Safety Science 79 (2015) 358–368

Contents lists available at ScienceDirect

Safety Science

journal homepage: www.elsevier.com/locate/ssci

w@reRISK method: Security risk level classification of stock keeping units in a warehouse

Miguel Gastón Cedillo-Campos [a], Hermes Orestes Cedillo-Campos [b]

[a] *Mexican Institute of Transportation, Transportation and Logistics Systems National Laboratory, Carretera Querétaro-Galindo Km 12, Sanfandila, Mpio. Pedro Escobedo, C.P. 76703 Queretaro, Mexico*
[b] *YoLogistico.COM, Francisco P. Mariel No. 155, C.P. 78233 San Luis Potosí, Mexico*

ARTICLE INFO

Article history:
Received 22 January 2015
Received in revised form 8 May 2015
Accepted 11 June 2015

Keywords:
Supply chain security
Risk management
Warehouse management
Inventory systems
Multicriteria analysis

ABSTRACT

Risk management in warehouses is a key issue to guarantee security all along the global supply chains. However, from a balanced approach including at the same time a solid theoretical background and practical processes of implementation, our comprehensive literature and field practices review proved that most of current methods to manage warehouses still do not take into account the risk level classification of stock keeping units (SKU). Thus, the ***w@reRISK method*** to analyze the security risk of SKU stocked in a warehouse is here exposed. Since risk analysis involves not only factual data, but also perceptions, this paper proposes a hybrid method based on the ABC classification of SKU as well as a XYZ variability system analysis, but also incorporates the Analytic Hierarchy Process (AHP) to ponder subjective values which are part of risk. The method includes a security risk level classification of SKU, then introduces an exhaustive list of 34 factors useful to judge the risk of a SKU stocked in a warehouse for comparison purposes. An application example is included to demonstrate the use of the method. The lack of analytical frameworks with solid technical basis to secure warehouses along the global supply chains makes this paper a contribution to the body of knowledge in supply chain security, as well as a friendly-user method to practitioners. The proposed method is susceptible to become an automated informatics tool. As a conclusion, key issues for designing secure manufacturing supply chains are discussed, and future research is presented.

1. Introduction

Supply chain security is a multidimensional area of knowledge, which should be engaged from a comprehensive as well as an integrated point of view. Since a large proportion of the cargo is completely or partially loaded through different warehouses, these logistics facilities become a critical link inside supply chains. Assessing all the combination of risks related to different stock keeping units (SKU) in a warehouse is complex. Even if some SKU have an evident level of risk which allows decision makers to define the right location where the SKU should be placed in a warehouse (computers, flash memories, cell phones, which are highly marketable), others are less obvious. This is the case of certain inoffensive (when used in everyday life) chemical or informatics products, which could be combined or assembled to produce a potential weapon. To place these kinds of products close to them in a warehouse could not only cause damage by accident, but also enables their illegal use by criminals. Since a specific risk analysis of every product in each warehouse along a supply chain is time-consuming and requires highly trained personnel, an integrated method based on a standardized approach is needed.

Thus, in the U.S., from a criminal risk perspective, the NBC recently reported that more than $1.2 million worth of computers, cameras and other electronic devices were stolen from warehouses in Fremont, California (NBC, 2014). From a simplistic point of view, it is a security issue which could be understood as a result of a weak policing or company's security systems. However, in emerging markets as Mexico, the multidimensional nature of security risk to supply chains is more evident. Since product type cargo thefts vary between regions, security risk level classification of SKU is not trivial. Electronics thefts frequently occur close to metropolitan areas in the central region of the country, while steel and other metals are more targeted in the north. High-value items and food remain the most pursued after cargo by thieves, as they are readily sold or marketable (U.S. Overseas Security Advisory Council, 2014). On the other hand, from a national security

E-mail address: gaston.cedillo@mexico-logistico.org (M.G. Cedillo-Campos)

http://dx.doi.org/10.1016/j.ssci.2015.06.009
0925-7535/

perspective and according to Bakir and Pakdaman (2006): "*US-bound containerized overseas cargo move through various phases, all of which present unique security challenges. Issues in container security can be summarized under five phases: loading phase at the warehouse, land transportation, port of origin, sea transportation and port of destination*". Thus, Bakir and Pakdaman (2006) highlighted that terrorists may load illegal weapons and explosives at the warehouses or distribution centers from which the cargo is dispatched. In that context, security breaches can sometimes compromise the existence of the companies (Markert, 1998; Johansson, 2008; Torabi et al., 2014).

Consequently, when analyzing the true cost of supply chain crime, Jones et al. (2009) identified an "*Iceberg Effect*". Their analysis reported $15–18 billion in direct costs, but 60 billion of indirect costs in losses (sales, reputation, insurances, investigation cost, re-order costs, administrative costs, paying claims, and others).

