VOLUNTARY SUPPLY CHAIN SECURITY PROGRAMS: A SYSTEMATIC COMPARISON

Ximena Gutierrez, Juha Hintsa
Cross-border Research Association, Lausanne, Switzerland ; EPFL ; HEC Lausanne

Abstract: International crime and terrorism has become a major concern to both governments and businesses, due to the vulnerability of international supply chains of being either a direct target for crime and terrorism, or a means to deliver weapons. In response to this new threat, several voluntary supply chain security programs have been created or modified. This paper analyses and compares nine different security initiatives around the world, to establish their compatibility and identify the security measures that may become mandatory in the near future. The study is carried out as an archive study, supported by direct input from various program experts.

Keywords: Supply chain security (SCS) management, SCS voluntary programs, SCS standards, SCS certifications.

1 Introduction

Companies have always dealt with disruptions that affect the efficiency of their supply chains. Disruptions can arise from a number of sources such as natural disasters, terrorist attacks, industrial or direct action, accidents, or operational difficulties (Willis and Ortiz, 2004). Their effects can be the delay or unavailability of material from suppliers, the violation of the integrity of cargoes or the delay or unavailability of communication infrastructure (Rice Jr. and Caniato, 2003). To protect their personnel and physical assets, companies rely on internal safety and security programs. However, the tremendous damage caused by the emergent international terrorism against developed economies highlights the vulnerability of current global supply chains and places the security issue at the top of the agenda of several governments and international organizations around the world. Enhancing global supply chain security has shifted from being a pure public or private concern to a public-private joint objective. The philosophy behind this new trend is that in order to enhance security in a cost-effective way, it is necessary to create and exploit synergies between the public and the private sectors.

Some governments and international organizations have already established binding regulations to be followed by some of the participants in international supply chains (e.g. ISPS code[1] for ports and ships and the 24 Hour Advance Manifest Rule for traders wanting to export to the United States of America). However, these regulations represent only a small part of all the potential security measures that could be implemented by these and other supply chain actors in order to secure the global movement of goods. Sheffi (2001) was the first to draw attention to the implications of this challenge for those managing international supply chains. He argues that companies will need to adjust their relations with suppliers and customers, contend with transportation difficulties and amend their inventory management strategies. Rice Jr. et al. (2003) identifies a set of security measures implemented by major global companies from different industry sectors as a response to this new threatening environment. The measures range from

[1] ISPS : International Ship and Port Facility Security code.

Paper prepared for ILS 2006, The International Conference on Information Systems, Logistics and Supply Chain. Lyon, France, May 15-17, 2006.

basic initiatives such as controlling access to facilities and employee background checks to advanced initiatives such as the creation of emergency control centers and a comprehensive security strategy. In addition to these individual responses from the business sector, several governments and border agencies are promoting voluntary supply chain security programs as a concrete option for public-private collaboration intended to enhance security. Most of these programs consist of a set of security measures recommended by the originating government or border agencies as best practices to guarantee security in the supply chain. Companies complying with (specific) security measures are considered "secure traders" and therefore will receive preferential treatment when crossing borders (e.g. will benefit from reduced inspections and lower risk rating).

These voluntary programs are of special interest for three main reasons: i) Even if they are promoted as voluntary, the cost of not being involved can be so high (due to more inspections, higher potential fees etc.) that companies may be obliged to engage if they want to benefit from acceptable conditions when crossing borders. ii) Companies involved in these programs will face the great challenge of implementing the required standards in a cost-effective way. In spite of the general guidelines that must be followed to become certified there remains a great degree of freedom as to how to implement the security standards depending on each company's situation. Rice (2005) argues that if adequately exploited investing in security creates opportunities and capabilities that can produce collateral benefits in addition to those directly related to security. This implies that identical certification can be obtained through different implementation strategies, therefore it is on the company interest to identify which one best fits its own needs and constraints. iii) There is a need to guarantee compatibility between programs and to establish their mutual recognition among governments and border agencies from different countries. This is of special interest for both multinational companies which aim for harmonized processes in their global operations and for small medium sized companies that might lack the resources to implement the required security measures.

Currently, there are several voluntary security initiatives which link business and governmental actors, in one way or another. The first security initiatives were created to fight against supply chain disruption such as theft, drug smuggling, loss, damage etc. Today, new and existent initiatives are evolving with a greater focus on measures against terrorism. At first glance, these initiatives appear to be very dissimilar: They have different main targets, originating parties and geographic focus. However, when analyzed in detail they all consist of a set of security measures which - if adequately implemented - constitute a supply chain security management system.

