Supply Chain Security Frameworks Utilization for Analysis and Design of Security Performance Evaluation System – Part 1

M. Vitteková*
Department of Logistics and Transport Management, Czech University of Technology, Prague, Czech Republic,
** Corresponding author: lanska@fd.cvut.cz*

DOI: 10.2478/v10158-012-0042-z

ABSTRACT: This paper deals with highly current topic of supply chain security with a focus on general supply chain security (SCS) frameworks. It analyzes two approaches to supply chain security and presents the author's future research focus in this area, which is aimed at expansion and completion of the general supply chain security management model and the creation of a security performance measurement tool. Such a measurement tool would allow complex comparison of security programs from an attained security level point of view. Initiatives currently aimed at security performance measurement and other perceivably immeasurable characteristics can be found in the areas of operational security and quality.

KEY WORDS: Supply chain security (SCS), SCS model.

1 INTRODUCTION

The provision of Supply Chain Security has been a key logistic issue in the past decades. Its rise is being initiated by governments and global companies on the one hand, and concerned entrepreneurial subjects on the other. Governments try to provide strategic security, which can be violated by illegal migration, smuggling, sabotage, military support of dubious organizations and terrorist acts. The interest of manufacturers and trade organizations is the effective optimization and minimization of delays caused by additional security provision. Effective optimization also lies in introducing commonly shared standards against theft during transportation and other logistical operations. Regional governments (EU, U.S., Asia) have created their own tools represented by a portfolio of compulsory and voluntary security programs and initiatives. Currently, there is a compatibility process on the international level in terms of these programs. Therefore, important scientific contribution created a general model/framework to describe the features of security management and security management system implementation

2 SECURITY MANAGEMENT SYSTEM

A secure state is not a natural state. In the supply chain environment, security threats are naturally present and can be ignited by "favorable circumstances". Complex supply chain security protection can be achieved only by the development of an artificial security management system.

Security management systems (1) define structures – define relations between personnel responsible for security and other nodes, (2) define security rules and regulations – standard

procedures, (3) define and execute actions needed for system functionality checks – controlling, audit and evaluation. In the framework of security management process security threats are identified and risks analyzed. The next step is risk mitigation in order to reduce potential security risks.

Each economic region creates its own security system according to the risks it is exposed to due to its business, social and political characteristics. The United States was forced to found new agencies such as the Transport Security Agency (TSA) within its customs administration structures and focus on terrorism-related security threats. Programs such as C-TPAT, CSI, FAST and others originated in the United States. The European Union is focused mostly on smoothening customs declaration processes (AEO programs). Manufactures and transport companies dealing with high-value goods focus especially on theft protection (TAPA EMEA program).

3 COMMON FRAMEWORK FOR SECURITY MANAGEMENT SYSTEM

Security systems of economic regions originate in common platforms that guarantee their compatibility, which is an extremely essential feature. An unnecessary complexity and security approach differences may cause a counter-effect resulting in an actual slowdown of goods flow and an increase of costs due to the necessity of overcoming the incompatibilities between the different security systems.

The common platform is composed of three core international standards: WCO SAFE Framework of Standards to Secure and Facilitate Global Trade (WCO SAFE), International Ship and Port Facility Code (ISPS Code) and Specification for security management systems for the supply chain ISO 28000 (ISO 28000).

These platforms have certain differences, however, even though they create a common framework encompassing supply chain security issues and pave the way to a mutual recognition of certified security programs. As the platforms cover a wide area of supply chain security issues they incorporate government bodies, non-government organizations, private enterprises, customs administrations, manufacturers, transport companies, forwarders, etc. across all means of transport. Common interest here is the maintaining of compatibility in supply chain security on an international level. The European program AEO, which is focused on establishing a certified economic entity, was inspired by WCO SAFE and uses ISPS Code, ISO 28000 and ISO 28001.

The next chapter introduces basic approaches defining general security management system components. The focus of the author's research is on the expansion of these general models and the definition of a new framework for measuring and evaluating supply chain participant's security performance.

4 BASICS OF GENERAL MODELS

The functionality of supply chain security programs is founded on different principles that all lead to one common goal. The security programs contain basic components that combine measures, tools and procedures. These measures, tools and procedures are present within these components in a proportion that ensures the efficient maintenance of security. The components form independent entities within the security programs and their combinations ensure an efficient security systems management of the future.

General models cover 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 for establishing 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 (Gutierrez & Hintsa, 2006).

In 2005, the APEC (Asia Pacific Economic Cooperation) consortium created a conceptual model based on 9 basic components (APEC, 2005). Its model was inspired by the 2004 IBM initiative (Closs & McGarrell, 2004) that focused on a multi-organizational and cross-functional approach to supply chain security.

