Using Total Quality Management to Mitigate Supply Chain Risk

Terry D. Crippen
Navmar Applied Sciences Corporation, USA

INTRODUCTION

With recent mergers in many industries such as the mergers of Merck and Schering-Plough, Wyeth and Pfizer, and Rouche and Genentech, there is growing pressure on industries to reduce costs. These reductions can include the outsourcing of key functions including manufacturing and distribution.

These pressures, along with a growing threat of altered or counterfeit products being inserted into the supply chains, has many industries on alert to implement the most secure supply chains possible. There are also efforts on the part of the Department of Homeland Security's Customs and Border Protection (CBP), as well as their counterparts around the world, to help businesses secure their supply chains. Part of their efforts focus on not just the physical security of the shipment, but on the security of the information being passed.

The goal of this article is to show that the Governments and regulatory agencies are dealing with the oversight on supply chain security, but that more needs to be done at the source (warehouse, plant, etc.) to install a Quality Management System (QMS). It will outline how to reduce the risks found in supply chains and how to employ a Total Quality Management system to mitigate risks both in the physical and electronic realms. Lastly, it will provide recommendations that will provide an outline of what aspects should be included in an overall Quality Management System for logistics.

BACKGROUND

Since September 11, 2001, there has been a serious focus on the physical security of supply chains due to the fact that it is one method that a terrorist could bring a weapon into this country. Lee (2001) states that, "Governments and industry have already responded with proposals to create more confidence in supply chain security, while maintaining smooth flows of goods and services in a global supply chain (p. 2)." One of the biggest problems faced by these entities is the need to add visibility to the supply chain without creating delays and bottlenecks. The free-flow of goods must continue without those delays and without substantial increases in costs. Additional costs include the need for increased stock levels due to longer lead times in shipping, additional insurance premiums for lost cargo, and the expansion of the supply chain to keep inventory where it is needed to meet customer demands (Lee, 2001, p. 2).

The Department of Homeland Security's Customs and Border Protection (CBP) has the responsibility of insuring that the freight entering the United States is secure and will not pose a risk to the country. Their authority is unmatched to accomplish this goal. The CBP states in their *2006-2011 Strategic Plan* that,

The border authority of CBP is unsurpassed in defense of national interests because examinations of cargo and persons do not require search warrants, probable cause, or particularized suspicion. In order to allow for the movement of legitimate travel and trade, CBP uses all resources at its disposal to target travelers and cargo that pose a risk for terrorism and to facilitate the flow of legitimate trade (p. 10).

CBP, through its Container Security Initiative (CSI), does not work solely at US ports; it has expanded its reach to foreign countries. They have agents posted at every port to inspect freight at the port of departure during normal down-times before loading so that any suspicious loads can be flagged for further inspection (CBP, p. 12). Partnerships overseas are vital to the success of these types of programs like the CSI. The European Commission, for example, welcomes this type

DOI: 10.4018/978-1-4666-5888-2.ch144

of program, "The European Commission continues to advocate the internationally recognized multi-layered risk-based approach including mutual recognition of trade partnership programs for enhancing and protecting the international supply chain (Verheugen, 2009)."

Even with the efforts of CBP and its partners around the world inspecting containers before departure and when it enters into the United States, it is still not possible for every container bound for the United States be physically inspected (Dedic, 2007). It is estimated that, "about 5 percent of containers are subject to such visual inspections in the United States or before leaving foreign ports (Lipton, 2006)." But is it realistic or even necessary to inspect every container? Dr. Stephen E. Flynn, former commander of the United States Coast Guard (ret.) thinks that it is not. "Examining 100 percent of all containers is not only wasteful, but it violates an age-old axiom in the security field that if 'you have to look at everything, you will see nothing'" (Flynn, 2003). He goes on to say that it is the anomalies that draw attention to suspicious shipments. He states that since criminals do not ship every day, and that they are more likely to make mistakes that could trigger an alert (Flynn, 2003). Scott Dedic (2007) of the International Cargo Security Council believes that there must be a "layered and holistic" approach to supply chain security, and that it needs to encompass "best practices, technologies, and people."

Up to this point, each of the initiatives described secures the freight during transit from the warehouse to the final destination. Not only is tighter security needed for inbound freight, but also the warehouses as well. The Eli Lilly case of 2010 illustrates that need for tight physical security in warehouses. Traynor (2010) wrote, " that there was no security fence around the warehouse at the time of the theft, although plans had been in place to install one."

The next focus needs to be on a QMS used by the warehouses both on the shipper's and the receiver's side which will encompass security and risk mitigation. The security of the facilities is done through many different security standards, two of which are the International Standards Organization's (ISO) 28000 series of security programs or the CBP's Customs-Trade Partnership Against Terrorism (C-TPAT) initiative. Both programs do not just secure the facilities; they attempt to secure the entire supply chain. Alan Bryden, the Secretary-General of the International Standards Organization stated on the ISO 28000 standard that:

Threats in the international market-place know no borders. The ISO 28000 series provides a global solution to this global problem. With an internationally recognized security management system, stakeholders in the supply chain can ensure the safety of cargo and people, while facilitating international trade, thus contributing to the welfare of society as a whole (ISO, 2007).

The focus here will be on the facility security aspects of each of these programs. Both programs dictate that organizations must employ security best practices at their facility and must be able to demonstrate adherence to those policies. This is done through audits by either the governing body or through a certified third-party vendor acting on their behalf.

The best practices cover a range of topics. They include how the facility is secured, whether there is an alarm system in place, security guards, and fencing. The goal is to prevent unauthorized individuals from having access to the facility. Some companies even employ biometric technologies for facility access (Katz, 2007). It addresses hiring practices, such as background checks and other pre-screening processes. There must be written Quality policies in place for cargo inspection procedures, packaging procedures, and discrepancies. It also addresses vendor qualification which is used to verify that the vendor will be maintaining the same security practices that are necessary to ensure that the entire supply chain remains secure. According to the *C-TPAT Best Practices Catalog*, "The Company requires that all business partners accept and implement the C-TPAT security criteria, if they wish to continue to do business (CBP, p. 13)." This does not mean that the business partners be C-TPAT certified, it just means that they must be able to demonstrate that they meet certain security standards to maintain the integrity of the supply chain. There are also standards for information security. Information systems must meet standards for both physical accesses to the systems as well as log-in security via passwords. There also must be standards for back-ups and disaster recovery (CBP, p. 47).

All of these programs are designed to increase the level of security for freight moving from overseas into the United States. While there probably will never be a completely secure supply chain, continued improvements to existing programs as well as the implementation of new programs will go a long way towards reducing risk. Of all the programs described within this article, Stephen Flynn states that: