



Risk management of Taiwan's maritime supply chain security

Yi-Chih Yang*

Department of Shipping and Transportation Management, National Kaohsiung Marine University, 142 Hai-Jhuan Road, Nan-Tzu, Kaohsiung 81143, Taiwan, ROC

ARTICLE INFO

Article history:

Received 22 April 2010

Received in revised form 2 September 2010

Accepted 29 September 2010

Keywords:

Risk management

Maritime supply chain

Security

ABSTRACT

This paper attempts to evaluate the impact of risk factors from the container security initiative (CSI) on the maritime supply chain in Taiwan, employs a loss exposure matrix to identify the severity and frequency of security risk, and uses a bowtie diagram to investigate appropriate risk management strategies to deal with maritime security risks.

This paper's findings consist of the following: (1) the leading categories of CSI risk factors are operational risk, physical risk and financial risk; (2) apart from two security risks comprising high-risk level, the majority of risk exposure is at the medium level; risk management strategies include loss prevention, loss reduction, avoidance, and non-insurance transfer; and (3) all maritime security regulations and measures should consider the balance among cost, time, security, efficiency and competition; failure to do so may lead to additional burdens for maritime supply chain service providers.

© 2010 Elsevier Ltd. All rights reserved.

1. Introduction

The US has implemented a series of container security procedures under the container security initiative (e.g. CSI, 24-h rule, CT-PAT, Megaports initiative, etc.) since the 911 terrorist attacks in 2001. In order to implement foreign supply chain security, the US customs authority has requested that Taiwan's customs authority sign a CSI MOU and station an American CSI team at the port of Kaohsiung. However, some potential CSI-related global maritime supply chain risks and uncertainties may affect maritime supply chain service providers and shippers in Taiwan.

The container security initiative is a four-part program that involves: (1) the establishment of security criteria for identifying high-risk containers based on advance information; (2) pre-screening of containers identified as high-risk before they arrive at US ports; (3) pre-screening of containers using high-tech devices; and (4) development and use of technology, including radiation detectors and large-scale X-ray and gamma ray machines, to quickly pre-screen high-risk containers, and development of secure and smart containers (OECD, 2003). The US customs authority has been entering into bilateral agreements or partnerships with foreign governments to ensure the implementation of CSI. The agreements provide for the deployment at foreign ports of US officers, who must target and pre-screen US bound cargo containers before they are shipped. The US officers are to work with host national counterparts (UNCTAD, 2004). Bilateral CSI agreements allowing US customs to target foreign-port containers bound for the US have already been signed with several mega-

ports which, as July 2003, accounted for 66% of container imports to the US (GAO, 2003). The benefits of CSI encompass deterrence and prevention of terrorists, protection of global trade, reduction of processing time for certain shipments, immediate handling of CSI-screened containers, and reduction of illegal migration, drug smuggling, and other criminal activity involving marine container shipping (JAGC, 2003).

On the other hand, the 24-h rule is a major security requirement under which carriers or their agents must submit a cargo declaration for each US-bound container 24 h before loading at the foreign port. In other words, outbound container manifests must be transmitted to the US customs authority within 24 h. This measure is probably the most controversial among all CSI actions in that it acts against logistical optimization and operational flexibility, and, more importantly, may distort competition between different market players (UNCTAD, 2004). The 24-h rule requires that liner companies and NVOCCs (Non-Vessel Operating Common Carriers) provide the US government with a 1-day advance notice of a container being loaded into a vessel. The 24-h rule, which applies to containers destined for or transiting United States ports, can therefore affect carriers, freight forwarders, and non-vessel operating common carriers (King, 2005).

While the main purpose of the security initiative (e.g. international ship and port security code, container security initiative, customs and trade partnership against terrorism, etc.) is to reduce the likelihood of maritime vectored terrorism, inappropriate implementation of these programs can affect competitiveness. Barnes and Oloruntoba (2005) claimed that there is a need to examine the goodness of fit of these security initiative measures versus business efficiency and competitiveness. Burdensome customs and security measures may hinder port and maritime

* Tel.: +886 7 3617141x3158.

E-mail address: hgyang@mail.nkmu.edu.tw

supply chain efficiency, which may in turn lead to a contraction in trade and overall efficiency (Wilson et al., 2003).

The government of Taiwan has introduced various security initiatives (such as the WCO SAFE framework, CSI, AEO, and ISPS) in compliance with global trends and the war on terror. However, many individuals in the shipping industry are still unfamiliar with the purpose and functions of CSI and the 24-h rule due to insufficient government publicity, and some relevant issues concerning the impact of CSI and the 24-h rule on the shipping industry are seldom discussed in public. This formed one of the chief motivations for this paper.

A review of recent literature concerning maritime security reveals that although a great number of qualitative works have been published, only a handful of papers engage in quantitative empirical investigation and analysis. Of a total of 30 relevant research papers, 20 are chiefly qualitative and only 10 are quantitative. Seven qualitative papers review security-related regulations and their current development status (Roach, 2003; Stasinopoulos, 2003; Harrauld, 2005; Cui, 2006, 2007; Liu, 2007; Chang et al., 2010); the other qualitative papers are concerned with the impact of security on specific industries, and include four papers on global supply chains (Sarathy, 2006; Williams et al., 2008; Japan External Trade Organization, 2008; Veselko and Bratkovic, 2009), five papers on the shipping industry (Roach, 2004; King, 2005; Thai, 2007; Bichou et al., 2007; Venus Lun et al., 2008), two papers on maritime supply chains (Barnes and Oloruntoba, 2005; Banomyong, 2005), and two papers on seaports (Bichou, 2004; North, 2009).

