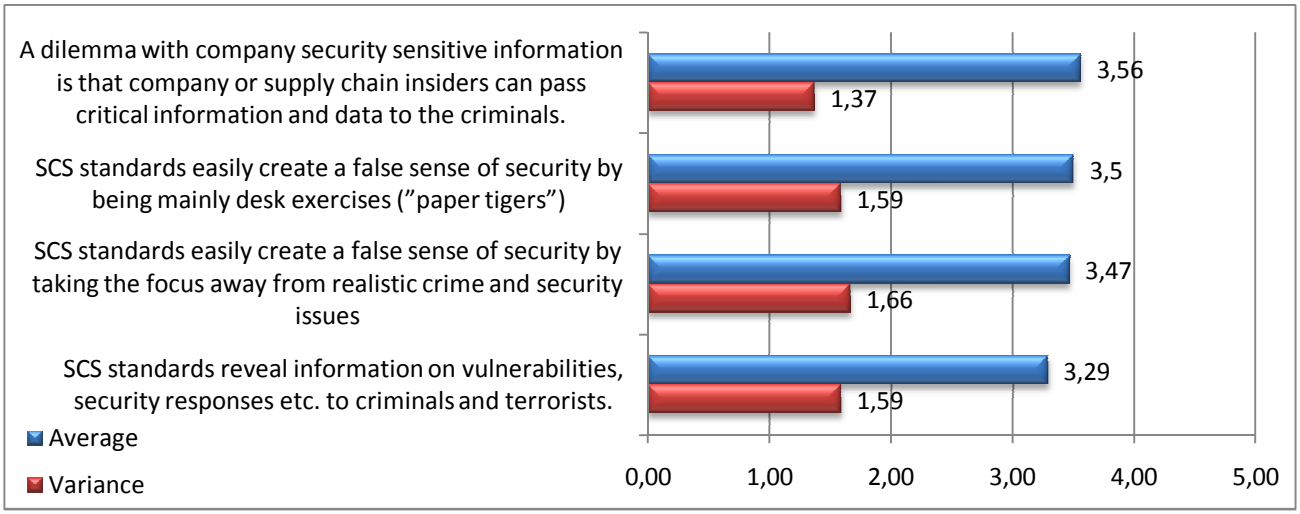

Figure 32 Views on potential dilemmas with SCS standards[70]

[70] A scale from 0 to 5 is used to show the answers accordingly: Fully agree(5) – Partially agree(4) – Neither agree or disagree(3) – Partially disagree(2) – Fully disagree(1). We start from 0 /include 0 to 1 in the scale because variances can be less than 1.

Box 17 False sense of security

By definition, a "false sense of security" makes someone feel secure when in reality s/he is not. Different situations and circumstances can create a false sense of security. A problem with SCS standards can be that certificated companies may have an unrealistic belief that the deployment of a SCS standard will shield the company from all criminal threats "Why should we worry about security issues anymore when we have an outstanding security standard deployed?" This fallacy may end up neglecting necessary day-to-day security management tasks.

The novelty of security technologies may also create a false sense of security, especially if the effectiveness of these technologies has not been proven. For example, it has been argued that the 100% scanning initiative introduced in the US will not deliver any real security benefits because criminals will still be able to gain access to the containers which have been already scanned.[71] Intuitive methods may also create a false sense of security: for instance, customs officials monitor physiological stress signals at the airports and use this in an attempt to detect smugglers; however, no one has managed to prove scientifically that stress and deception can be associated together with high confidence.[72]

Counterproductive security measures may also create a false sense of security when the virtuous idea of a security measure is, in reality, turned upside-down. The example given earlier with the case of drug smuggling from Mexico to the US, was facilitated by the illusion that SCS certificated companies would be the strongest link in the supply chain (in practice, smugglers exploited trucks of the certificated companies to ship marijuana across the border into the US).

The CBRA research team makes the straight forward recommendation for further research to be undertaken on all possible instances where people might be lulled into a false sense of security in order to identify and avoid such possibilities in the future.

5.8 Findings specific to possible new standard(s)

Finally, the operator survey findings specific to possible new SCS standards are presented, in descending order of preference, in Figure 33 below; noting that the last three items on the graph about modularity, mutual recognition, and multi-modal approach, are actually "negative form" statements, with words "not" and "less". All the 16 items are briefly discussed after the graph.[73]

[71] Report to Congress on Integrated Scanning System Pilots (Security and Accountability for Every Port Act of 2006, Section 231)
[72] Security Measures Lead To False Sense Of Security: Scientists Dispute Use Of National Security Tools (Science daily 2, 2009)
[73] A scale from 0 to 5 is used to show the answers accordingly: Fully agree(5) – Partially agree(4) – Neither agree or disagree(3) – Partially disagree(2) – Fully disagree(1). We start from 0 /include 0 to 1 in the scale because variances can be less than 1.

