

# SUPPLY CHAIN SECURITY MANAGEMENT: AN OVERVIEW

**Juha Hintsa, Dr. Philippe Wieser, Ximena Gutierrez, Dr. Ari-Pekka Hameri**

*HEC University of Lausanne, Ecole Polytechnique Fédéral de Lausanne*

*Cross-border Research Association (CBRA), Lausanne, Switzerland*

[juha.hintsa@cross-border.org](mailto:juha.hintsa@cross-border.org), [philippe.wieser@epfl.ch](mailto:philippe.wieser@epfl.ch),

[ximena.gutierrr@epfl.ch](mailto:ximena.gutierrr@epfl.ch), [ari-pekka.hameri@unil.ch](mailto:ari-pekka.hameri@unil.ch)

**Abstract:** Supply Chain Security Management [SCSM] is a relatively new discipline in the field of Operations Management Research, thus lacking introductory and tutorial papers. The recent concerns on security in global supply chains are driving the introduction of new security initiatives, standards and measures to such an extent that they are becoming an integral part of supply chain management. This paper presents the current state of SCSM initiatives, and discusses their managerial implications, including the importance of interplay between various parties, i.e. authorities, manufacturers, distributors etc., to support the fluent and secure flow of goods in the global economy. The paper concludes that a gap exists between theoretical supply chain security studies, emerging security standards and practical managerial actions, and that the academic research community has a clear mission to bridge this gap, e.g. via pragmatic case studies within real world supply chains.

**Keywords:** Supply Chain Security Management, Supply Chain Security Programs, Supply Chain Security Standards

## 1 Introduction

Security, its demands and constraints, constitute obstacles (logical and physical barriers) in the flow of supply and distribution. These “barriers” created by a perceived increased need for security, or political reasons, reduce the reaction capacity and the physical and economical performance of the company. Integrating the security dimension into the logistics strategy, organization and operations has become a new challenge for supply chain management.

The recent security concerns have led to the development of multiple initiatives and potential solutions to enhance security in international supply chains without affecting efficiency. Businesses, governments and researchers are tackling the problem from different perspectives and by using several methodologies. However, inherent complexities such as the large quantity and diversity of the actors involved in international supply chain processes, and the need to identify cost-effective security measures, have generated multiple academic research questions in the domain of SCSM. Among others, the relevant research topics can include:

- What government- and business-community driven *SCSM programmes, regulations and standards* have emerged since 9/11 and will emerge in the foreseeable future?
- What are the *new security measures* and paradigms that companies should implement, and which will affect their existing SCSM practices?
- What are the *real cost and operational impacts* that SCSM programs, regulations and standards have on companies – from small- and medium-sized enterprises (SMEs) to Multinational Companies (MNCs), at various industrial and national levels?

- What are the *broader topics surrounding SCSM* initiatives and decisions, including global trade facilitation, technical trade barriers etc.?

This SCSM paper aims to present a pragmatic framework for future research, regulations development, and industry practitioner purposes, with the following three-step approach:

- By providing an overview of SCSM background and evolution.
- By providing an overview of existing SCSM initiatives from governments, businesses, international organizations and researchers, and by working out a preliminary framework to classify them.
- By presenting possible impacts for business actors of international supply chains; and discussing the future views and predictions.

## **2 Supply Chain Security Management Background**

By SCSM, we mean enhancing and embedding the traditional security management aspects into holistic management of integrated supply chains, especially within a global context. SCSM has roots in multiple fields: Supply Chain Management; International Trade, Logistics and Cross-border Operations Management; Supply Chain Resilience Management; Quality Management; Risk Management; Insurance Policies and Instruments; and Customs Policies, Procedures and Reforms.

Since 2001 governments, Customs administrations, international organizations, researchers, and businesses have carried out diverse actions, and delivered different types of reports, and articles on the topic. The first pure SCSM paper was published at MIT (Sheffi, 2001), a few months after the infamous terrorist attacks in September 2001. Since then, researchers and industrial practitioners have organized and published SCSM conference and journal papers, primarily in the US but also in Europe and other continents.

Most of the researchers, presently contributing to building SCSM theory, have mainly been active in research fields such as Transportation and Logistics (i.e. Sheffi & Rice, 2003), Supply chain Management (i.e. Lee & Wolfe, 2003) and Supply chain risk and vulnerability (i.e. Christopher & Peck, 2004). The existing literature on SCSM, is somehow adding a layer of security to each researcher's own expertise domain. Some of the discussed principles are presented in the following paragraphs.