Quantitative papers include four papers employing survey questionnaires to perform empirical investigation and analysis (Thibault et al., 2006; Thai and Grewal, 2007; Kumar et al., 2008; Voss et al., 2009), three papers using a cost analysis approach (Bichou, 2004; Bennett and Chin, 2008; Gutierrez et al., 2008.), two papers using analysis by means of mathematical formulas (Lee and Whang, 2005; Lee et al., 2008) and one paper involving path analysis (Chao and Lin, 2009). The following characteristics of these papers have inspired this study's research motivations: First, since only two papers investigated maritime supply chains, there should be further, in-depth investigation of the impact of CSI on maritime supply chain industries. Second, the majority of the foregoing research papers used qualitative methodology to probe the impact of maritime security because of the complexity of quantitative analysis. Third, while the research methodology of the aforementioned quantitative papers encompassed questionnaires, cost analysis, analysis using mathematical formulas, and path analysis, no paper adopted a risk management perspective to evaluate the impact of security on maritime supply chains.

As the issue of maritime supply chain security is still fresh and relevant laws and regulations in Taiwan are still insufficient, many companies and the general public are not familiar with the real purpose and features of CSI. Since it is difficult to obtain enterprises' internal financial statements and documents due to business confidentiality concerns, this study employed a risk management perspective and figured out maritime supply chain security risk factors via literature review and personal interviews, identified the category of security risk based on factor analysis, determined risk levels by means of a survey questionnaire and risk exposure matrix, and used a bow tie diagram to formulate risk management strategies for the maritime supply chain industry sector.

Supply chain security management is broad in scope, and encompasses raw material vendors, semi-finished or finished product manufacturers, exporters and shippers, freight forwarders, customs brokers, shipping and global logistics service providers, importers, and consignees, and these parties work in a complicated environment. In order to narrow its research scope, this study fo-

cused on maritime supply chain service providers, including shipping companies, shipping agencies, freight forwarders, and custom brokers.

The purpose of the paper is to:

1. Highlight maritime supply chain risk feature and assessment factors.
2. Review current developments and industry insights concerning CSI and the 24-h rule in Taiwan.
3. Perform risk assessment for maritime security risks.
4. Formulate risk management strategies for maritime supply chains.

The reminder of this paper is organized as follows: The second section consists of a review of literature concerning maritime supply chain security, risk management, and CSI aspects; the third section explains the study's research methodology, including its risk exposure matrix, assessment factors, questionnaire design, and data collection; the fourth section performs empirical investigation and analysis based on the loss exposure matrix and bow tie diagram; and the final section offers a number of conclusions and provides suggestions for the industry and academic researchers.

2. Literature review

2.1. Maritime supply chain security

Risk is the probability that an event or action may adversely affect the organization (Hutchins, 2003). Risk categories include strategic risk, operational risk, financial risk, knowledge risk, and compliance risk (The Institute of Risk Management, 2002). Alan Braithwaite (2003) concluded that global logistics chains must face the following risks: risk of collaboration costs, risk of ineffective activity execution and poor quality products, demand risk, supply risk, and environmental risk. The sources of risk in maritime supply chains encompass environmental risk, organizational risk, and network-related risk (UNCTAD, 2007). Shipping risk factors connected with terrorism include cargo, vessel, financing/logistic support, trade disruption and security costs. The sources of risk include any variable that cannot be accurately predicted, and which can lead to a supply chain disruption of some kind. These sources include accidents (i.e. fire), force majeure (i.e. natural disasters), and socio-political actions (i.e. terrorist attacks) (Juttner, 2005).

Risk management is the decision-making process whereby actions are taken in view of the outcome of risk assessment. Risk assessment is a systematic process for assessing the impact, occurrence, and the outcome of human activities involving products or systems with hazardous characteristics. The three stage of risk assessment comprise risk identification, risk estimation, and risk evaluation (Duijne et al., 2008) Risk assessment focus on the consequences or impact of specific risks. In the case of a global supply chain, risk assessment is concerned with understanding supply chain vulnerabilities along their entire geographically-dispersed lengths, as well as among their various elements, from goods to information, transportation modes and people (Sarathy, 2006). The risk assessment process measures eight factors that are deemed critical to having a reliable, predictable, cost effective supply of materials and services; these factors are design cost, legal, availability, manufacturability quality, supply base, environmental, health and safety impacts (Zsidisin et al., 2004).

Risk management reduces the negative effects of uncertain future losses by making those losses less likely, less severe, or more predictable, allowing more effective allocation of an organization's scarce resources. Risk management has been defined as the process of making and carrying out decisions that will minimize the ad-

متن کامل مقاله

دریافت فوری ←

ISIArticles

مرجع مقالات تخصصی ایران

- ✓ امکان دانلود نسخه تمام متن مقالات انگلیسی
- ✓ امکان دانلود نسخه ترجمه شده مقالات
- ✓ پذیرش سفارش ترجمه تخصصی
- ✓ امکان جستجو در آرشیو جامعی از صدها موضوع و هزاران مقاله
- ✓ امکان دانلود رایگان ۲ صفحه اول هر مقاله
- ✓ امکان پرداخت اینترنتی با کلیه کارت های عضو شتاب
- ✓ دانلود فوری مقاله پس از پرداخت آنلاین
- ✓ پشتیبانی کامل خرید با بهره مندی از سیستم هوشمند رهگیری سفارشات