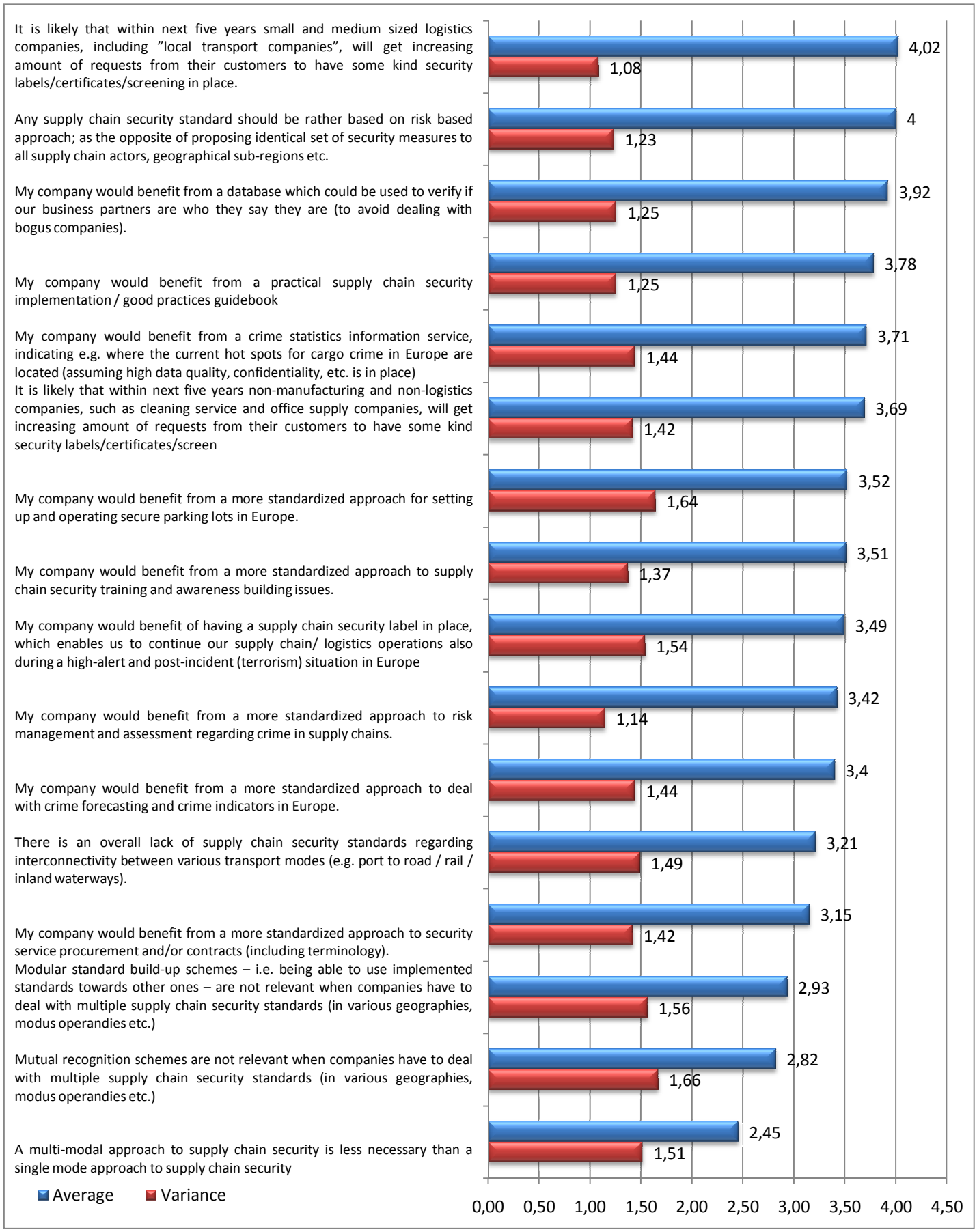

Figure 33 Findings specific to possible new SCS standard(s)

First, the items with an average of higher than 3.5 (in the opinion scale from 1 to 5, where 1 indicates high disagreement and 5 high agreement), are listed and discussed:

a) *Any supply chain security standard should be rather based on risk based approach; as the opposite of proposing identical set of security measures to all supply chain actors, geographical sub-regions etc*. = this argument has gained high consensus throughout the study process, thus a risk based approach becomes a framework level recommendation for any new SCS standard development in Europe.