For the purpose of this study the researchers have selected nine voluntary security initiatives worldwide that appear to have or are expected to have significant impact on short and long term supply chain security development. The study was carried out using existing public sources of information on these programs to elaborate a systematic comparison amongst them. In section 2 the researchers provide a general overview by briefly describing each program, and providing some factual data. In section 3 the concrete security measures promoted by each initiative are identified and a "General supply chain security management framework" is developed. This analysis allows the translation of each security initiative into a common framework where they can be compared. By identifying the most widespread security measures

amongst these programs, it was possible to highlight certain security measures that could potentially become the "minimum mandatory security standards for global supply chains".

This study might be of interest for business to obtain a better understanding of these voluntary initiatives that could dictate the minimum requirements for participating in global supply chains. It is also of interest to those who develop programs and policy makers as it constitutes a tool to benchmark their programs with others, identify possible contradictions or synergies and evaluate to which extend it can be generalized to different trading environments. As Graigner (2005) mentions: "…traders and their governments share the same objectives, which is to operate in a prosperous and secure business environment. Through partnership between business and government stakeholders, this objective can be met". The existing schemas of voluntary supply chain security programs appear to be the most appropriate way to bring this collaboration to concrete operational actions. However, it is not sufficient to create programs that only fit the special characteristics of a certain trading environment or type of company. This paper is one of the first efforts to address this problematic from a global perspective and it aims to become a cornerstone for the future evolution and expansion of supply chain security standards.

2 Security program descriptions

The existing voluntary security programs have been created for different purposes and by different agencies or organizations. The researchers identified four types of programs: i) Customs compliance programs to which the security layer has been added; ii) Government origin, pure security programs; iii) International organization origin, security standards programs; and iv) Private origin, pure security programs. Table 1 summarizes the main motivation and philosophy for each type and provides examples of programs belonging to each group.

Table 1. Identified types of voluntary supply chain security programs

Type of Program	Examples	Main motivation and philosophy
Customs compliance programs to which the security layer has been added	PIP (Canada), StairSec (Sweden), ACP & Frontline* (Australia), AEO (EU)	Customs administration aiming to streamline Customs processes (e.g. accounting, payment and clearance) for compliant importers/exporters. Due to new security concerns these programs have added a security layer. This implies that importers/exporters eligible for border crossing facilitation benefits should not only be Customs compliant but also low risk.
Government origin, pure security programs	C-TPAT(USA), Secured Export Partnership (New Zealand)	Governments and border agencies motivated by recent terrorist attacks. Security measures aiming to transfer some of the customs control responsibilities to importers/exporters, in order improve the capacity to detect illegal activities. These programs have become prerequisites for participating in other Customs compliance programs.
International organization origin, security standards programs	WCO framework of standards, ISO (International organization for standardization)	International organizations aiming to establish supply chain security standards that can be generalized for the entire trading community.
Private origin, pure security programs	BASC (Latin America), TAPA (technology companies)	Private companies exposed to high risk of suffering from illegal activities in their cargo management operations. Security measures targeting the protection of cargo from being tampered or removed illegally.

**Accredited client Program: the Australian simplified Customs procedures Program. Presently, some security guidelines have been added, but there is no established supply chain security program yet; government agencies and business sectors are working together to design it. Frontline is a cooperative program between Customs and industry groups to prevent illegal activities related to international trade. However, it cannot be considered a supply chain security program in itself; it is only a commitment on behalf of program participants to communicate any suspicious action to Customs.*

For the purpose of this study, the researchers have selected only those programs where concrete security measures have been defined. In the following paragraphs a brief description of each program is presented using text extracts from each program's description.

BASC, Business Alliance for Secured Commerce / (formerly: Business Anti-Smuggling Coalition). "Cooperation program between the private sector and national and international organizations, created to promote a secure global supply chain. The main goal is to encourage within its membership the development and implementation of voluntary steps to address the risks of narcotics and merchandise smuggling through legitimate trade, as well as the threat of a disruption in the global economy brought about by terrorism"[2].