Sheffi (2001) presents the need for companies to simultaneously operate under heightened security environments and the need to prepare for rapid recovery after terrorist attacks. In addition he establishes seven supply chain design trade-offs that management will face when designing secure supply chains: i) Repeatability vs. unpredictability ii) The lowest bidder vs. the known supplier. iii) Centralization vs. dispersion. iv) Managing risk vs. delivering value. v) Collaboration vs. secrecy. vi) Redundancy vs. efficiency and vii) Government cooperation vs. direct shareholder value.

Rice et al. (2003), presents the need for companies to simultaneously build secure and resilient supply chains. He identifies potential actions to improve physical, freight and information security, classifying them into four levels: Level 1 – Basic (i.e. physical security measures such as access control, badges, camera systems); Level 2 – Reactive (i.e. existence of supply continuity plans, analyse of supply bases); Level 3 – Proactive (i.e. Advanced cyber security, Business continuity plans); and Level 4 – Advanced (i.e. learning from past disruptions, formal security strategies).

Lee et al. (2003) draws lessons from total quality management programs applicable to the world of supply chain security management. Following the famous slogan from quality management, he argues that security is free; as long as it is assured with security measures that also increase supply chain efficiency.

Christopher & Peck (2004) argue that the challenge is to manage and mitigate supply chain risk by creating more resilient (flexible, agile) supply chains. They establish the four basic principles that support resilient supply chains: i) resilience should be designed in the processes. ii) There is a need for a high amount of collaboration iii) resiliency implies agility, which means being able to react quickly and iv) fostering a risk management culture within an organization is a prerequisite for resiliency.

Apart from researchers, governments and international organisations are currently very active in the design of supply chain security programs, regulations and standards, while businesses are settling for mandatory measures and participating in the design of some of these new measures. It could be argued that at the present time, the main challenge facing governmental actors is to define and implement adequate control measures which increase security without jeopardizing trade or burdening themselves and businesses with additional excessive operational costs. The main challenge for businesses is to invest wisely in security in such a way that they comply with the new regulations and at the same time achieve potential additional benefits that contribute to their supply chain efficiency.

The interaction between all these actors, shall define the future of SCSM as a new research discipline. It has yet to be determined whether academics will contribute to the development of security standards and policies or whether the new security regulations will constitute new restrictions to be tackled by the academic world. In addition the lack of academic papers mapping the research into practical actions in the real world is still a great chasm that has to be bridged.

### **3 Supply chain security responses and actions**

Multiple types of responses and actions have been undertaken by different governmental organisations, international organisations and businesses to enhance global supply chain security. These reactions range from country specific operational regulations to global research programs. They have different originating agents and they target specific goals. An extensive literature review, the multiple conference venues, discussion groups and security related events have allowed researchers to identify the most appropriate responses and actions in this field. It has been observed that most of these initiatives vary in the following ways:

- i) Type of originating actor: International organizations, governmental agencies (i.e. Customs administrations; Frontier guards; Border police; Transportation authorities; Home affairs offices, etc.), private sector.
- ii) Transport mode (sea, air, road, rail)
- iii) Enforceability: Mandatory vs. voluntary,
- iv) Main specific goal: Enhancing Customs administrations security control capacity, reducing specific industry/geography vulnerability, developing global security standards, Technology development.

The following table presents an extensive list of the existing initiatives, organized by the category iv) described above, and by providing the value for the other dimensions presented.

**Table 1.** Classification of security initiatives by type of specific goal

<b>Enhancing Customs Administrations security control capacity</b>				
Action/ Response	Originating actors	Transport modes	Enforceability	Examples
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), Secured Export Partnership (New Zealand)
Preventing at the source and using advance 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	24 hour rule advance manifest rule and 96-hr notification of arrival vessel
<b>Reducing specific industry/geography vulnerability</b>				
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 risky transport modes	International Organisations	Sea	Mandatory	ISPS by IMO
		Air	Mandatory	Aviation security plan of action by ICAO
<b>Developing global security standards</b>				
Establish security standards that can be generalized for the entire Customs and trading community	International Organisations	All	Voluntary	WCO Framework of Standards to Secure and Facilitate Global Trade.
Become the leading supply chain security management standard.		All	Voluntary	ISO (International organization for standardization)
<b>Technology development and deployment for security purposes</b>				
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.