b) *It is likely that within next five years small and medium sized logistics companies, including "local transport companies", will get increasing amount of requests from their customers to have some kind security labels/certificates/screening in place* = this view came originally from one expert during the interviews, and became enforced in the survey; it is brought to the study recommendations, but with certain disclaimers, mainly due to the cost and recognition concerns by the research team.

c) *My company would benefit from a database which could be used to verify if our business partners are who they say they are (to avoid dealing with bogus companies)* = this idea was indirectly hinted by one expert during the interviews; it would obviously be of good use in the markets; however, the research team questions the possibilities to take this further within the CEN framework, thus hesitating to recommend this for any immediate future development.

d) *My company would benefit from a practical supply chain security implementation / good practices guidebook* = this idea was given by couple of experts during the interviews, and the research team sees it as a value adding, practical and low cost (for the users) tool to share experiences on SCS success factors between the European supply chain operators; thus, becomes part of the final recommendations for further development (even though, to the best understanding of the research team, it would not make "an actual standard", but "just a guidebook").

e) *My company would benefit from a crime statistics information service, indicating e.g. where the current hot spots for cargo crime in Europe are located (assuming high data quality, confidentiality, etc. is in place)* = this idea was shared by two experts during the interviews; and based on the operator appreciation and anticipated low cost level for the users, it becomes a key recommendation for this feasibility study, to be detailed in the final chapter of this report.

f) *It is likely that within next five years non-manufacturing and non-logistics companies, such as cleaning service and office supply companies, will get increasing amount of requests from their customers to have some kind security labels/certificates/screening in place* = this is similar to the view b) above; and, with cost definition and recognition disclaimers, it becomes part of the set of final recommendations for the study.

g) *My company would benefit from a more standardized approach for setting up and operating secure parking lots in Europe* = this idea was hinted by couple of experts during the interviews; even though it´s relatively high operator survey ranking, and the common sense understanding of

parking areas being a weak spot for security in supply chains, the research team does not bring it to the front of possible standards to be developed to enhance SCS in Europe. The main reason being all parallel efforts carried out on this topic, and the lessons learned in them.

Second, the items with lower level of agreement, between 3.15 to 3.49 (in the opinion scale from 1 to 5, where 1 indicates high disagreement and 5 high agreement), are listed and discussed:

h) *My company would benefit from a more standardized approach to supply chain security training and awareness building issues* = training issues were hinted by one expert during the interviews. Even though the respondents do not see that high need here, the research team would consider combining this aspect with the possible good practices guidebook –initiative (if such was to emerge, as discussed in point d) above).

i) *My company would benefit of having a supply chain security label in place, which enables us to continue our supply chain/ logistics operations also during a high-alert and post-incident (terrorism) situation in Europe* = this idea was hinted by one expert during the interviews; even though it could be attractive for a small group of logistics companies in Europe, i.e. companies who want to be (also) doing business during such situations (a major strategic choice), the research team is not convinced of the practical feasibility of such a standard – at least it would require further research and analysis work.

j) *My company would benefit from a more standardized approach to risk management and assessment regarding crime in supply chains* = even though the relevance of risk management in the context of SCS standards was highlighted many times during the study, the actual standard idea on risk management with supply chain crime was ranked relatively low. Thus, the research team would not recommend to move forward with a "stand alone risk management" –standard; but possibly to consider it as part of a broader package with "process and data SCS standards"; to be explained in the last chapter of this report.

k) *My company would benefit from a more standardized approach to deal with crime forecasting and crime indicators in Europe* = this idea brought on the table by the research team itself was not rated high in the survey; thus, the only basis to continue with it towards any SCS standards would be to include it as part of "process and data SCS standards"; to be explained in the last chapter of this report.

l) *There is an overall lack of supply chain security standards regarding interconnectivity between various transport modes (e.g. port to road / rail / inland waterways)* = the lack of interconnectivity regarding SCS standards was not seen as a major issue by the respondents; this again is reflected at the final chapter of this report.

m) *My company would benefit from a more standardized approach to security service procurement and/or contracts (including terminology)* = this standard idea was hinted by one expert during the interviews; but the interest in the survey was not high; and, something on this area is likely to exist already; thus the research team would propose to drop this idea from further development agenda.

Third, the statements with "negative embeddings", i.e. "not" or "less" are listed and discussed. As they are in the graph between 2.45 and 2.93, it means that they all have a slight positive average interpretation by the survey respondents:

n) *Modular standard build-up schemes – i.e. being able to use implemented standards towards other ones – are not relevant when companies have to deal with multiple supply chain security standards (in various geographies, modus operandi etc.)* = this implies that modular build up schemes can be useful, i.e. if a company has already certain component of SCS in place, it could contribute towards a "broader SCS scheme"; however, the practical aspects are not clear for the research team.

o) *Mutual recognition schemes are not relevant when companies have to deal with multiple supply chain security standards (in various geographies, modus operandi etc.)* = this confirms to some extent the common observation that companies prefer their SCS standards to be mutually recognized by various SCS initiatives and authorities in global scale. Again, this could play a crucial role in any future SCS standard development; but is likely to have some obstacles to make it happen.

p) *A multi-modal approach to supply chain security is less necessary than a single mode approach to supply chain security* = this statement exposes slight preference by the respondents towards multi-modal SCS standards, over single mode / single actor based standards.

5.9 Conclusions

This operator survey chapter had the following two goals:

1. To test with actual European supply chain operators all the SCS standard ideas identified during the expert interviews of this study; and to draw preliminary conclusions on the feasibility of any new standards.
2. To explore facts and opinions within a broader frame of SCS management theories, principles, concerns etc.

Regarding the survey population one can note that a broad variety of supply chain actors (total of 86 valid replies) from manufacturing, logistics and trade businesses have replied; from many European countries; with all turnover levels covered; each bringing their sector or company or culture specific views on the table. At the same time, the sample size is relatively small, and the population contains some biases – thus one cannot claim a "statistically valid representation of all European businesses".

Regarding the broader frame of SCS management, trends, concerns etc., the following findings were made:

- Crime in supply chains, in particular cargo theft, is a growing concern in European supply chains; even though not any kind of "top management priority".
- Company internal policies and/or guidelines appear to be the most common way of managing security in the supply chains; followed by EU AEO; TAPA; and other public administration created standards.

- The most relevant benefit components include protection and promotion of company brand name; and reduction in the number / value of crime incidents.¨
- The concern with the lack of tangible benefits appears to be higher with government enforced SCS standards than with business developed SCS standards.
- The most relevant cost components include technology, infrastructure and procedural investments in facility and cargo security.
- Potential dilemmas with SCS include “company or supply chain insiders can pass information and data to the criminals”; and “SCS standards easily create a false sense of security”.

Findings specific to any new SCS standards, including “crime statistics reporting”, and “good practices guidebook”, are brought forward to the last chapter of this report.

6 Conclusions and recommendations

6.1 Introduction

Based on the findings made in this study, crime – in particular cargo theft – is perceived as a growing problem for supply chains in Europe. It is also perceived as an increasingly cross-border problem, caused by criminal organizations working internationally. Terrorism, on the other hand, is not perceived as a major threat in supply chains, by the experts and companies participating in this feasibility study.

One should seek for pragmatic, cost efficient solutions, to fight against crime in supply chains. Supply chain security (SCS) standards offer one possible avenue to introduce such solutions. Introduction of new European regulations is not necessary.

The last chapter of this feasibility study makes a handful of recommendations regarding the further development of possible SCS standards in Europe. The study conclusions and recommendations are presented in following structure:

- Chapter 6.2 Framework for SCS standards development
- Chapter 6.3 Recommendations for a European SCS standard
- Chapter 6.4 Recommendations for a SCS guidebook development
- Chapter 6.5 Brief notes regarding the other SCS standard ideas
- Chapter 6.6 Other aspects to consider in SCS standard development

6.2 Framework for SCS standards development

First, this study presents a framework for (any) future SCS standards development, in order to fix main focus points, priorities, development parties etc. for such work. The parameters in this framework, nine in total, reflect the points which were originally raised during the expert interviews, and - based on the findings in the literature, in the expert interviews, in the in-depth SCS initiative analysis, and/or in the operator survey – are now concluded with concrete recommendations, per framework issue –level. These recommendations are first visualized in Figure 34 below, and then discussed after the diagram.