PIP, Partners in Protection. "Designed to enlist the co-operation of private industry in efforts to enhance border security, combat organized crime and terrorism, increase awareness of customs compliance issues, and help detect and prevent contraband smuggling"[3]. This program does not have a "certification" component as such. Companies may be refused if they don't fulfill the requirements, but once accepted in the program they work together with Canadian Customs to improve their supply chain security, even though they will not get a certification as such. A PIP participant can apply for CSA (Customs Self-Assessment program) to expedite goods (in)to Canada.

C-TPAT, Customs-Trade Partnership Against Terrorism. "Joint government-business initiative to build cooperative relationships that strengthen overall supply chain and border security"[4]. Central to the security vision of C-TPAT is the core principle of increased facilitation for legitimate business entities that are compliant traders. Only importers and carriers based in the US are eligible to participate in this program and one of its main motivations is to protect US borders from terrorist attacks occasioned by goods entering the country. C-TPAT participants can apply for FAST (Free and Secure Trade program) to expedite goods from Canada to the US.

WCO Framework of Security standards to secure and facilitate global trade. This is a framework of security standards developed by the World Customs Organization. It intends to provide a new and consolidated platform which will enhance world trade, ensure better security against terrorism, and increase the contribution of Customs and trade partners to the economic and social well-being of nations. It aims to improve the ability of customs to detect and deal with high-risk consignments and increase efficiency in the administration of goods, thereby expediting the clearance and release of goods. Letter-of-intent signed by 100 countries (July 8, 2005). World Customs Organization (2005).

---

[2] http://www.wbasco.org/english/basc.htm
[3] http://www.cbsa-asfc.gc.ca/general/enforcement/partners/menu-e.html
[4] http://www.customs.gov/xp/cgov/import/commercial_enforcement/ctpat/fact_sheet.xml

EU AEO, European Union Authorized Economic Operator. This designates the status that Customs authorities from European member states should grant to reliable traders established in the European Community. AEO traders will be able to obtain one or both of the following certificates: i) Simplification for Customs procedures ii) Facilitation for security and safety. European Commission (2005).

ISO, International Standards Organization. This organization is developing security standards aiming to become the global supply chain security standard program. It is intended to be in concert with and complementing the World Customs Organization's Framework of security Standards and it does not attempt to cover specific Customs agency requirements. ISO (2005).

TAPA, The Technology Asset Protection Association. This is an association of security professionals and related business partners from high technology companies who have been working together to address emerging security threats that are common to the technology industry and high-tech businesses[5]. This program has no government recognition.

StairSec. This is a new module introduced to the Swedish Customs program Stairway (originally created to facilitate customs processes for compliant traders). "This module makes it possible to quality assure operators within the Stairway not only for quality in their customs routines but also for the security measures they have taken to prevent terrorists from using the operators commercial flow of goods for transporting weapons of mass destruction"[6].

Secured Export Partnership. "It is designed to protect cargo against tampering, sabotage, smuggling of terrorists or terrorist-related goods, and other transnational crime, from the point of packing to delivery"[7] . Exporters from New Zealand are eligible and encouraged to participate; especially those moving goods to the US. The program emphasizes that security measures are customizable depending on the applicant's situation.

Table 2 complements the previous qualitative description of the programs by comparing some factual data: Operational since (year); Number of total applications; Number of (fully) certified companies; and Geographical aspects.

[5] http://www.tapaonline.org/new/engl/what_is_tapa.html
[6] http://www.tullverket.se/en/Business/the_stairsec/
[7] http://www.customs.govt.nz/library/Publications/Secure+Exports+Partnership.htm

Table 2. Voluntary security programs facts comparison.

Program	Operational since	Total applications	Fully certified companies	Geography
PIP	1994	1600	No certification process	Any country to (one country/Canada) import
BASC	1996	1800	1500	Region to region (Latin America to North America/Europe)
TAPA	1997	77	*21*	From and to any region and country.
C-TPAT	2002	9715	811*	Any country to (one country/US) import
Secure Export Partnership	November 2003	159	86	One country to any country export (New Zealand)
StairSec	January 2004	50	30	Any country to (one country/ Sweden) import
WCO Framework of Security stds	Not yet (Adopted June 24, 2005)	NA	NA	Any to any, global coverage
AEO (EU)	Not yet	NA	NA	Any country to region, import & export
ISO	Draft form	NA	NA	Any to any, global coverage

** C-TPAT certification is a 2-step process. First, only companies demonstrating compliance with minimum security requirements are accepted in the program. Presently, there are 5176 accepted companies. The second step called "validation", is only obtained after specialists have visited and evaluated company facilities. Companies with proven effective security measures are deemed compliant. At the moment there are 811 compliant companies*[8].

