Development of a strategic roadmap towards a large scale demonstration project in European logistics and supply chain security

Overview

Summary

There are many gaps in supply chain security, according to industry and governmental organizations close to the subject. The LOGSEC project team has uncovered these gaps and condensed them into 3 key areas, referred to as ‘clusters’: inadequate knowledge and awareness of crimes, the threats they pose and what to do about them; an inability to successfully authenticate and trust the information, data, people and companies used in managing supply chain and logistics activities; and thirdly being unable to effectively protect the freight in transit. The LOGSEC project has concluded that future supply chain security demonstration projects should focus on these three areas as a way to address the main gaps in supply chain security, and have a significant impact on the fight against crime which costs the European economy billions of Euros every year, as well as to mitigate the risk of terrorist acts in the supply chains.

Introduction

Global supply chains and logistics systems are threatened. Theft, trade and customs law violations, counterfeit products, organized immigration crime, sabotage, cyber crime, sea piracy, terrorism and other illicit acts generate direct losses, logistics delays, damage to reputation, and other costs for the private sector, particularly for cargo owners and logistics companies. The 2001 terrorist attacks in the USA ("9/11") triggered an avalanche of governmental programs and regulations to mitigate the risks from terrorism such as those from large scale destruction in the supply chain system itself and/or upon specific targets and locations. Consequently the cost of preventative security for the private sector has increased.

LOGSEC, the 12-month EU FP7 Roadmap project for Supply Chain Security (SCS), set about to find an answer to the key question: “What should be done in the future to enhance SCS in a cost-efficient manner, in the European context?”, and furthermore, “Why and how should these enhancements be carried out, while avoiding unnecessarily high investments and operational expenses?” To start with, LOGSEC takes a broad view on the various crime types and terrorism (defined commonly as “man-made illicit acts for gain”) taking place in supply chains, while appreciating the fact that SCS is highly context dependent (manufacturing sectors, transport modes, geographies etc.).

LOGSEC (project number 241676) is co-funded by the European Commission under the FP7 Security Program – LOGSEC was executed by a Consortium of 8 partners; EFP Consulting (UK) Ltd; Cross Border Research Association; Innovative Compliance (Europe) Ltd; European Shippers' Council; CLECAT; European Association for Forwarding, Transport; Logistics and Customs Services; ATOS-Origin; Warsaw School of Economics; and, Swiss Federal Customs Administration. (www.logsec.org).
In the process of seeking the answers to the above questions, the project concluded that for supply chain actors, there is a lack of security awareness, knowledge and skills, often combined with poor intelligence and risk management practices, among those involved in supply chain and logistics management. In particular there exists; a lack of awareness of past crime incidents, statistics, modes of operation by criminals; limited or no access to relevant crime incident data, statistics and trends; a limited pro-active real-time response to disrupt criminal networks and activities; non-compliance with export and import regulations; limited awareness of security and varying – sometimes negative or agnostic, attitudes towards crime threats and security management; limited security knowledge and skills; and limited cross recognition of multiple SCS programs, both nationally and internationally.

Closely linked to these issues are those relating to the collection and treatment of data regarding crime risks in the supply chain, intelligence sharing, and integrated risk management processes. In all these areas there are problems which reduce the effectiveness or impede the implementation of effective supply chain security measures.

Being able to filter out false, fake and bogus elements from the supply chain – when it comes to companies, people, licences, documents, data, raw-materials and products is also linked to effective supply chain security, but this is an area which is often neglected. More specifically, it is important to be able to:

- authenticate genuine, trustworthy business partners and sub-contractors, including logistics, sales channel and reverse-logistics partners;
- authenticate individuals, licences, and permits;
- detect forged documents, counterfeit raw-materials and components, and finished products and falsified product test certificates.

Another important area includes the securing of ‘e-trade’, supply chain fulfilment and logistics information systems against data theft and tampering.

A major SCS issue relates to cargo in transit. 'Cargo-in-transit is cargo-at-risk’, especially when cargo is "at-rest" during the transit operation itself. In this regard, the gaps identified by the LOGSEC project call for attention to the following: securing of cargo; securing of vehicles; safety and security of drivers; securing parking areas for cargo vehicles; integrity during logistics handovers; rapid response and investigation by the authorities to crimes and pursuit of criminals; and tracing of products sent for “final destruction”.

What this in fact implies is that there are 3 distinct areas, referred to in the LOGSEC Roadmap as Clusters, in which supply chain security is today compromised. Every issue or SCS gap (36 in total) that was identified through interviews, workshops and surveys conducted among private sector
companies (manufacturers, retailers and logistics service providers) can be directly associated with one or more of the three LOGSEC Clusters.

Within every Cluster exists a set of ‘themes’, each of which offers the potential to be a subset of the Cluster and a distinct area for a future project, but the sum of these under all of the Clusters will address all the 36 identified gaps. Six themes (potential areas for future projects) were identified for each of the three Clusters.

**A roadmap to demonstration projects**

The roadmap towards suggested demonstration projects to address SCS gaps is depicted by focussing on each Cluster and taking all or the most significant themes as the basis for individual projects.

The LOGSEC roadmap provides for each project area some suggested project objectives and potential deliverables. These are indicative suggestions subject to closer evaluation and assessment of objectives and deliverables when planning for further research/demonstration programmes.

**Security Awareness and Risk Management (Cluster A) Project Areas**

The areas defined for the security awareness and risk assessment Cluster are described under the following headings:

1. Risk management processes and tools;
2. Knowledge on past incidents and modes of operation
3. Security economic models, metrics and performance measures;
4. Security training and awareness building;
5. Security compliance management and audit tools; and
6. Intelligence on evolving threats.

The table overleaf provides further ideas relating to the objectives and deliverables which could be developed within demonstration projects addressing security awareness and risk management.

<table>
<thead>
<tr>
<th>Sub-project area</th>
<th>Objectives and deliverables</th>
</tr>
</thead>
</table>
| A1. Risk management processes and tools | **Objective**: to develop relevant models, processes and tools to manage risks in the supply chain, both from the private sector as well as the public sector perspective, e.g. to model criminal hazards, to identify and prioritise supply chain vulnerabilities, identify effective and cost efficient countermeasures, monitor effectiveness, etc  
**Deliverable**: model to enable decision makers to focus their security management resources to the areas of high risks. |

---

2 The term “Security” here refers to “Supply Chain Security” or “SCS”
| A2. Knowledge on past incidents and modes of operation | **Objective**: to develop processes and data sharing platforms for crime incident reporting and statistics. The input is collected both from the private and public sector actors.  
**Deliverable**: approach for decision makers in both sectors to better perform risk assessment |
|---|---|
| A3. Security economic models, metrics and performance measures | **Objective**: to develop relevant models and metrics to assess the costs and benefits of security investments, both on individual security measures as well as for different security programmes. Including a methodology that allows for impact assessment of security measures, covering also legislation.  
**Deliverable**: tools for private and public sector decision makers to better plan security policies, strategies and measures, as well as to monitor the effectiveness of implementation. |
| A4. Security training and awareness building | **Objective**: to raise the overall level of awareness and knowledge of crime and security threats in supply chains, thus influencing the attitudes of various private and public sector actors towards more secure supply chains.  
**Deliverable**: content and process architecture for efficient supply chain security awareness building and operational training for management and staff. |
| A5. Security compliance management and audit tools | **Objective**: to simplify the management of security programs and to facilitate preparation for related audits, storing and providing the information required for external and internal security audits, and to identify the consistent methodology and approach of independent validators.  
**Deliverable**: standardised but flexible approach for effective verification of security measures under various operational environments and circumstances. Independent validation guidelines. |
| A6. Intelligence on current and evolving threats | **Objective**: to identify, analyze and share intelligence evolving crime threats in supply chains. Intelligence gathering from public sources will be the core of this sub-project, together with public-private and private-private intelligence sharing schemes.  
**Deliverable**: upgrade and adapt risk management system to take into account emerging threats. |

**Authentication, Certification and Data Protection (Cluster B) Project Areas**

The six themes defined for the authentication, certification and data protection Cluster are described under the following headings:

1. Authentication of companies;
2. Integrity of personnel;
3. Authentication of documents;
4. Protection of supply chain IT systems;
5. Authentication of boxes, containers and seals;
The following table provides further ideas relating to the objectives and deliverables which could be developed within demonstration projects addressing authentication, certification and data protection.

