SLOVENSKI STANDARD
SIST-TP CEN/TR 16412:2012

01-november-2012

Varnost oskrbovalne verige - Navodilo z dobrimi praksami za male in srednje velike dobavitelje

Supply chain security (SCS) - Good practice guide for small and medium sized operators

Logistik - Handbuch für bewährte Praktiken für die Sicherheit von Lieferketten

Sécurité de la chaine d'approvisionnement - Guide de bonnes pratiques pour les petites et moyennes entreprises

Ta slovenski standard je istoveten z: **CEN/TR 16412:2012**

ICS:

03.100.10	Nabava. Dobava. Logistika	Purchasing. Procurement. Management of stock

SIST-TP CEN/TR 16412:2012 **en,fr**

TECHNICAL REPORT

RAPPORT TECHNIQUE

TECHNISCHER BERICHT

CEN/TR 16412

September 2012

ICS 03.100.10

English Version

Supply chain security (SCS) - Good practice guide for small and medium sized operators

Sécurité de la chaîne d'approvisionnement - Guide de bonnes pratiques pour les petites et moyennes entreprises

Sicherheit von Lieferketten - Handbuch für bewährte Praktiken für kleine und mittlere Unternehmen

This Technical Report was approved by CEN on 13 August 2012. It has been drawn up by the Technical Committee CEN/TC 379.

CEN members are the national standards bodies of Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, Former Yugoslav Republic of Macedonia, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and United Kingdom.

EUROPEAN COMMITTEE FOR STANDARDIZATION
COMITÉ EUROPÉEN DE NORMALISATION
EUROPÄISCHES KOMITEE FÜR NORMUNG

Management Centre: Avenue Marnix 17, B-1000 Brussels

Ref. No. CEN/TR 16412:2012: E

Contents

Page

Foreword

This document (CEN/TR 16412:2012) has been prepared by Technical Committee CEN/TC 379 “Supply Chain Security”, the secretariat of which is held by NEN.

Supply chains move huge quantities and values of products and services between businesses and between businesses and consumers throughout Europe and between Europe and countries in other continents. These movements present enormous opportunities for organized crime and terrorists. The intrusion of crime and terrorist activity has become a major risk in doing business for the majority of operators within the supply chain, i.e.:

— cargo owners;

— shippers;

— forwarders;

— terminal operators;

— transporters.

1 Scope

This Technical Report aims to provide Small and Medium sized Enterprises (SMEs) basic knowledge about how to manage and mitigate the risk of criminal and terrorist activities. This is a shared objective for the private and public sector.[1] For the private sector, companies have gained experience on measures, which can assist in preventing security breaches from happening, to protect against supply chain interruption. Also some business standards have been developed identifying measures, which companies can execute in order to obtain labels which certify business operations and reward them with a security quality label. The public sector has developed security legislation which companies should either mandatory or voluntary apply into their business operations.

This Guide provides an easy-to-read overview on:

1) How SMEs can apply a supply chain security approach to their operations (Clause 2).

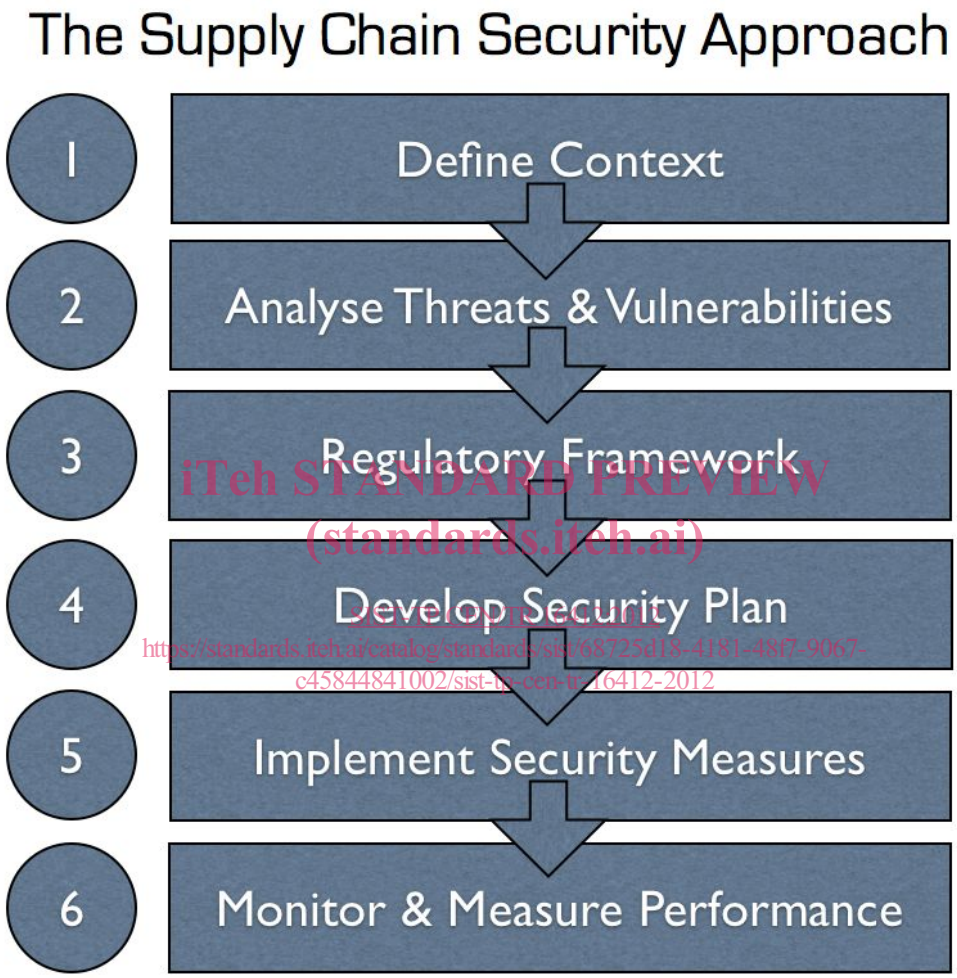
2) The main crime types in the supply chain including some measures to fight these crime types from occurring (Clause 3).

3) Supply chain security legislation and programs, with their respective compliance requirements (Clause 4).

[1] In the context of this guide, “supply chain security” covers risk management, crime prevention, security procedures and technologies, as well as security regulations and programs. The overview and examples in this book are based on recent academic work and interviews with experts in the field, including CEN SCS Feasibility Study (2010); EU FP7-LOGSEC Roadmap (2011) and interviews with CEN TC/379 experts.

2 Recommended Supply Chain Security Approach

How to integrate supply chain security into your business? Various ways are possible and being explored by companies. Existing guidelines and best practices often refer to the exploitation of risk management approaches. However, the practical application of these approaches is often difficult to understand and apply in practice for SMEs. Hence, in this guide a concrete step-by-step approach is explained, with examples of practical security measures to mitigate specific crime risks, and to comply with specific security regulations and standards. In this guide, the following six steps are recommended[2]:



FIRST, **define the context** for your supply chain, crime prevention and security management activities. The major questions being:

- Which business are you in, and how “security sensitive” is it?
- Which geographies and transport modes are included?
- Who are the customers, suppliers, insurance providers, governmental agencies and other key stakeholders your supply chain operates with?

As an outcome, you create the context before moving on to the next considerations.

---

[2] There is no guarantee that a certain security measure brings a sustainable, positive outcome.

SECOND, perform a **threat and vulnerability analysis**, when it comes to actual criminal and terrorist threats in your supply chain. [3] The major questions being:

- Where are the risks of failing today, i.e. where are the gaps calling for enhanced security?
- Which crime types are of particularly high risk in your supply chain? Use statistical sources, if available, while carrying out such risk assessments.
- What are the realized and/or potential consequences of one or more crime incidents?

THIRD, consider **regulatory and program aspects**.[4] The major questions being:

- Which regulations are required for you to operate successfully in your defined business environment, and which programs could support achieving your business objectives?
- What do your customers expect from you? What about your suppliers?
- Have your insurance providers established any requirements?
- What about relevant governmental authorities, including customs and police?

FOURTH, create an overarching **security plan** for your company and/or supply chain, where you consider a variety of security management aspects, taking into consideration the outcomes of your business context; threat and vulnerability; as well as security program and regulatory aspects analysis (steps one, two and three above). The aspects you should take into consideration are:

- Physical security (facilities, vehicles, containers, shipments etc.);
- Data security (in particular systems with supply chain data);

- Human resources security (including selection, training, and exit procedures); - Business partner security (including selection, and auditing); and

- Process control and monitoring of deviations.

FIFTH, choose the **combination of concrete security measures** – investments in technologies, procurement of services, in-house solutions and so forth – and implement them into practice. Embed security procedures and technologies as much as feasible into daily operations, as part of your overall supply chain, logistics, and transport management functions.

SIXTH, monitor and measure the security performance and feedback to the planning cycle. Take corrective actions. Increase security at weak spots, and reduce in the areas where overinvestment has taken place. Pay attention to the dynamics and changing situations when it comes to criminal focus areas and "criminal portfolios"; technical and operational improvements - both licit and illicit aspects - and legislative requirements, and consequences, both for the licit and illicit actors.

---

[3] Clause 2 helps to increase understanding the types of threats one could be subject to and do something about.

[4] Clause 3 provides an overview of key regulation and programs.

3 Crime prevention in supply chains

3.1 Introduction

Ten relevant crime types have been chosen fallen under the following five categories**:**

1) **Property theft**: Cargo theft; Intellectual property violations.

2) **Targeted damage**: Terrorism; Sabotage.

3) **Cross-border duty and tax fraud**

4) **Illegitimate transporting / importing and/or exporting**: Smuggling of prohibited and restricted goods; People smuggling.

5) **Crime facilitation**: Document forgery; Bogus companies; Cyber crime.

For each crime type, the

— issue (What are the main characteristics and what are the typical products / sectors involved?),

— scope of the problem (Why is it a problem?) and

— actions to take (How to mitigate the risks?)

are being elaborated on.

3.2 Cargo theft

Cargo theft can be defined as "...***any theft of shipment committed during its (surface) transportation or within a warehouse.***"[5]. This covers straightforward theft, hijacking, robbery, fraudulent pick-up, and load diversions, etc.[6]. The value of a single load can be anything from a few thousand to few dozen million Euros. On the other hand, in case of getting caught, cargo crimes often result only in minor legal punishment. Valuable commodities, which have high demand on the after-market and are easily transportable, are quick to sell and particularly vulnerable for cargo theft[7]. These commodities include consumer electronics, cigarettes, food, alcohol, brand apparels, precious metals and prescription drugs. Cargo crime incidents can occur in any part of a supply chain, but truck stops and unsecured parking lots are the most vulnerable spots in the chain (NICB 2010).

In addition to the high financial losses estimated to be over 8 billion Euros in Europe in 2009 [8], the human suffering caused by threats and violence involved in cargo theft is huge.[9] From the private sector perspective, cargo theft is commonly considered the most frequent crime threat in supply chains today. All operators can be usual victims of cargo theft. Manufacturers face material shortages due to theft incidents, resulting in production downtime, missed deliveries and lost sales[10]. For the logistics sector, cargo theft causes liability and insurance problems, lower customer satisfaction and so on. For the **public sector**, cargo theft is a cost

---

[5] Cargo Theft Report. Applying the Brakes to Road. Cargo Crime in Europe. Public version excluding Appendix D (Europol Restricted). The Hague, 2009. Editorial note: term "surface" is used instead of "road".

[6] Cargo theft is being perceived as an attractive, high reward, low risk criminal industry FIA 2001, Contraband, Organized Crime and the Threat to the Transportation and Supply Chain Function

[7] Felson and Clarke, 1997, Opportunity makes thief

[8] http://www.tapaemea.com/public/

[9] IRU 2006 Attacks on Drivers of International Heavy Goods Vehicles

[10] Anderson, Bill (2007), Securing the Supply Chain – Prevent Cargo Theft, *Security*, Vol. 44, N°5, pp. 56-58

and reputation factor for the police and the legal system. It can be dangerous for consumers, who unknowingly or knowingly buy stolen goods. As yet, fighting cargo crime has not traditionally been a high priority concern for policymakers[11].

Measures to mitigate the risk of theft relate to

- Physical security measures for buildings, parking areas, and vehicles are key.
- Selecting low-risk routes, avoiding unnecessary stops, and not picking up unknown people into trucks are good policies.
- Careful selection and training of personnel and supply chain partners, as well as conducting audits of security capabilities of the logistics service providers normally helps to mitigate the risks.
- (Hidden) tracking devices among the cargo as well as tracking devices in the vehicle – and even vehicle immobilization systems can help to recover the stolen items. [12]
- Training of warehouse workers and drivers can also be a useful recovery measure.