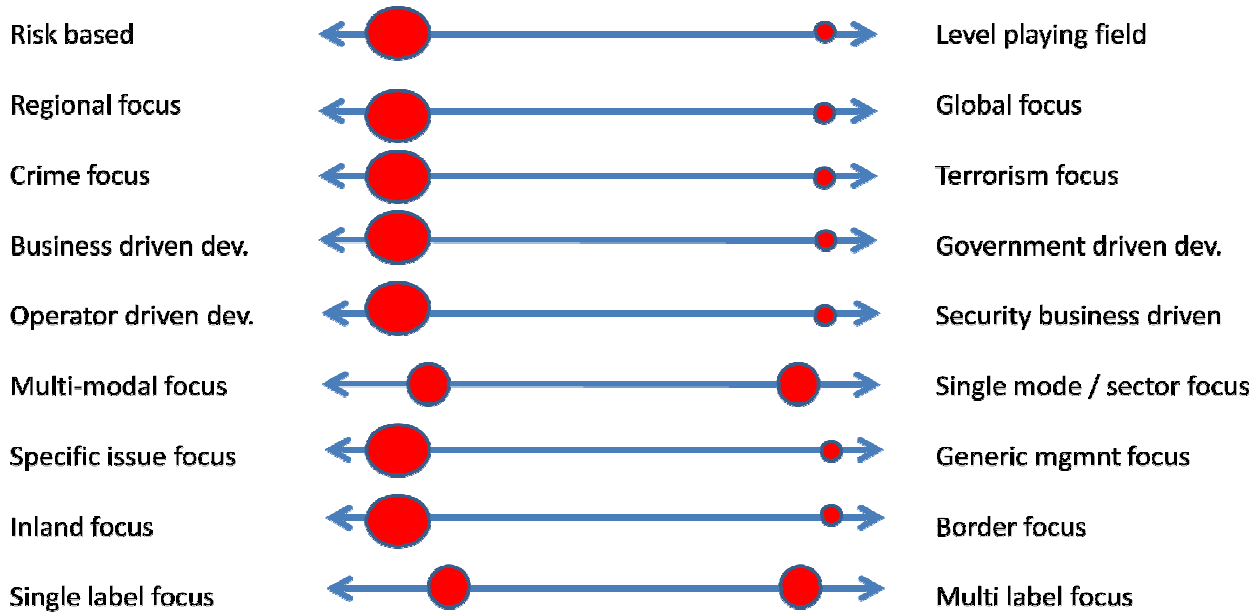

Figure 34 Final framework for SCS standards development

First, following the findings on this study, 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 into identical implementations of SCS requirements, independent on the differences in threats and/or vulnerabilities between various supply chains – geographies, industry sectors, transport modes etc. However, with some aspects of SCS standards there may be the minimum requirement level on how to implement it.[74]

Second, 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/or implementation lead time, than a global initiative. However, regional SCS standards should be linked with global (or other regional) standards, in order to facilitate global trade, and to support fight against crime on worldwide basis, whenever feasible.

Third, based on the study findings, the main focus of new SCS standards should be ”normal crime”, in particular cargo theft; instead of terrorism. However, in some cases one can work to ”kill two birds with one stone”, for example by developing a family of SCS standards, where one or more of them focus specifically on anti-crime issues, and one or more on anti-terrorism issues. In some cases, the same exact standard could work for both aims.

Fourth, regarding the development driver of new SCS standards, business 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.

[74] As illustrated with the small circle on next to ”Level playing field” parameter in the diagram above.

Fifth, within the business community, the main driver for any new SCS standards should be the supply chain operators, i.e. companies who manufacture, ship, transport, stock, distribute and sell the goods. However, security service and/or technology companies may be in the position to provide relevant expertize during the process, thus they should not be overlooked as sources of useful information.

Sixth, regarding the question whether new SCS standards should focus on multi-modal transport and interconnectivity between various transport modes; or to enhancing security for single actors and/or industry sectors, the recommendation is following: new SCS standards should not emphasize one over the other – but this decision should be made on case by case basis, potentially involving both aspects in the standard / family of standards.

Seventh, this study recommends focusing on SCS standards aiming to solve specific issues regarding crime in supply chains – instead of developing a generic management standard; or a ´another security check list´ – type of standard. However, it would be useful if the specific standards were linked into a broader management frame, or a standard – again to be solved on case by case basis.

Eight, regarding new SCS standards in the inland supply chain versus cross-border (EU external borders) supply chain context, this study recommends focusing in the former, simply due to the fact that various customs SCS programs exist already, and one should not duplicate them. However, new SCS standards should seek for links and/or recognitions with the existing customs SCS initiatives.

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

6.3 Recommendation for a European SCS standard

Based on the findings in this study, the research team recommends to develop ***a European standard for crime incident reporting***, based on the following reasoning:

- This standard idea was ranked reasonably high in the operator survey[75]; while the idea was never pointed as some sort of cost or other concern during the study.
- Practical experience with a limited number of European companies appears to be positive regarding the functioning and benefits of the scheme.[76]

Positioning this standard idea ("standard") within the framework presented in Figure 34 above, one can make the following observations and conclusions:

- This standard fits very well into the risk based approach -scheme, while the implementation of the standard would provide useful data for supply chain risk analysis purposes.