<table>
<thead>
<tr>
<th>Sub-project area</th>
<th>Objectives and deliverables</th>
</tr>
</thead>
</table>
| B1. Authentication of companies                        | **Objective**: help to ensure that manufacturing, trade, logistics, reverse logistics, and other service companies in the supply chain are authentic, and in possession of required licences. The scope of the sub-project includes verification of company data and information against trusted databases etc.  
  **Deliverable**: assistance to effectively validate the security level, standard or qualification of business and supply chain partners |
| B2. Integrity of personnel                             | **Objective**: to verify past and present criminal activity among people engaged in the supply chain, through personnel background checks, integrity checking, verification of credentials, etc.  
  **Deliverable**: tools and procedures for enhanced pre employment background checking and pre and on-going evaluation of personnel integrity, in compliance with EU privacy legislation and national employment rules, where applicable. |
| B3. Authentication of documents                        | **Objective**: to prevent the introduction of false documents in the supply chain including personnel credentials, trade and logistics documents etc.  
  **Deliverable**: tools and methods to identify forged documents in the supply chain and to take action to minimize their ability to compromise the supply chain |
| B4. Protection of supply chain IT systems              | **Objective**: to reduce successful attempts to steal data, to alter data, and to cause any type of harm in ‘e-trade’, supply chain management, order fulfilment and to logistics platforms.  
  **Deliverable**: tools and procedures to enhance the identification and authentication of users and electronic systems and where possible, to block unauthorised access to computer systems and databases which might otherwise compromise the security of data and communications in the supply chain. |
| B5. Authentication of boxes, containers and their contents | **Objective**: to increase the trust of and authenticity of declarations (documentary or otherwise) regarding the content of boxes, containers and seals (i.e. “what's on the box is in the box – and vice versa”), and the integrity of packaging.  
  **Deliverable**: tools and procedures to ensure that the content of shipments reflects the description on the company paperwork. |
| B6. Authentication of raw-material and products         | **Objective**: to identify and filter out counterfeit products and falsified product certificates in the supply chain.  
  **Deliverable**: tools and procedures to aid recognition of various types of counterfeit products and certification forgeries |

**Physical Transportation Security and Cargo Monitoring (Cluster C) Project Areas**

The themes defined for the physical transportation security and cargo monitoring Cluster are described under the following headings:

1. Protection of drivers;  
2. Protection of vehicles;
3. Protection of cargo, loads, containers;
4. Inspection, scanning and screening of cargo;
5. Ensuring integrity during logistics handovers;
6. Protection during stops/parking.

The following table provides further ideas relating to the objectives and deliverables which could be developed within demonstration projects addressing the physical transportation security and cargo monitoring.

<table>
<thead>
<tr>
<th>Sub-project area</th>
<th>Objectives and deliverables</th>
</tr>
</thead>
</table>
| C1. Protection of drivers | **Objective**: to provide enhanced protection for truck drivers against all personal threats.  
**Deliverable**: catalogue of validated equipment and procedures through the implementation and evaluation of new and existing tools for enhanced driver protection measures - such as anti-burglary solutions, alarms with local and distant functionality, detection sensors, armoured cabins, deterring procedures and equipment, and good/best practice. |
| C2. Protection of vehicles | **Objective**: to provide enhanced protection for trucks and other vehicles against any type of intrusion, while balancing the measures to protect vehicles with the protection of drivers.  
**Deliverable**: catalogue of validated equipment and procedures through the implementation and evaluation of new and existing tools for conveyance protection – such as anti-burglary solutions, alarms with local and distant functionalities, detection sensors, engine and brakes blocking devices, satellite controlled trip detectors, geo-location dynamic engine controllers, etc., and good/best practice. |
| C3. Protection of cargo, loads, containers | **Objective**: to provide enhanced protection for cargo, loads and containers against any type of intrusion.  
**Deliverable**: catalogue of validated equipment and procedures through the implementation and evaluation of new and existing tools for cargo protection - such as anti-burglary solutions, alarms with local and distant functionalities, detection sensors, tamper proof packaging, tamper evident seals, and tamper detection materials such as inks, powders etc., and good/best practice. |
| C4. Inspections, scanning, screening of cargo | **Objective**: to enhance the prospect for efficient inspection, scanning and screening of cargo.  
**Deliverable**: catalogue of validated equipment and procedures through the implementation and evaluation of new and existing tools and techniques for inspections, scanning, screening of cargo - such as various non-intrusive high throughput, non disruptive, scanning technologies, etc and good/best practice. |
| C5. Ensuring integrity during logistics handovers | **Objective**: to enhance the security of freight handovers and prevent discrepancies occurring.  
**Deliverable**: catalogue of validated equipment and procedures through the implementation and evaluation of new and existing tools and approaches to freight handovers - such as theft protection measures, checking of product labels and quantities; documentation; seals etc. |
| C6. Protection during stops / parking | **Objective**: to provide enhanced protection for trucks, cargo and drivers during stops against any type of intrusion.  
**Deliverable**: catalogue of validated solutions and procedures through the implementation and evaluation of new and existing technologies, processes and best/good practice to guard parking areas, drivers, vehicles, and their cargo during mandatory and voluntary truck stops, including the evaluation of alternative approaches to "traditional concept of secure parking". |
Stakeholders and management tools for Demonstration projects

