Critical Issues of Security in Supply Chain Management

Yui Yip Lau, Joseph
MacGregor Education Services Limited
Principal and Senior Programme Manager

Introduction

Logistics security refers to the threat of attack to cargoes or people involved in the logistics process. It involves criminal activities like theft, terrorism and smuggling and so on. Threats and smuggling will affect the smooth flow of the supply chain. There really need to be some measures or actions to eliminate possible terrorist attacks during shipments. In this study, we will investigate how the current security practices are implemented in supply chain management. In regard to policies, different requirements need to be introduced for ensuring logistics security. This study sheds light on the latest developments in initiatives on security in the supply chain management. The findings also help managers and researchers better understand how these measures affect daily operations of logistics organizations.

The European Union
AEO Programme

The EU Authorized Economic Operator legislation came into force in the EU at the beginning of 2008. By the middle of September some 270 companies had been certified. At the end of the spring the Commission opened a website where it is possible to search for AEO-certified companies or for types of certificates, i.e., if the companies have a certificate for customs simplifications, a certificate for security and protection, or a combined certificate. However, companies can state in their applications that they do not wish their certification to be made public.

Advance cargo declaration

The advanced cargo declaration scheme, sometimes called the 24-hour rule, is the EU's version of a US system requiring that cargo interests file container manifest information a day before loading. It is designed to prevent terrorists from using onboard boxes as a conduit for weapons of mass destruction. It came into effect from July 2009. Under these requirements, businesses will have to provide customs with the additional cargo information listed in Annex 30A of EC Regulation 1875/2006. This will have to be submitted in advance, for use in the risk assessment process to help identify high risk consignments before their arrival in, or departure from, an EU customs territory. For goods entering the EU, advance cargo information will have to

be provided, prior to arrival, in an Entry Summary Declaration (ENS), to be submitted electronically to the customs office of first entry (usually the first port of entry) via the Import Control System (ICS). For exports, this will have to provide in an Exit Summary Declaration (EXS), submitted via the Export Control System (ECS), prior to departure.

Amendments to Regulation 1875

As a result of the ongoing discussions about implementation, it has become apparent that some changes need to be made to Regulation 1875, and a number of amendments are expected to be agreed in the autumn. These include changes to the timelines for submitting cargo declarations and to the data table for the advance information (Annex 30A). In addition, the original requirements for a Pre-arrival Notification (PAN) and for multiple Entry Summary Declarations for subsequent port calls will be deleted.

The United States

ISO seal

The US Customs and Border Protection (CBP) issued a notice stating that, with effective from 15th October 2008 all maritime containers in transit to the United States are required to be sealed with a seal meeting the International Organization for Standardization Publicly Available Specification (ISO/PAS) 17712 standard. The background to this are the provisions contained in the legislation:"Implementing Recommendations of the 9/11 Commission Act". Certain non-standard containers can be exempted. The notice goes on to state that vessel carriers must transmit, via the Vessel Automated Manifest System (AMS), all seal number to CBP at least 24 hours before cargo is laden aboard a vessel at a foreign port.

ISPS

The International Ship and Port Facility Security (ISPS) Code is an amendment to the Safety of Life at Sea (SOLAS) Convention (1974/1988) on minimum security arrangement for ships, ports and government agencies. It came into effect in 2004. It is a kind of responsibility to governments, shipping companies, shipboard personnel, and port/facility personnel to detect security threats and take preventative measures against security incidents affecting ships or port facilities used in international trade. The Code is a two-part document to show minimum requirements for the security of ships and ports. Part A provides mandatory requirements while Part B provides guidance for implementation. The ISPS Code applies to ships on international voyages (including passenger ships, cargo ships of gross tonnage (GT) of 500 tons or

more and mobile offshore drilling units) and the port facilities serving such ship.

CSI

The Container Security Imitative (CSI) was launched in 2002 by the U.S. Bureau of Customs and Boarder Protection (CBP), and the agency of the Department of Homeland Security. It's purpose was to increase security for container cargo shipped to the United States. As the CBP puts it, the intent is to extend the zone of security outward so that American borders are the last line of defense, not the first. Under the CSI programme, the screening of containers that pose a risk of terrorism is accomplished by teams of CBP officials deployed to work in concert with their host nation counterparts. CSI consists of four cores: (1) Using intelligence and automated information to identify an target containers that pose a risk for terrorism; (2) Pre-screening those containers that pose a risk at the port of departure before they arrive at U.S. ports; (3) Using detection technology like X-ray, gamma ray, and radiation detection devices to quickly pre-screen containers that pose a risk; (4) Using smarter, tamper-evident containers.

C-TPAT

The Customs Trade Partnership Against Terrorism (C-TPAT) is a voluntary supply chain security programme led by US Customs and Boarder Protection (CBP) and focuses on improving the security of private companies supply chains with respect to terrorism. The programme was launched in November 2001 with seven initial participants, all large US companies. As of April 2005, there were more than 9000 companies involved.

US Customs 24-hour rule

As a result of increased security measures within the United States, the US Government has implemented a number of changes in cargo documentation requirements for all cargoes imported in the US. As of 2nd December 2002, all shipping lines have to submit manifests 24 hours prior to loading in Asia. The shipping lines are not allowed to load cargo unless the manifest information is submitted and accepted in accordance with the above deadline. The rule applies to container shipment and break bulk.

AMS

The Automated Manifest System (AMS) is a multi-modular cargo inventory control and release notification system for sea, air and rail carriers. AMS speeds the flow of cargo and entry processing and provides participants with electronic authorization to

move cargo prior to arrival. AMS facilitates the intermodal movement and delivery of cargo by rail and trucks through the inbound system.

AMS reduces reliance on paper documents and speeds the processing of manifest and waybill data. As a result, cargo remains on the dock for less time, participants realize faster tracking, and Customs provides better service to the importing community.

Conclusion

The terrorist events of 11th September 2001 in the US have brought a great focus to the ways in which national security is viewed. International agencies such as the International Maritime Organization and most national governments have been active in developing new security policies. One of the outcomes of 11th September 2001 has been a significant tightening of all supply chain security regimes throughout the world as the US has become increasingly concerned about the possible impacts on its internal security. This also has led to the European Union having a focus on pushing out the security boarders.