[75] The statement in the survey was: "My company would benefit from a crime statistics information service, indicating e.g. where the current hot spots for cargo crime in Europe are located (assuming high data quality, confidentiality, etc. is in place)".
[76] At least TAPA and EUROWATCH are working on this topic, for their members and/or customers.

- This standard has a strong focus on fight against transnational crime in Europe.
- This standard could be developed essentially by the supply chain operators themselves, while the implementation (data collection etc.) could be done in collaboration with the public authorities.
- This standard would look at both multi-modal as well as single mode / sector aspects in supply chain crime and security, wherever the reported incidents take place.
- This standard would have a specific ´fight against crime via better exploitation of data´ -focus; while it can be also connected to a broader SCS / company management system.[77]
- This standard would look primarily at crime issues inside Europe; at the same time, one can use it also in the real cross-border environment, for example in a partnership approach with customs.
- And, this standard would start as a simple, one label system; while it could be later included in a broader multi-label family of SCS standards.

Besides, the research team makes following two assumptions regarding such a possible standard:

- The team anticipates very low costs on the user side.[78]
- The team anticipates it to remain literally voluntary for any supply chain actor to adapt or not.

A further illustration of some of the possible details and characteristics of such a crime incident reporting standard is presented in Box 18 below – taking into consideration that the detailed scope and content of the possible standard would be created and agreed only at a later stage.

Box 18 Illustrative scenario for a crime incident reporting standard

Law enforcement agencies collect crime incident data and publish crime statistics. Crime investigating officer often has the possibility to decide which kind of information he gives out or publishes during the investigation process. If he keeps the case fully closed and incident reports are filed and compiled traditional way in official statistics, the most relevant data for prevention and protection purposes has evaporated beyond security professionals.

The statistics include information such as the number of criminal offences, prosecutions and convictions. Because the legal definitions of the crimes differ across countries, statistics cannot be reliably used for comparing levels of crime across countries at the European or international level. There is evidence that police compiled statistics data cannot be reliably used to estimate changes in the crime level, at least over a brief period of time. Furthermore, there are large differences in willingness of the citizens or companies to report crimes to the police.

International victimization surveys and voluntary incident reporting systems (e.g. TAPA and EUROWATCH) have proven to be more reliable and useful than police maintained statistics. However, these incident reporting systems cover only part of crime types, supply chains and industry sectors. Consequently, there is a need for crime incident reporting standard, which establishes common rules for incident reporting data, data collection and securing process independently whether the reporter/collector is a private company, association or public authority.

The incident reporting data could include the following information: incident place and time, product category, transport mode or other location type, conveyance, cargo transport unit, crime act description, bypassed protection measures and police reporting. The challenges for practical implementations are manifold. The data must be accurate enough and well-defined to qualify for comparing the efficiency of different security measures and for reliably assessing crime trends. Additionally, the challenge extends from the traditional specification of data requirements to security clearance and screening for individuals, who are authorized to access and process data and reports.

[77] For example in a PDCA – management cycle, providing important data for the Check-step.
[78] Basically a computer, web connection, and the time spent for data entry and report reading.

6.4 Recommendation for a European SCS guidebook

The second main recommendation of this feasibility study is to develop a ***Good practices guidebook for SCS implementations in Europe,*** - even if it would not be an actual standard, but "initiative" - based on the following reasoning:

- This initiative idea was ranked reasonably high in the operator survey[79]; while the idea was never pointed as some sort of cost or other concern during the study.
- Successful examples of good practices guidebooks exist in the field.[80]
- This initiative can support SCS training and awareness building processes.

Positioning this initiative idea ("initiative") within the framework presented in Figure 34 above, one can make the following observations and conclusions:

- This initiative fits very well into the risk based approach -scheme, while the good practice samples can be mapped with various risk levels in the supply chains.
- Some good practice cases can help to fight against transnational crime in Europe.
- This standard could be developed essentially by the supply chain operators themselves.
- This standard would look at both multi-modal as well as single mode / sector aspects in supply chain crime and security.
- This standard would have a specific ´fight against crime via better exploitation of knowledge´ - focus; while it can be also connected to a broader SCS / company management system.[81]

Besides, the research team makes following two assumptions regarding such a SCS initiative:

- The team anticipates very low costs on the user side.[82]
- The team anticipates it to remain literally voluntary for any supply chain actor to adapt or not.

The structure, style and content of this guidebook would need to be designed in the beginning of the possible follow-up process.

6.5 Brief notes regarding the other SCS standard ideas

Regarding any other SCS standard ideas collected during the expert interviews and tested in the operator survey, they were placed in three groups, with brief notes and recommendations by the research team.