In 2006, Gutiérrez and Hintsa from the Cross Border Research Association based in Lausanne, Switzerland, published a study based on the analysis of the 9 security programs in which they created a general supply chain security management system (Gutiérrez & Hintsa, 2006). Their model has 6 basic components.

These general models give the necessary framework needed for the better understanding of concrete security measures proposed in each of the security programs and may be used for the evaluation of how much the programs have in common. The general models thus allow the comparison of security programs and the finding of their common features that create systems interconnection. Detailed analysis is able to identify the different levels of security measures implementation and offer possibilities for their completion.

4.1 APEC Model

The APEC model is based on 9 basic elements (Figure 1) which describe all security layers in the supply chain system. Recommended features and procedures are recommended for each element.

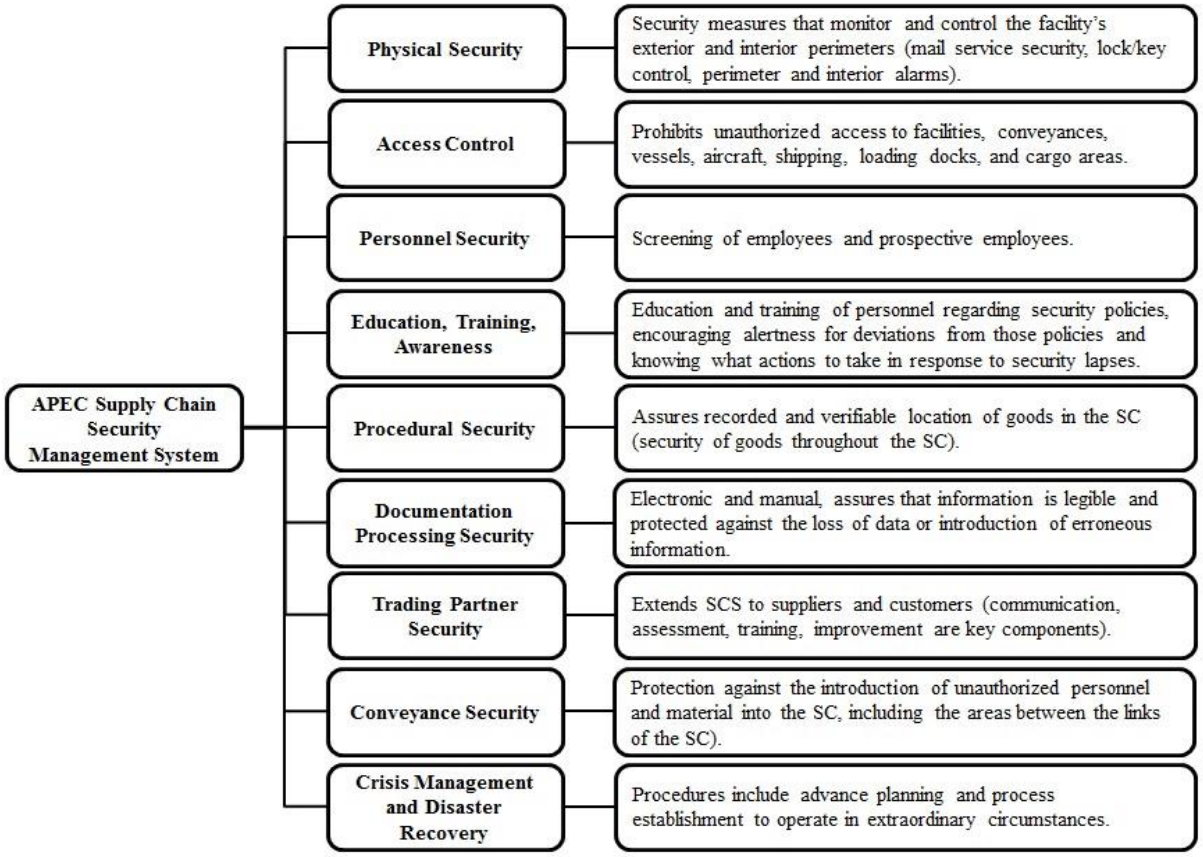

Figure 1: APEC Supply Chain Security Management System (APEC, 2005).