Further **reading** on how to reduce cargo theft in the supply chain:

- *IRU Road Transportation Security Guidelines 2005, which is available at http://www.iru.org/en_guidelines-goods*
- *TAPA FSR 2011 and TAPA TSR 2008, which are available at http://www.tapaemea.com/*

3.3 Counterfeit goods

Counterfeiting can be defined as "***the illegal reproduction or imitation of products, given that this illegality is the result of a violation of any type of intellectual property rights***"[13]. Counterfeits products are mostly transported to affluent markets via legitimate supply chains, whereby the production of the counterfeits often takes place at the upstream of an otherwise legitimate supply chain. Counterfeiting trade can bring huge profits, while there is a low risk of being caught and moderate punishment in case of being caught. In some countries, the public perception is that counterfeiting can be socially acceptable. Advances in technology increasingly give counterfeiters the tools to copy.[14]

It has been estimated that since early 1990s, global trade in counterfeits has increased eight times faster than legitimate trade. Today's global markets for counterfeit products account for 5 % - 7 % of world trade[15]. In a worst-case scenario, counterfeit products can cause serious damage to human health and safety (even death). Medicines, electronics and software remain the most counterfeited products in the world. [16]. Counterfeiting can reduce demand of genuine products resulting in lost sales as well as damage the reputation of the brand owner. This is particularly the case when a customer is deceived and buys a copy thinking it is a real product with proper functionalities and quality. Consumers buy counterfeit products both knowingly and unknowingly.

---

11 EC (2003), "Freight transport security", EC Consultation Paper, European Commission, Brussels.

12 **Detection and recovery** are partially about getting information about an incident as soon and accurately as possible, for both law enforcement and security service centre follow-up.

13 Nations Interregional Crime and Justice Research Institute (2007). *Counterfeiting: a global spread, a global threat*. Turin: UNICRI.

14 http://www.iccwbo.org/id399/index.html

15 World intellectual Property Association, International Anti-counterfeiting Coalition

16 http://www.havocscope.com/black-market/counterfeit-goods/counterfeit-goods-ranking/

Measures to mitigate the risk of counterfeit goods relate to:

— **Prevention** of counterfeit goods in the supply chain:

- Close co-operation between the relevant private and public sector actors, i.e. awareness campaigns, development of international agreements and national legislations.
- Tight contracts with all the supply chain partners to eliminate counterfeit attempts within the (normally) legitimate supply chain.

— **Detection and recovery** relying on capabilities to identify counterfeit products at various stages of the supply chain, in a cost-efficient, non-intrusive and high quality (low false-positives and false-negatives) manner. Measures include:

- High and low technology means to facilitate the detection process (on product level) including hologram tags, bar codes, micro text and phone help-desks.
- Monitoring and auditing of consumer sales, auction websites, as well as physical outlets enables detecting (and seizing) counterfeit products.

Further **reading** on how to tackle counterfeit related problems in the supply chain:

— *The International Trademark Association (INTA) and the International Chamber of Commerce (ICC) Business Action to Stop Counterfeiting and Piracy (BASCAP) at http://www.bascap.com/*

— *IP Crime Group: Supply Chain Kit, available at http://www.ipo.gov.uk/ipctoolkit.pdf*

3.4 Terrorism in supply chains

Terrorism can be defined as ***"any act intended to intimidate a population or to compel a government or an international body to act."***[17] Besides destroying (parts of) supply chain itself, terrorism is likely to be connected with a variety of crime types[18]. Terrorists may exploit legitimate supply chains to achieve their malicious objectives. Furthermore, terrorist groups can generate profits and fund their operations with legitimate or illicit businesses throughout the supply chain. Terrorist networks may also use of the logistic chain as a conduit to deliver weapons and individual terrorists to a target destination.

Governments across the globe have identified terrorism as unlawful and a major threat to political and social stability. Since 9/11, a large number of counter-terrorism supply chain security initiatives have been launched. These initiatives also impose a challenge for the **private sector operators**[19]. First, they must adapt their operations to a new operating environment with heightened security requirements. Secondly, they have to be prepared to deal with the aftermath of a major terrorist attack. Supply chain operators do not commonly see terrorism as an imminent threat. The bill of anti-terrorist measures imposed by government programmes can be too expensive for companies, especially when these programmes imply monetary investments, or reduce supply chain efficiency as lead times become longer and more unpredictable, i.e. more stringent customs inspection at borders.

---

[17] http://news.bbc.co.uk/2/hi/americas/4716957.stm

[18] : "To strengthen coordination and cooperation among States in combating crimes that might be connected with terrorism, including drug trafficking in all its aspects, illicit arms trade, in particular of small arms and light weapons, including man-portable air defense systems, money-laundering and smuggling of nuclear, chemical, biological, radiological and other potentially deadly materials." United Nations. General Assembly. The United Nations Global Counter-Terrorism Strategy. A/RES/60/288, Distribution on 20 September 2006.

[19] Sheffi (2001). Supply Chain Management under the Threat of International Terrorism