Apparently there is a great variety of initiatives, all targeting supply chain security enhancement, but from different perspectives. However, a closer analysis of the concrete security measures promoted by each initiative showed that there are several areas in which they overlap or at least are interconnected. For instance, it was observed that the practical SCSM measures proposed by various initiatives typically fall into the following five intuitive categories (for more details see Gutierrez et al. 2006):

**Table 2.** SCSM practical measures categories

Category	Samples of practical security measures
<p><b>1. Cargo management:</b> Protecting cargo during all steps of manufacturing, shipping and transport processes.</p>	<ul style="list-style-type: none"> <li>• Efficient prevention, detection and reporting of shipping process anomalies (routes and schedules continuous review; alerts management, etc.)</li> <li>• Adequate inspections during the shipping process (in points where liability changes, to packaging materials and vehicles before being in contact with cargo etc.).</li> </ul>
<p><b>2. Facility management:</b> Guaranteeing the security of the facilities where goods are manufactured and cargo is stored and handled.</p>	<ul style="list-style-type: none"> <li>• Optimal warehouse/terminal layout design (entry/exit controllability; clearly marked control areas; sufficient light conditions etc.)</li> <li>• Efficient facility monitoring (24hr camera system, security guards, filming activities of loading containers, picking etc.).</li> </ul>
<p><b>3. Information management:</b> Protecting critical business data and exploiting information as tool for detecting illegal activities and preventing security breaches.</p>	<ul style="list-style-type: none"> <li>• High protection of business information/data (management procedures and storing methods designed to protect information from unauthorized access and usage)</li> <li>• Accurate and complete recordkeeping of shipping information for potential security audits (improved recordkeeping methods; quality control of records, errors correction etc.).</li> </ul>
<p><b>4. Human resources management:</b> Guaranteeing trustworthiness and security awareness of all personnel with physical or virtual access to the supply chains</p>	<ul style="list-style-type: none"> <li>• Professional employee hiring / exit process (background checks; interviews for leaving or fired employees etc.)</li> <li>• Efficient information dissemination process (internal and external publication of the company security policies).</li> </ul>
<p><b>5. Company management systems:</b> “Building security” into internal and external organizational structures and company management systems, including supplier, partner and client management processes</p>	<ul style="list-style-type: none"> <li>• Adequate business partners evaluation system (selection of low risk and high security compliant suppliers, clients and subcontractors)</li> <li>• Complete company security management system (defined security processes, defined and controlled security indicators, internal and external audits, etc.)</li> </ul>

It was observed that Cargo management is emphasised by most of the prevailing security initiatives. Facility management and Human resources management are mainly mentioned in supply chain security programs created either to enhance Customs administrations security control capacity or to reduce specific industry/geography vulnerability. It was noted that practical measures falling into Information management category are a very important component of the efforts to enhance Customs administrations control capacity. For instance the 24 hour advance manifest rule and 96-hr notification of vessel arrival are part of the few existing mandatory measures, and consist of managing the information flow on cargo in such a way that the risk can be detected before the physical flow arrives at the border. Finally, the fifth category provides the broadest view of SCSM.

Measures that fall into this category appear to be less straightforward to implement. There might be multiple potential good ways to implement them and different criteria to decide upon the required security level for a company, depending on its specific situation. In addition, it is highly probable that the implementation of these measures will require changes at strategic levels.

Apart from the actual SCSM measures, one should also consider the emerging SCSM (sub)-paradigms and their possible implications, such as:

- ‘Advance cargo information’ schemes refer to sending cargo- and trader-related Customs clearance and other data before goods arrive at certain points, i.e. border crossings or even pre-departure.
- ‘Known shipper’ and ‘authorised economic operator’ schemes mean identifying trustworthy companies which are given privileges in international supply chains.
- ‘Secure trade corridor’ schemes mean creating security controlled end-to-end transportation pipelines with state of the art tracking, screening and other capabilities, especially in the maritime environment.
- ‘Security built into products and processes’, and ‘integrated supply chain security management’ mean embedding security deep into the business, e.g. by following analogical approaches of total quality management while creating secure supply chains.

It can be argued that although there are common elements among many initiatives, each of them is nevertheless an independent effort to tackle different aspects of SCSM. Most of them are still in the developing stage and they will continue to suggest new operating processes and protocols, regulations and adoptions of new technologies. Whether or not these initiatives will converge is a new research question for the SCSM discipline. The authors of this paper believe more in opt for the “mutual recognition” between them, rather than in the establishment of a single global security standards system. There is a discrepancy between the development of security standards and the practical actions taken within companies worldwide – it would be beneficial to bridge the gap in the future, or at least oblige companies to take more actions.

## **4 Managerial Implications and Discussions**

The logistic function of a company must integrate this new security managerial dimension into its strategy and organization along the whole supply chain. The logistician should help managers to realize the importance of taking into consideration the security demands from the conception and development of the product to its final distribution to clients. Following the previous chapters in this paper on SCSM background, initiatives and measures, one should consider what kind of managerial implications SCSM is already having and is likely to have in the future. These issues are discussed below.

### Expectations and Impacts

It is obvious that various industrial sectors have different backgrounds and attitudes towards SCSM. Some sectors have been traditionally governed by strict safety regulations in order to avoid explosions and other accidents (e.g. chemicals and petroleum), consumer problems (e.g. food and pharmaceuticals) etc. For them, many of the “new” SCSM measures are relatively easy, sometimes even trivial, to implement. Companies dealing with high value goods and / or easily tradable stolen goods (consumer electronics, tobacco etc.), and with dual-use type products also have a long tradition of highly protecting their assets. Therefore new SCSM initiatives might not require major investments

Most companies expect direct benefits from SCSM by immediate reductions in the following problem areas: theft, smuggling, counterfeit, and loss and damage, all of which are closely connected to the security measures described in the previous section. In addition, SCSM measures can help to avoid any kind of business disruptions, and to recover more quickly if something goes wrong, either due to internal or external factors; thus improving supply chain resilience. Such disruptions may include disruptions in supply, in transportation and at company facilities, freight breaches, and disruption in communications; they may be caused by accidents, fires, acts of nature, labour disputes, ordinary criminals etc. It is possible that reduction of such disruptions may happen already, thus justifying some of the SCSM investments. Besides reducing various risks in supply chains, SCSM may contribute to multiple collateral benefits, as presented in a recent paper by Rice et al. (2005).

Governments, in particular Customs administrations seem to be eager to announce various types of benefits for supply chain actors who take proactive, highly compliant roles in their SCSM measures. In principle, the set of incentives could be grouped into the following three categories: (i) fast border flow under normal conditions, i.e. when no special threats are foreseen, “business as usual”; (ii) Fast border flow under special conditions, e.g. high alert and post-disaster situations; and (iii) Other possible incentives, e.g. tax incentives, connections with trade compliance / “traditional Customs incentives”; regulation consulting partnerships etc. However, for the time being it is still unclear how such potential benefits will evolve into measurable format.

One of the key questions regarding the future of SCSM is that of money: how much “it” will cost, and who will be the direct and indirect “payers”. Interviews show that some MNC’s seem to tolerate the introduction of some 10 to 30 USD security fees per container shipment quite well, by their LSP’s, who claim such fees would cover in particular port and airport cost increases. At the same time, some companies notice that the “new” security fees are being added to their freight bills, even though the tasks were performed already before the past terrorist attacks. It is unlikely that a consensus will be reached as to how security should be priced – and by the end of the day, the final consumers will be the ones who pay.

Multiple concerns are being raised by various political, business and academic actors surrounding the broad picture and future of Supply chain security management (SCSM). Development agencies are highly concerned about the potential for introducing new trade barriers, affecting developing countries in particular, who may lack the resources and may not be able to afford the investments and operational costs set by SCSM requirements and expectations from industrial countries. Also SMEs at both developing and developed regions may find themselves in another “regulatory jungle” without resources to comply with all the SCSM aspects, and thus being cut out of part (or all) of international trade. In the worst case scenario, the trading world will be divided into two sections, “known parties” and “unknown parties”, where the latter will find themselves finally being pushed out of business.

#### Future projections

It is clear that the SCSM standardization work will continue to be driven by both governmental as well as business communities. It appears that an important part of this responsibility may be shifting to regional and global standardization bodies, such as CEN

(European level) and ISO (global level). How to create and manage truly global, enforceable standards for the SCSM, remains an open question for future research and challenges various decision makers in the field. Also, the whole mechanism, from SCSM certification to auditing, remains open for the time being, including defining the main responsible government authority / authorities for the process, such as Customs, transport and other authorities.

It is evident that multiple expanded and new businesses are emerging around SCSM, while companies from various sectors, including aerospace and defence technologies, security technologies and services, Information Technology and services, shipment inspection and trade compliance services, management consulting etc., are seeking for new business and revenue opportunities. This includes new SCSM technologies, IT platforms, consulting, training and auditing services etc. It remains an open question as to which sectors and partnerships will manage to create the most reliable and cost efficient solutions and services for long-term success in the field. The pricing and financing of security, SCSM public-private-partnerships and other business and fiscal aspects remain a topic for future research.

Logistics should increasingly be the function capable of integrating the security dimension along the whole supply chain of a product or a service, in order to guarantee the reactivity and performance of any given company. Thus, the academic research community has a clear mission to bridge the gap between theoretical supply chain security studies, emerging security standards and practical managerial actions. One way of doing this is to proceed with pragmatic case studies on supply chain security implementation models in the context of real world supply chains.

## **5 References**

- Christopher, M. and Peck, H (2004). Building the Resilient Supply Chain, *International Journal of Logistics Management*, Vol.15, No.2, 2004, pp1-14.
- eyefortransport (2005). Cargo and Supply Chain Security Trends 2005. eyefortransport Cargo & Supply Chain Security Report. August 2005.
- Gutierrez X., Hintsas 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, 2006.
- Hintsas, J., Hameri, AP., Tsikolenko V. (2005). Impacts of New Supply Chain Security Regulations and Programmes in International Trade and Cross-border Operations Automation Systems – A Preliminary Study. The First International Conference on Transportation Logistics, Singapore, 27-29 July 2005.
- ISO28000 (2005). Specification for Security Management Systems for the Supply Chain. Draft publicly available specification ISO/CD/PAS 28000.
- Lee, Hau L. and Wolfe, Michael, (2003). Supply Chain Security Without Tears, *Supply Chain Management Review*, January/February 2003.
- Rice, Jr., J. B. and Caniato F. (2003). Building a Secure and Resilient Supply Network, *Supply Chain Management Review*, September-October 2003.
- Rice Jr. J. B. and Spayd P. W., (2005). Investing in Supply Chain Security: Collateral Benefits, IBM Center for The Business of Government, May 2005.

Sheffi, Yossi, (2001). Supply Chain Management under the Threat of International Terrorism, *The International Journal of Logistics Management*, Volume 12, Number 2 2001.

Sheffi, Y. and Rice Jr., (2003), Supply Chain Response to Global Terrorism: A Situation Scan, EurOMA POMS Joint International Conference, June 2003.

Velea, I., Hintsä, J., Hameri, AP. (2005). Internet as an Information Delivery Channel for Supply Chain Security Information from Customs Administrations to Trade and Logistics. The First International Conference on Transportation Logistics, Singapore, 27-29 July 2005.

WCO (2005). WCO Framework of Standards to Secure and Facilitate Global Trade. June 2005.

Willis, H.H. and Ortiz, D.S., (2004). Evaluating the Security of the Global Containerised Supply Chain, RAND Corporation, 31 pages.

## **6 Biography**

JUHA HINTSA has a Master of Science (Eng.) degree from Helsinki University of Technology, in Industrial Management and Artificial Intelligence (1994). After working eight years in steel manufacturing and supply chain software industries, he started a global Cross-border Operations and Supply Chain Security Management research program (Cross-border Research Association, CBRA; [www.cross-border.org](http://www.cross-border.org)) in close collaboration with DHL, World Customs Organization and HEC University of Lausanne (summer 2001). He became full-time Research Assistant and Doctoral Candidate at HEC Lausanne in 2003, and he is aiming to complete his Doctoral Thesis by end of 2006.

PHILIPPE WIESER, born in 1954, obtained his diploma of engineer in mechanics at the EPFL in 1977 and he got his PhD in 1981. After a few years working in an engineering consulting company, he joined the EPFL as lecturer. His fields of research and teaching deal with logistics and information systems and integrated logistics. Since May 2000, Mr. Wieser is the executive director of IML: International Institute for the Management of Logistics (EPFL - Lausanne and ENPC - Paris). Mr. Wieser teaches in EPFL-Lausanne (Master and Executive Master MSL) and ENPC-Paris (Executive Master). He is author and co-author of more than sixty publications.

XIMENA GUTIERREZ has a Master of Science in Industrial Engineering from Universidad de Los Andes, Columbia and an Executive Master's in Management of Logistical Systems from Ecole Polytechnique Fédérale de Lausanne (EPFL), Switzerland. She is a PHD student at the Collège de Management at EPFL and is mainly interested in Logistics, Supply Chain Security and Cross-border Operations Management.

ARI-PEKKA HAMERI is full professor of operations management at University of Lausanne, Switzerland. He has been involved with numerous EC-funded and other international research projects dealing with industrial IT and operations and supply chain management. He has published over 50 articles in international management and science journals concerning industrial IT, and management of production, projects and supply chains.