(1) Physical security includes security measures that monitor and control the facility's exterior and interior perimeters. For fulfilling the function of this layer peripheral and perimeter barriers,

electronic security systems including CCTV, segregated goods systems within the warehouse and other features are suitable for implementation. Procedures will include supervision of gates, separated employee and visitor parking, etc. (2) Access control prohibits unauthorized access to facilities, conveyances, vessels, aircraft, shipping, loading docks, and cargo areas. If access control is not possible, increased precautions in other security aspects may be needed. (3) Personnel security is concerned with the screening of employees and prospective employees, as appropriate and as allowed for by law. (4) Education, training and awareness encompass the education and training of personnel regarding security policies, encouraging alertness for deviations from those policies and knowing what actions to take in response to security lapses. (5) Procedural security assures the recorded and verifiable location of goods in the supply chain. Procedures should provide for the security of goods throughout the supply chain and contingency procedures should be included within the scope of procedural security. (6) Documentation processing security both electronic and manual, assures that information is legible and protected against the loss of data or the introduction of erroneous information. (7) Trading partner security extends supply chain security to suppliers and customers. Communication, assessment, training, and improvement are key components.

(8) Conveyance security provides protection against the introduction of unauthorized personnel and material into the supply chain, including the areas between the links of the supply chain. (9) Crisis management and disaster recovery procedures include advance planning and process establishment to operate in extraordinary circumstances (APEC, 2005).

4.2 Gutiérrez and Hintsa General Model

Gutiérrez and Hintsa (2006) mean securing premises for the production of goods and handling, the storing and loading of cargo. Unlike the APEC model, the Gutiérrez and Hintsa model facilitates six elements that express how to manage a complex environment of supply chain facilities (Figure 2).

For proper (1) Facility management, facility layout design is developed. This part of security system management should ensure entry and exit controllability, clearly marked control areas, adequate product marking, sufficient light conditions, etc. Inventory management and control require the adequate management of inventory information, use of product marking standards, etc. Protection of the facility includes fences, locks and walls. Subsequent measures involve facility monitoring through 24 hour camera systems, security guards, filming the activities of loading containers, etc.. For access and presence control processes and technologies, including RFID and biometrics, should be used. (2) Cargo management means protecting the goods during all stages of their transportation. In this part of the system, five subcategories are involved. Prevention, detection and reporting of shipping process anomalies, inspections during the shipping process, exploitation of cargo inspection technical solutions, exploitation of cargo tracking technical solutions, exploitation of cargo and vehicle anti-tampering technical solutions. (3) Human resources management means ensuring that the background of all personnel is checked and that they are reliable and aware of the risks. This part involves employee hiring and exit process, personnel training process and continuous training on security issues and risk awareness. Information dissemination process facilitates internal and external publication of the company security policies. Organizational roles and responsibilities lie in establishing security goals, assigning security responsibilities to personnel and identifying security required skills. Role of (4) Information and communication management is in protecting important data and using information as a tool for tracing illegal activities and shortcomings in security. In the case of this element we can mention quality information and data management as a tool for managing more complete and accurate shipment information and to establish error-proof documentation processes data integration. Protection of business information and data uses procedures and storing methods designed to protect information from unauthorized access and usage. Recordkeeping of shipping

information for potential security audits can maintain complete records of the custody of cargo, improved recordkeeping methods, quality control of records and errors correction. Other measures for information management are data exchange with customs administrations and the use of international standards for data management (WCO Customs Data model, Unique Consignment Reference, digital signatures, digital certificates, etc.). (5) Business network and company management systems include security in the internal and external structure of the organisation and in the company's business systems. The company security management system involves defined and documented security processes, defined and controlled security indicators, internal and external audits. Evaluation of scenarios of natural risks, accidents, intentional human acts, or terrorism is a part of the logistic system which is designed for reducing risks. Contingency plans, additional capacity, and alerts management system provide quick eventual disaster or failure recovery. A selection of low risk and high security compliant suppliers, clients and subcontractors is a function of Business partner evaluation system. (6) Crisis management and disaster recovery cover issues of Business continuity plans, Formal security strategies, Emergency control centres and Incident management.