3 Comparison of program content: Security measures. Model of minimum security standards

In order to carry out a systematic comparison of the selected security programs the researchers reviewed the security measures that companies must fulfill in order to be considered security compliant. There is high variability regarding the level of detail in which these measures are presented. While some programs provide a complete list of activities, processes, controls and technologies that need to be implemented, others just provide a small list of what could be called "security musts" putting the onus on each company to enforce the security measures that they consider necessary given their own constraints. In spite of these differences, it can be observed that most of the programs promote security measures which target one or more of the following security goals:

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

[8] Written enquiry with a C-TPAT Director. August 2005.

- Business network & Company management systems: "Building security in" into internal and external organizational structure and company's management systems.

Each of the previous goals can be achieved in different ways. For instance, Information management is a combination of procuring high quality cargo information, storing it adequately, sharing it with the pertinent partners and protecting it from unauthorized access and usage. At the same time, high quality cargo information can be achieved by implementing error-proof documentation processes, increasing the quantity of data, integrating the data and many other related measures. In order to create a common supply chain security management framework, with an appropriate level of detail but still general enough to be able to compare the different programs, it was decided upon that a classification of the security measures belonging to each of the previous five goals, into five sub categories was necessary. Figure 1 summarizes the resulting framework.

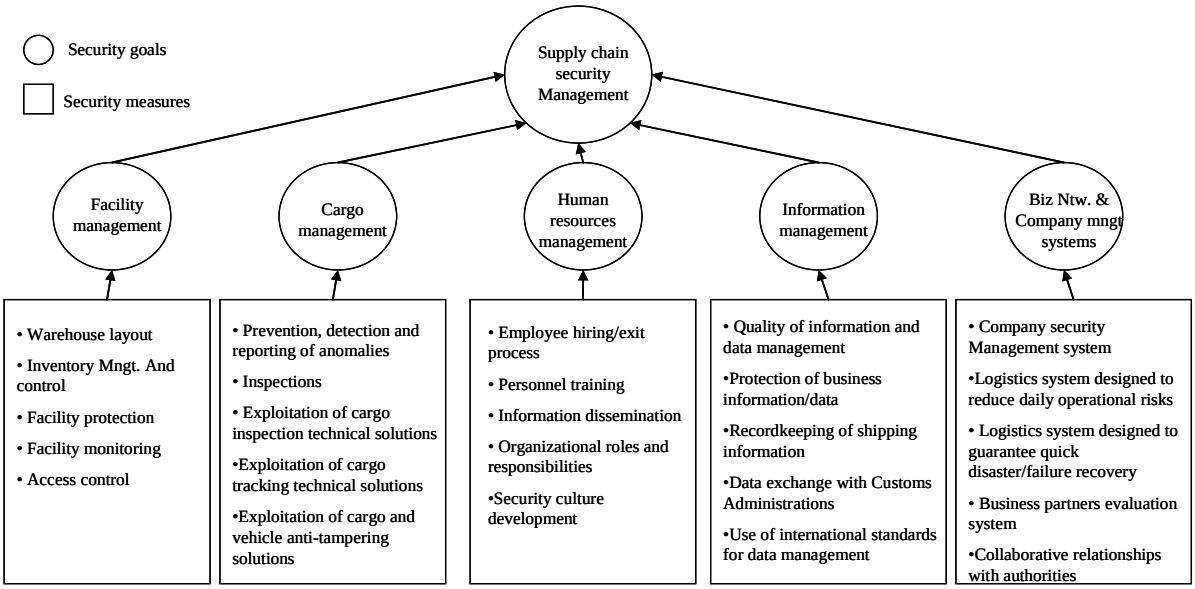

Figure 1: General supply chain security management framework

Even though this framework covers most of the security measures suggested by the current leading supply chain security programs, it is important to note that there is no exact formula to establish an adequate supply chain security management system. The security measures that constitute the framework are not all-inclusive; meaning that implementing them all does not necessarily mean that the security system will be complete, and that implementing only part of them does not necessarily mean that the security will be inadequate. However, this framework provides a better understanding of the concrete measures suggested by each program and can be used to evaluate how similar or dissimilar these programs are. Table 3 shows the security measures within the general framework that are present in each of the studied programs

Table 3. Comparison of security programs with general supply chain security framework

Security measures \ Security Initiative	PIP	BASC	TAPA	C-TPAT	Sec. Exp. partnership	StairSec	WCO	AEO	ISO	Category index
1. Facility management										
1.1 Warehouse/terminal layout design (entry/exit controllability; clearly marked control areas; adequate product marking, sufficient light conditions etc.)	1	1			1		1			
1.2 Inventory management and control (adequate managemet of inventory information;use of product marking standards etc.)		1						1		
1.3 Facility protection (fences; locks; walls; minimization of exit and entry points etc.)	1	1	1	1	1	1	1	1	1	67%
1.4 Facility monitoring (24hr camera system, security guards, filiming activities of loading containers, picking etc.)		1	1	1	1		1		1	
1.5 Access/presence control processes and technologies (id / badges; smart cards; biometrics etc.)	1	1	1	1	1	1	1	1	1	
2. Cargo management										
2.1 Prevention, detection and reporting of shipping process anomalies (routes and schedules continuous review; alerts management, detection and follow-up of overages and shortages etc.)		1	1		1		1		1	
2.2 Inspections during the shipping process (in points where liability changes, to packaging materials and vehicles before getting in contact with cargo, reporting of shortages overages etc.)	1	1	1	1			1	1	1	
2.3 Exploitation of cargo inspection technical solutions (use of various scanners; nuclear/chemical/biological weapon sensors/detectors etc.)							1			44%
2.4 Exploitation of cargo tracking technical solutions (bar codes, RFID, satellite tracking, etc.)										
2.5 Exploitation of cargo and vehicle anti-tampering technical solutions (use and control of high security seals; vehicle immobilisation devices, etc.)		1	1	1	1		1			
3. Human resource management										
3.1 Employee hiring / exit process (background checks; interviews for leaving or fired employees etc.)	1	1	1	1	1		1	1	1	
3.2 Personnel training process (continuous training on security issues; risk awareness etc.)	1	1	1	1	1	1	1	1	1	
3.3 Information dissemination process (internal and external publication of the company security policies)	1	1	1				1		1	58%
3.4 Organizational roles and responsibilities (establish security goals, assign security responsabilities to personnel, identify security required skills etc.)		1							1	
3.5 Security culture development (motivation and incentive programs targeting for cooperation and engagement with security issues)		1					1			
4. Information management systems										
4.1. Quality information/data management (manage more complete and accurate shipment information, establish error-proof documentation processes, data integration etc.)	1			1	1				1	
4.2. Protection of business information/data (management procedures and storing methods design to protect information from unauthorized access and usage)	1		1	1	1	1	1	1	1	
4.3. Recordkeeping of shipping information for potential security audits (maintainance of complete records of the custody of cargo, improved recordkeeping methods; quality control of records, errors correction etc.)		1		1				1	1	53%
4.4. Data exchange with Customs administrations (readiness to provide complete and on-time information as required; in particular compliance with Advance cargo information schemes etc.)	1	1		1		1	1	1	1	
4.5. Use of international standards for data management (WCO Customs Data model, Unique Consignment Reference, digital signatures, digital certificates etc.)							1			
5. Business network & Company management systems										
5.1 Company security management system (defined and documented security processes, defined and controled security indicators, internal and external audits, etc.)		1		1		1	1	1	1	
5.2 Logistics system designed to reduce risks (Evaluation of scenarios of natural risks, accidents, intentional human acts, terrorim etc.)										
5.3 Logistics system designed to guarantee quick eventual disaster/failure recovery (contingency plans, additional capacity, alerts management etc.)							1			47%
5.4 Business partners evaluation system (selection of low risk and high security compliants suppliers, clients and subcontractors)	1		1	1	1		1		1	
5.5 Establishment of collaborative relationships with Customs administrations and other border agencies with control or security functions. Procedures for the notification of anomalies or illegal activities. Consultation customs regulations and security matters.	1	1	1	1			1	1	1	
Degree of similarity to the general supply chain security framework	48%	68%	48%	56%	44%	24%	76%	44%	64%	

It is clear from the table that there are no two programs suggesting the exact same set of security measures. In contrast, it can be observed that each one targets the same security objectives but suggests different ways to achieve them. In spite of this apparent incompatibility between the programs it is possible to observe/see that there are several voluntary security measures that are

suggested by most of the studied programs. Figure 2 shows the security measures organized by the percentage of programs that suggest them.