For decades, the constant quest for efficiency in productive operations has led companies to pursue the zero inventory and just-in-time paradigm through philosophies such as "*Lean Manufacturing*". Yet, the increase in demand variability and the risk linked to security threats on global supply chains, are reshaping the way to design, organize and manage more resilient logistics systems (Cedillo-Campos and Perez, 2010; GAO, 2010; Pfohl et al., 2010; Thun and Hoening, 2011; Vilko and Hallikas, 2011; The White House, 2012; Elmoselhy, 2014; Cedillo-Campos et al., 2014). In fact, modern companies are now looking for improving their "supply chain fluidity", which is understood as the capability degree to achieve continuously a reliable, secure, and accurate flow of process, supporting effectively the supply chain goals. Given the important interrelation among actors, any disruptive effect, when a security risk materializes in the supply chain, can bring important economic consequences for a company, as well as for other supply chain members as a result of risk propagation (Johansson, 2008; Bakshi and Gans, 2010; Serdarasan, 2013; Bueno and Cedillo-Campos, 2014). Globalization has facilitated trade; however, the supply chains are every day more vulnerable (Donner and Kruk, 2009; Ochoa, 2010; Sodhi and Son, 2012; Kern et al., 2012; Cedillo-Campos, 2012; Chopra and Meindl, 2013); the complexity of current supply chains makes them highly vulnerable to direct impacts such as thefts, shrinkage or indirect impacts arising from fines or other situations, as a result of non-fulfilling with standards like C-TPAT (Customs-Trade Partnership Against Terrorism).

Since supply chain vulnerability is increasing, interest to understand risk and how to deal with the effects of the disruptions in supply chains has arisen as a global priority (Lee and Whang, 2005; Buesa et al., 2007; Ochoa, 2010; Bueno and Cedillo-Campos, 2014). Nowadays, threats are an international matter that use supply chains of companies respectful of the law to do harm. Containers, products, and modes of transportation create a screen, preventing quick detection of harmful contents, making them very attractive to criminals. In that sense, the ideal would be to implement 100% scanning policies at all points of rupture of the cargo, but it would be virtually impossible (GAO, 2008; Xue and Villalobos, 2012; Cedillo-Campos et al., 2014).

Actually, total security supply chain can only be reached if every link, from the point of origin to its final destination, is responsible for the security of its part of the supply chain (Holler and Schanck, 2010; Schlegel and Trent, 2012; The White House, 2012). Since warehouses are important, because of their number inside a supply chain and of their important role in the synchronization of manufacturing flows, controlling security in warehouses makes a critical link in the security of the whole supply chain.

In a modern and global supply chain, any warehouse must guarantee the security of the products and of the workforce handling them. The warehouse is the link that must guarantee the appropriate handling and custody of SKU. Depending on the types of products located in the warehouses, different criteria are used to their design, such as the classification of SKU, inventory turnover, environment conditions, and other specific aspects. Nevertheless, the lack of internationally standardized systems for warehouse management to reduce security risks makes them a highly vulnerable link in the supply chain.

Based on the global studies developed by Johansson (2008) and Hintsa et al. (2010) and completed by a comprehensive literature and field practices review, we concluded that, from a balanced approach including at the same time a solid theoretical background and a practical processes of implementation, methodologies to improve warehouse management considering the security risk level of SKU were not found. Consequently, the objective of this paper is to develop an analytical framework for providing managerial insights for those dealing with security risk classification of SKU located in a warehouse.

The article is organized as follows: Section 2 exposes the analytical framework as well as the opportunity area; Section 3 presents an illustrative example, and finally, Section 4 discusses the concluding remarks and the future work derived from this work.

2. Analytical framework

For companies, the aim of reducing security breaches is to mitigate the economic losses that may be due to the contamination or loss of products causing financial impacts as well as to keep safe the trademark prestige (Johansson, 2008; Hintsa et al., 2010; Bueno and Cedillo-Campos, 2014; Cedillo-Campos et al., 2014). However, in spite of the great number of international security initiatives, warehouse systems lack a practical, technically robust, and not time-expensive method that enables evaluating, from a supply chain management perspective, different risks in warehouses.

In order to cover this significant gap, our flexible and hybrid method enables classifying products in a warehouse, using the combination of different analytical tools taking into account: (i) Characteristics of how SKU are used (ABC); (ii) Variability; analysis of consumption (XYZ); and (iii) A multi-criteria perception of risk (AHP). Therefore, both qualitative and quantitative criteria were integrated in the proposed method (see Fig. 1).

2.1. ABC analysis

The ABC inventory control method is a helpful technique for determining which inventories should be counted more frequently and managed more closely than others (Ramanathan, 2006; Al Kattan and Bin Adi, 2008). The ABC classification method shows where the efforts in handling the inventories can be best applied and where the best opportunities can be found to reduce costs

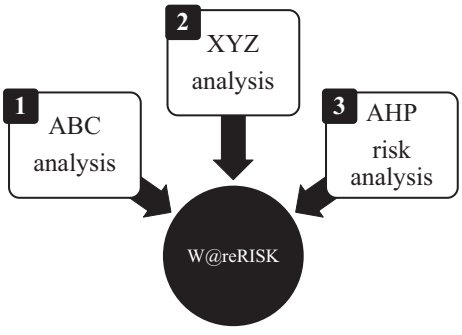

Fig. 1. ***w@reRISK method.***