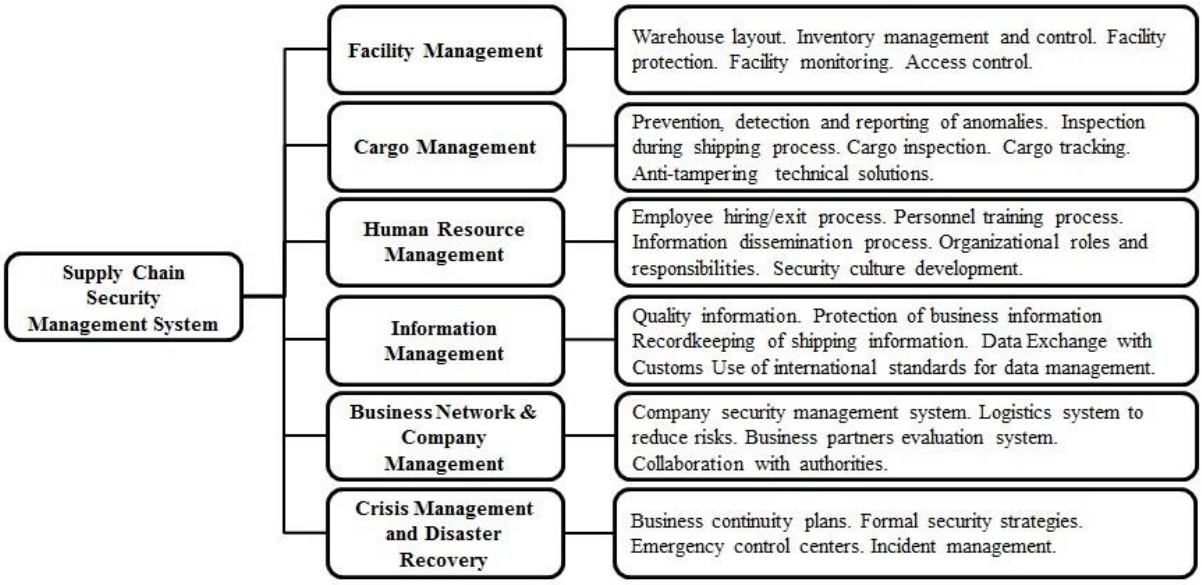

Figure 2: Gutiérrez and Hintsa Supply Chain Security Management System (Gutiérrez & Hintsa, 2006).

Security management systems structural analysis is important not only from the practical application point of view. Results of such analysis form the base for a better understanding of security measures and their impact on the whole security system. The expansion of the general model as well as common and different features location allows for a further detailed analysis of the core problem and the creation of new applications. The expanded model will be used for security performance quantification of organizations and will allow the creation of a security index that could be used for a comparison of organizations. Based on the measured general model components performance the security recommendations could be adopted more easily. System characteristics measurement is currently a problem that is related not only to reliability and quality but also to the operational security of organizations doing business in high-risk industries.

Due to possible financial losses and the maintenance of economic region strategic security, security is not a risk-free part of supply chains. Finding solutions for these security-related issues allows for the application of acquired information as well as active participation in security programs optimization initiatives. Establishing a compatible environment

and the simplification of operations connected to the maintenance of security in the EU and other economic region borders will be the subject of the upcoming research.

5 CONCLUSION

The next research of this topic is to widen the general model/framework and describe coherence among programs, with emphasis being primarily on regions with a strong potential for growth. In the short term we also expect an increased interest from Czech exporters to conquer new markets. Therefore it is vital to present these findings to experts/personnel that will deal with supply chain security in their professional lives. An additional task for research will be the formation of a model to measure the security performance of different subjects. This task follows solutions of quantificational problems in different fields. Currently, one can measure, for example, the performance in operational security and quality.

ACKNOWLEDGEMENT

The research was supported by CTU SGS13/155/OHK2/2T/16.

REFERENCES

APEC, 2005. *Supply Chain Security Programs: Guidelines* [online]. APEC, U.S. [cit. 2013-03-14]. Retrieved from: http://www.apl.com/security/documents/APECSupplyChainSecurityGuidelinesfinal1.pdf

CBP, 2008. *C-TPAT: Customs-Trade Partnership Against Terrorism* [online]. U.S. Customs and Border Protection. [cit. 2013-03-14]. Retrieved from: http://www.cbp.gov/xp/cgov/trade/cargo_security/ctpat/

Closs, D. J., McGarrell, F. M., 2004. *Enhancing Security Throughout the Supply Chain* [online]. Washington, U.S.: IBM Center for The Business of Government [cit. 2013-02-12]. Retrieved from: http://www-03.ibm.com/procurement/proWeb.nsf/objectdocswebview/filesupply+chain+security+white+paper+and+assessment+guide+april+2004/$file/supply+chain+security+white+paper+and+assessment+guide+april+2004.pdf

Gutiérrez, X., Hintsa, J., 2006. *Voluntary Supply Chain Security Programs: A Systematic Comparison* [online]. Lausanne (Switzerland): Cross-border Research Association, Lausanne: EPFL, HEC Lausanne [cit. 2013-03-14]. Retrieved from: http://www.cross-border.org/pdf/lyon2006-voluntaryscs-gutierrez-etal-may2006.pdf

Knight, P., 2003. *Supply Chain Security Guidelines* [online]. New York, U.S.: IBM Corporation [cit. 2013-02-12]. Retrieved from: http://www-03.ibm.com/procurement/proweb.nsf/objectdocswebview/filesupply+chain+security+guidelines/$file/supply+chain+security+guidelines+12sep03.pdf

WCO, 2012. *SAFE - Framework of Standards to secure and facilitate global trade.* WCO - World Customs Organization.