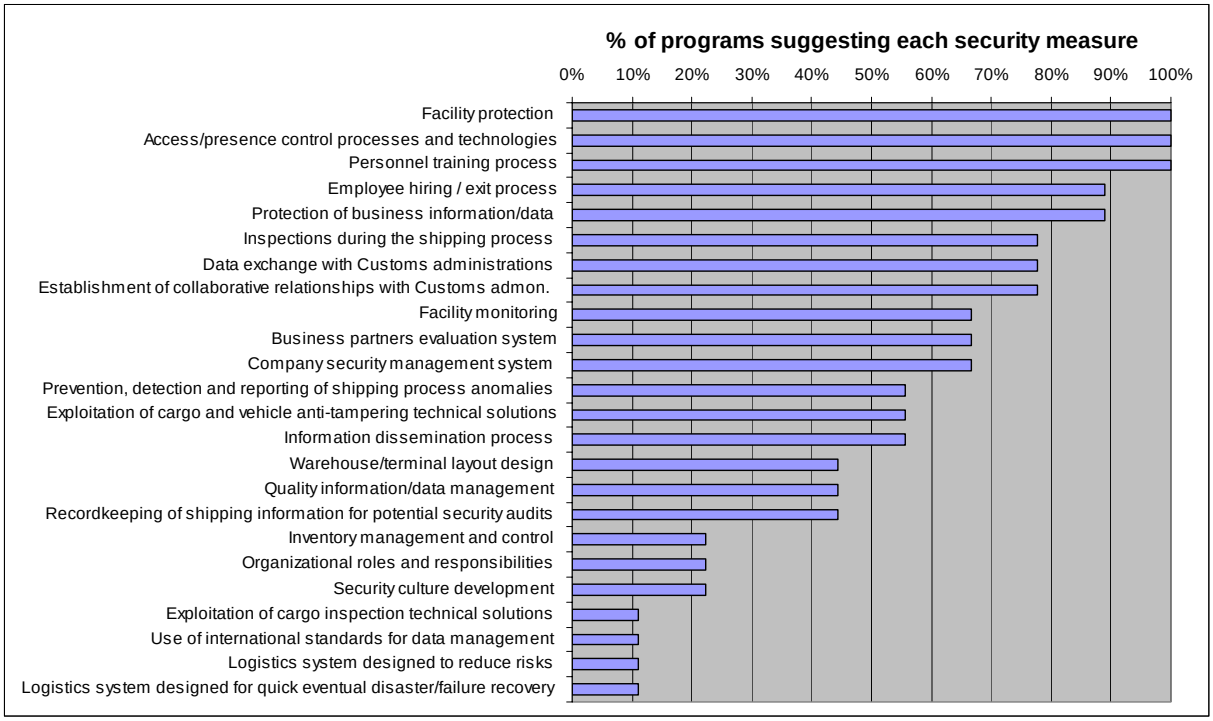

Figure 2. Security measures organized by percentage of programs suggesting them

It can be observed that there is a group of five security measures (Facility protection, Access/presence control process technologies, Personnel training process, Employee hiring process and Protection of business information/data) that are present in more than 80% of the studied voluntary security programs. Due to the importance of these programs in different regions around the world and the increasing attention geared toward security, it is highly probable that these measures could become mandatory for organizations involved in international trade activities. Following this group, it is possible to identify six measures that appear on average in 70% of the existing programs (see details in Figure 2). It can be noted that they mainly refer to collaboration with government and other business partners, and to internal company security processes. It can be argued that while the five most common security measures target the security of the human, physical and information resources itself, the second most frequent group of measures deals with the internal and external processes that interconnect these resources during daily operations. On the other hand, measures targeting quick recovery after disaster and those suggesting the use of specific data or technological standard were found to be the least common measures among the analyzed programs.

It was observed that the use of cargo tracking technical solutions (bar codes, RFID, satellite tracking etc.) is not suggested by any of these security programs. The research team founds this result somewhat counterintuitive given that this field has been both practical reality (especially bar codes) and an active piloting area since some years (especially RFID; tested in programs such as Operation Safe Commerce).