Group 1. SCS standard ideas based on systematic processes and data exploitation consist of:

- ***Standard idea for SCS risk management and risk assessment***
- ***Standard idea for crime forecasting and indicators***

[79] The statement in the survey was: "My company would benefit from a practical supply chain security implementation / good practices guidebook".
[80] For example with the C-TPAT program.
[81] Including ISO 2800 series and EU AEO
[82] Basically time spent for the guidebook reading, and/or possible training sessions with the guidebook.

Even though these two were ranked relatively low in the operator survey, the research team proposes to consider them as possibly complementary components with the proposed crime incident reporting – standard – common dominators including process and data orientation, risk focus, fight against transnational crime, and low cost for users, amongst others.

Group 2. SCS standard ideas likely to require actual investments of facility, cargo, human resource and possible other SCS management areas are:

- ***Standard idea for logistics companies who are not entitled for EU AEO***; but may be requested (in the future) by their business partners / customers to have a "SCS label" in place.
- ***Standard idea for any "non supply chain operator";*** who may be requested (in the future) by their business partners / customers to have a "SCS label" in place.
- ***Standard idea for any company who wants to operate under "heightened security conditions"***[83]***;*** based on their own strategic decisions.

The research team sees some potential with a CEN SCS standard / family of standard to tackle these issues. However, additional research is required to explore this idea, and to build a proper business case around it. The additional case studies should follow this format:[84]

- Consider scenarios for the minimum security requirements, for each of the three ideas above.
- Carry case studies on cost implications, i.e. how much would it cost for say 20-30 sample companies to implement this.[85]
- Talk to relevant governmental parties on any type of recognition, modularity and other possible schemes.
- Analyze the process steps and costs for the possible certification and monitoring process.

Finally, based on the factual Cost-Benefit –analysis, the final conclusions and recommendation should be made.

Group 3. Other ideas for SCS standards – with relatively high ranking in the survey - include:

- Procedural and data content standard of capturing, storing, and verifying ***company registration data***; in order to minimize the risk of accidentally dealing with "bogus companies".
- Procedural and security measure standard for ***secure parking lots***; in order to minimize security incidents while trucks are parked for various reasons.[86]

However, the research team does not have adequate information on how realistic these two standard scenarios are; what work has been done already; what are the legal and other constraints, both on national and on European level, etc. Thus the recommendation is to set these ideas aside, and maybe visit them again in 1-2 years time.

[83] One can learn some aspects related to this idea from the European COUNTERACT-project.
[84] The research team estimates that this process would require 6-9 months process, to carry out a meaningful, high quality analysis, with a minimum of 20 case companies on board.
[85] Each case company may have a different starting point with their existing SCS measures.
[86] EC DG TREN, and TAPA, amongst other possible parties, are doing some work on this topic.

6.6 Other aspects to consider in SCS standard development

Several other aspects to take into consideration, on case by case basis, when considering any new SCS standards, are listed in Box 19 below, titled "From SCS to Value Cain Security (VCS) Management". Again, one should not exploit it as a flat check list, but instead consider each VCS-component if and how it could make sense in any future standardization work.

Box 19 From SCS to Value Cain Security (VCS) management.[87]

Value Chain Security (VCS) management can be characterized by:

- Is strongly bases on risk management principles.
- Looks at crime hazards and security both upstream (including supplier factories) and downstream (including consumer outlets) the logistics chain / network.
- Covers a broad spectrum of possible crime types (or perceived crime types) in the value chain.
- Covers a broad spectrum of possible security responses in the value chain, aiming to find a balance between preventive, detective/reactive and recovery measures
- Considers broad SCS theories and dynamics, when designing new standards; including situational crime prevention; security scope (prevent; detect/react; recover); and continuous improvement cycle
- Exploits existing standards and good practices to the maximum benefit, and learns actively from the dilemmas, shortcomings and weaknesses with previous SCS initiatives.
- Aims to optimize the total level of security spending in the value chain, in relation to proactive, mandatory and reactive security costs.
- Requires a broad intra- and inter organizational collaboration schemes for a sustainable implementation.
- Highlights the relevance of public-private collaboration.
- Is careful with ´security secrets´ and pays attention to avoidance of ´counterproductive security´.

[87] The term ´Value Chain Security, VCS´ was first presented in public by Mr. Hintsa, during a student lecture at HEC University of Lausanne, 13.11.2009. Behind the VCS philosophies there is a CBRA working paper (2010) "From Supply Chain Security (SCS) to Value Chain Security (VCS) Management" (to be published in 2010 as a journal paper: Hintsa J., Ahokas J., Männistö T., Sahlstedt J., Journal tbd.)