The LOGSEC Roadmap provides further leadership in the thinking behind future demonstration projects by offering various considerations which will be important when evaluating the conditions under which demonstration projects based on the Roadmap Clusters will provide the highest benefit for enhancing supply chain security across the EU, and beyond.

Stakeholder participation

In order for the Demonstration project(s) to be successful, a wide variety of private and public sector actors and stakeholders should participate. This includes representatives from the private sector (manufacturers, retailers, other cargo owners, and logistics service providers) and private sector equipment and IT service providers. Public sector participants should include customs, police, intelligence and transport security agencies, with the addition of product safety, data security, and civil protection agencies.

Integration requirements

Projects to resolve supply chain security gaps must address both internal (as a core element of any additional scenarios within a Demonstration project) and external (in relation to other sources of supply chain information) integration. Internal integration requirements will relate to incident and threat reporting, information security, knowledge of business partners, and provide input to awareness and training. With respect to external integration, the projects must demonstrate integration with business, police, intelligence and other sources of threat/risk data.

Context dependencies

Supply Chain Security management is very much context dependent, i.e. the design and implementation of optimum security responses depends highly on:

- manufacturing sector/ commodity types (e.g. high value goods, consumer goods, dangerous goods etc.);
- transportation modes (road/ rail/ maritime/ air etc.);
- geographical location and transport routes;
- geopolitical situations;
- financial circumstances (global and local); etc.

For LOGSEC Demonstration project(s), the context must be taken into account, both before-during-after planning and assessment phases.
The LOGSEC logistics flow map

A precursor to any demonstration project is an impact assessment. It is important to identify where in the supply chain any measures are implemented and where any impact will take place. In order to evaluate the success or otherwise of a demonstration project one must also establish performance criteria that can be compared prior to, during and after the project. This requires measures to be taken before the implementation of a project; along those parts of the supply chain where the proposed security ‘solutions’ are implemented; and, where they are expected to manifest themselves. A LOGSEC logistics flow map, which was developed by the project team, and applied as an aid in the collection of information from private sector respondents to the study, forms a solid basis for this crucial mapping and impact assessment exercise.

An 8-layer SCS management model

Another management tool to support the detailed design, specification, documentation and assessment of future Supply Chain Security (SCS) demonstration project(s), is an “8-layer SCS management model”, introduced and applied throughout the Roadmap. The characteristics of each security measure planned for the demonstration should be assessed both a priori and a posterior, against this 8-layer model, in order to create detailed knowledge on which aspects (i.e. layers) of the holistic SCS management approach are being addressed, why and with what outcomes. The principles of continuous improvement, and Plan-Do-Check-Act (PDCA)-cycle should be fully embedded into the 8-layer approach.

Demonstration metrics and performance measures

As a key component in any supply chain security demonstration it is necessary to define the set of metrics to be applied before-during-after the demonstration. Just as with any operation and supply chain management project or process, it is crucial to develop, apply and monitor concrete metrics and key performance indicators which support budgeting and investment planning, risk/threat analysis, in the day-to-day security project management, and other associated activities.

Principles of standardisation

Standards play an important role in any management systems, including SCS management. For the Demonstration project(s), one should both refer and, if appropriate, build upon existing standards, as well as propose and develop new standards during the Demonstration work, when appropriate. Standards should, however, provide sufficient flexibility in their application in order to cater for different conditions, circumstances and environments, and not be restrictive or force standards into circumstances that might prove to be unnecessary, costly or inappropriate. Also good practices from existing sources should be taken into consideration, on a case-by-case basis. Existing SCS related standards and also “good practices” to consider can be checked with, for example, the International Standards Organization (ISO); European Committee for Standardisation (CEN); any national
European standards body, e.g. in the UK (BS) and in Germany (DIN); Transported Asset Protection Association (TAPA); and ASIS International (ASIS).

**Third-country involvement**

Lastly, related to the ‘stakeholder participation’ and ‘context dependencies’ aspects mentioned before, some considerations regarding potential involvement of third countries in LOGSEC Demonstration project(s) are made. High risk locations per crime type need to be considered when considering imports from third countries to Europe, e.g. certain Latin American countries as sources or points-of-transit for narcotics; certain Asian countries for counterfeit products; certain African countries for endangered species; etc. In addition, considering SCS compliance and mutual recognition aspects, participation of US companies and regulatory authorities would be beneficial to the Demonstration project(s).

**Prioritising demonstration projects**

There are clear overlying issues between the Clusters, for example, addressing awareness and knowledge of people within supply chains will also impact their effectiveness in relation to the identification of bogus companies and the introduction of effective freight security when the goods are out on the road. Therefore, combining all three Clusters into a cohesive whole would, if one were able to successfully address the issues, comprehensively close the gaps identified in supply chain operations.

Deciding, therefore, which areas or clusters and individual themes might have a higher priority in any future demonstration projects is an inherently difficult task; nevertheless, an attempt to do so has tentatively concluded that the following sub-project areas exhibit the highest ratio of “gap-quotation-scores”

<table>
<thead>
<tr>
<th>Cluster</th>
<th>Sub-project areas</th>
<th>Sub-project description</th>
</tr>
</thead>
<tbody>
<tr>
<td>B</td>
<td>4</td>
<td>Protection of supply chain IT systems</td>
</tr>
<tr>
<td></td>
<td>1</td>
<td>Authentication of companies</td>
</tr>
<tr>
<td></td>
<td>2</td>
<td>Authentication of documents</td>
</tr>
<tr>
<td>A</td>
<td>1</td>
<td>Risk management processes and tools</td>
</tr>
<tr>
<td></td>
<td>4</td>
<td>Security training and awareness building</td>
</tr>
<tr>
<td></td>
<td>5</td>
<td>Security compliance management and audit tools</td>
</tr>
<tr>
<td></td>
<td>6</td>
<td>Intelligence on current and evolving threats</td>
</tr>
<tr>
<td>C</td>
<td>2</td>
<td>Protection of Vehicles</td>
</tr>
<tr>
<td></td>
<td>3</td>
<td>Protection of cargo, loads, containers</td>
</tr>
</tbody>
</table>
The highest “gap-quotation-scores” were achieved by sub-project areas in Cluster B – Authentication, certification and data protection, however, the highest total number (4) of sub-project areas with high “gap-quotation-scores” were found in Cluster A – Security awareness and risk management. The two sub-project areas from Cluster C – Physical transportation security and cargo monitoring that made the list of highest “gap-quotation-scores”, are in fact the central sub-project areas in this Cluster.

In effect the project concludes by tentatively suggesting that priority be given in sequence to sub-project areas dealing firstly with protection of supply chain IT systems, followed by those sub-project areas focused on authentication of companies and of documents, and risk management processes and tools, and equal priority thereafter to the sub-project areas covering security training and awareness building, security compliance management and audit tools, Intelligence on current and evolving threats, and the protection of vehicles and of cargo, loads and containers

Conclusions

The culmination of the project is the roadmap which establishes recommendations for future large scale demonstration projects; however, these were formulated to provide considerable flexibility in the number and scale of projects that could be undertaken in order to address specific supply chain security gaps identified by this project. The analysis and assessments made within the LOGSEC project will help to prioritise the issues that projects could address. Nevertheless, establishing projects around all three Clusters would ensure the possibility of addressing all the identified gaps. The LOGSEC project team submitted this report and its conclusions, confident they represent a meaningful, flexible way forward to the enhancement of supply chain security in the EU. Focus of demonstration projects in the areas identified by this report will, if proven successful, prove to be beneficial to industry and Member States, and increase the protection of EU citizens from crime, the criminals and the impacts of crime in the supply chain.

The full roadmap can be downloaded from the LOGSEC Website www.logsec.org.