4 Conclusions and discussions

Companies and organizations operating in the international trade environment aim for global supply chain security standards and processes. However, this study shows that there still is a big spread/chasm between existing voluntary security programs. Even if they all target identical objectives, when analyzed and compared in terms of their content, it is not possible to say that a company that is certified by one program will have the requisites to be certified by another. A measure of this difference is that only 3 of the 25 security measures that compose the general supply chain security framework are required by all of the existing (or drafted) programs. It should also be noted that these differences increase when analyzing the breadth and depth of security measures in the various programs. While some provide a detailed list of security standards that must be implemented in order to become security compliant, others just mention the security conditions that should be achieved, leaving room for different interpretations on how to implement them.

It seems that being security compliant has become more a minimum requirement for participating in international trade transactions, than a means to obtain better treatment than others while crossing borders. Even if most of the programs (especially those created by Customs administrations) promise potential operational benefits such as faster clearance time due to less frequent inspections, it should be noted that there are other factors which strongly influence this time, such as the streamlining Customs procedures. A detailed review of the existing voluntary security programs in the world shows that such benefits will still be kept for those companies complying with traditional Customs compliance program requirements (e.g. strict recordkeeping techniques, automatic transmission of information, accurate accounting methods, etc.) and in addition complying with security standards. For instance, only companies participating in C-TPAT or PIP are eligible to apply for FAST or CSA in order to be able to expedite goods while crossing the border, but being only C-TPAT or a PIP participant is not sufficient for obtaining the benefits of Customs streamlined processes.

This paper provides valuable insights that can be used for the future expansion of supply chain security standards. By creating a general supply chain security framework which compiles most of the existing voluntary security programs content, it provides a common platform that can be used to establish compatible security programs or to develop global security standards. In spite of the differences, it is clear that all programs suggest at least one security measure to achieve each of the five security goals identified in the general supply chain security framework. This drives us to conclude that there is coherence and agreement regarding the security goals that must be achieved, but the way to get to these goals has not yet been agreed upon. On the one hand, these differences represent an obstacle for the establishment of global security standards, but on the other hand they suggest that if global standards are created they should be specified in such a way that there is enough room to accept differences based on the country situation and the company characteristics.

This study provides a better understanding of the concrete security measures that can be implemented in order to enhance supply chain security. However, these measures should not be considered as a check list that must be fully implemented to establish an adequate supply chain security system. Given the limited resources and the need to enhance security without jeopardizing the flow of goods, it is necessary to define and implement intelligent criteria that enable the selection of cost effective security measures. At the moment there is few empirical data in this respect. Future studies should be directed to establish the cost of implementation and maintenance of these measures, as well as their effectiveness to increase supply chain security.

5 References

Graigner A. (2005). Andrew Grainger, EUROPRO. In the Proceedings of: *Customs 2007 Seminar*, Wroclaw, Poland. 6 April 2005.

Rice, Jr. et al (2003). Building a Secure and Resilient Supply Network. In: Supply Chain Management Review. Sep/Oct.2003.

Rice, Jr. J. and Spayd P. (2005). Investing in Supply Chain Security: Collateral Benefits. Special report from IBM Center for the Business of Government.

Sheffi Y.(2001). Supply Chain Management under the Threat of International Terrorism. *International Journal of Logistics Management*. Vol 12, Number 12, page 1- 11.

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

Official program documents

European Commission (2005). The authorized Economic Operator. TAXUD/A4/SA D(2005). March 2005.

ISO TC 8/SC 11(ISO/WD 0, ISO TC 8/SC 11/WG 1). Custody Best Practices to enhance Supply Chain Security. : 2 May 2005.

New Zealand Customs Service. Secure Exports Partnership, Important Information for applicants. December 2003.

Partners in protection (PIP) Importer security recommendations: http://www.cbsa-asfc.gc.ca/general/enforcement/partners/imp_recommend-e.html.

StairSec®. White Paper on Accreditation of Operators and the Supply Chain Security. A way forward – Proposal to connect national customs accreditation systems and create an authorized supply chain security (pilot).

TAPA 200- 2005. Freight suppliers' minimum requirements. January 2005.

US Customs and Border Protection. C-TPAT validation process guidelines. January 2003:

World BASC Organization. BASC standards. 2002.

World Customs Organization. Framework of Standards to Secure and Facilitate Global Trade. June 2005.

6 Biography

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.

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) 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.