References

APEC Private Sector Supply Chain Security Guidelines, 2005. Available at: http://www.apl.com/security/documents/APECSupplyChainSecurityGuidelinesfinal1.pdf [Accessed January 14, 2010].

Bowers, N., L., Gerber, H., U., Hickman, J., C., Jones, D., A. & Nesbitt, C., J., 1989. Actuarial Mathematics. Itasca, Illinois: The Society of Actuaries.

Bühlmann, P., H., 1985. Premium calculation from top down. ASTIN Bulletin.

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

Cornish, Derek B. & Clarke Ronald V., 1986.The Reasoning Criminal. The rational choice perspective on Offending. Springer-Verlag.

Europol The Threat of Organized Crime report, 2006. Available at: http://www.europol.europa.eu/publications/European_Organised_Crime_Threat_Assessment_%28OCTA%29/OCTA2006.pdf [Accessed January 14, 2010].

Europol, 2008. OCTA – EU Organised Crime Threat Assessment. Available at: http://www.europol.europa.eu/publications/European_Organised_Crime_Threat_Assessment_%28OCTA%29/OCTA2009.pdf [Accessed January 14, 2010].

Eurowatch Freight Crime Bulletin, 2008. Available at: http://docs.google.com/gview?a=v&pid=gmail&attid=0.1&thid=1227381c37985a30&mt=application%2Fpdf [Accessed January 14, 2010].

Factory mutual, 2000. Burglary and Theft - Property Loss Data Sheets

Felson, M., Clarke R., V., 1998. Opportunity makes the Thief – Practical theory for crime prevention, Police Research Series, Paper 98, Home Office Policing and Reducing Crime Unit.

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.

Harland, C., Brenchley, R. & Walker, H., 2003. Risk in supply networks. *Journal of Purchasing and Supply Management*, 9(2), 51-62.

Hintsa, J., Ahokas J., Männistö T., Sahlstedt J., 2010. From Supply chain security (SCS) to Value chain security (VCS). *CBRA Working paper*.

Hintsa, J., Wieser, P., Gutierrez, X., Hameri, A-P, 2009. Supply chain security management: an overview. *International Journal of Logistics Systems and Management*, Vol. 5, No. 3-4: 344-355

Kesting, D., H., 2007. Risk report: “Hedging climate change”. Allianz SE.

Khan, O. & Burnes B., 2007. Risk and supply chain management: creating a research agenda. *The International Journal of Logistics Management* Vol. 18 No. 2 , pp. 197-216.

Kliger, D., Levikson, B., 1998. Pricing insurance contracts - an economic viewpoint. Insurance: Mathematics and Economics 22 , 243-249.

Liem, K., 2009. The European security research programme. Inland Transport Security seminar, Geneva, 15 January.

Lowrance, W., 1980. The nature of risk. In A. Schwing, How Safe is Safe Enough? New York, NY: Plenum Press.

Mitchell, V.-W. 1995. Organisational risk perception and reduction: a literature review. *British Journal of Management*, Vol. 6 , pp. 115-33.

Moore, P., 1983. The Business of Risk. Cambridge: Cambridge University Press.

Sarathy, R., 2006. Security and the global supply chain. *Transportation Journal*, Vol. 45 No. 4, pp. 21-28.

Simon, P., Hillson, D. & Newland, K., 1997. Project Risk Analysis and Management Guide (PRAM). Norwich: Association for Project Management.

Singhal V. & Hendricks K., B., 2005. Association Between Supply Chain Glitches and Operating Performance. Management Science.

UNODC Global reports on trafficking in persons, 2009. Available at: http://www.unodc.org/documents/Global_Report_on_TIP.pdf [Accessed January 14, 2010].

Waters, D., 2009. Supply Chain Management: An introduction to logistics. Palgarve macmillian.

Weisburd, D., 1993. Contrasting Crime General and Crime Specific Theory: The case of Hot spots of Crime. *Advances in criminological Theory*, Volume 4.

World Bank Supply Chain Security Guide 2009 Available at: http://siteresources.worldbank.org/INTPRAL/Resources/SCS_Guide_Final.pdf [Accessed January 14, 2010]

Voss, M.,D., 2006. The Role of Security in the Supplier Selection Decision. Michigan State University, 192 pages.

Zsidisin, G., 2003. Managerial perceptions of supply risk. *Journal of Supply Chain Management*, Vol. 39 No. 1 , pp. 14-25.

Annex 1. Operator survey questions (see separate file)

Annex 2. Report presentation slides, Dec.2009 (see separate file)