Facing the Realities and Probabilities of Enhancing Supply Chain Security

Wednesday, June 1, 2011

by Dr. Jim Giermanski

Supply chain security is not a 9/11-only phenomenon. Governments, non-Government Organizations (NGOs), and the private sector been working to improve the global supply chain since the late 1990s. The core objective was and is to know definitively what the cargo and its quantity really are and monitor its movement from origin to destination. The following agreements, programs, and laws, in one way or the other, acknowledge this core objective.

HISTORICL PROGRESSION AND OVERVIEW

**Kyoto Convention of 1999 (1)** The Kyoto Convention was the genesis for improving and modernizing Customs practices around the world and looked at high risk shipments. It specifically supported the concept of applying new technology to Customs practices and encouraged the electronic transmission of information.

**Trade Act of 2002 as amended by The Maritime Transportation Security Act** As amended, the Trade Act of 2002 required the use of advance electronic cargo data and the importance of ensuring maritime Intelligence. See below, *Trade Act of 2002* summary of rules.

**UN Economic Commission for Europe Recommendation 33 - Single Window (2004)** The Single Window concept is an electronic framework through which “…trade-related information and/or documents need only be submitted once at a single entry point to fulfill all import, export, and transit-related regulatory requirements.”

**Automated Commercial Environment (ACE) and E-Manifest Systems** As a result of The Trade Act of 2002, as amended by the Maritime Transportation Security Act of 2002, Customs and Border Protection (CBP) promulgated regulations to begin collecting all cargo manifests electronically.

**Customs Trade Partnership Against Terrorism (C-TPAT), 2001** C-TPAT, amended after the WCO Standards in 2005 and 2006, requires origin-to-destination control clearly acknowledging that security begins at stuffing. It also recommends the use of tracking, monitoring and breach detection systems.

**U.S. Container Security Initiative (CSI), 2002** CSI merely an initiative of the U.S. Commissioner of Customs after Sept.11, 2001, has been codified into U.S. Law in the SAFE Port Act. Among its core elements are the identification of high-risk containers (advance information and intelligence), the prescreening and evaluation before sailing to the United States, X-ray and gamma ray screening and the use of smarter, more secure containers.

**Kyoto Convention ICT Guidelines (Information and Communication Technology)2004** These guidelines called for an electronic exchange of information for export and import activities, creating a chain of “electronic” data. These went into effect in 2006.

**World Customs Organization (WCO), Framework of Standards to Secure and Facilitate Global Trade 2005** The WCO developed its *Framework Standards to Secure and Facilitate Global Trade (Standards)* (2), to “...push
the security of cargo and container further back into the supply chain by involving the private sector and by requiring increased security at the point of origin, e.g. the point of stuffing a container at a foreign manufacturer’s loading docks, and as the container is moved point to point through the supply chain.” (3)

**SAFE Port Act, October 2006** The SAFE Port Act signed into law on October 13, 2006, recognized the role of in-container security devices and defined them:

**CONTAINER SECURITY DEVICE.**—The term “container security device” means a device, or system, designed, at a minimum, to identify positively a container, to detect and record the unauthorized intrusion of a container, and to secure a container against tampering throughout the supply chain. Such a device, or system, shall have a low false alarm rate as determined by the Secretary

**Implementing the 9/11 Commission Recommendations Act of 2007 (ICRA)** The ICRA goes much farther than the SAFE Port Act by requiring the use of breach detection and access to the container “prior” to entering the U.S.

**International Standard Organization (ISO) Standard 28000, 2007** Known as the Specification for Security Management Systems for the Supply Chain, the ISO 28000 series specifies the requirements for a security management system to ensure safety in the supply chain. Its standards can be applied by organizations of all sizes involved in manufacturing, service, storage or transportation by air, rail, road and sea at any stage of the production or supply process.

**Ten + Two Program** One of the latest CBP programs is the Ten + Two Program. This program requires the filing of 10 pieces of information by the U.S. importer on companies involved in an import shipment. If not filed, CBP could issue a “no load” order on the import.

**THE REALITY OF KNOWING**

1. **Knowing Container Content**

All of these agreements, programs, and laws, one way or the other have 4 common elements:

   a. container content;
   b. its control during its voyage;
   c. its threat level; and
   d. the timely transmission of these data.

From Kyoto to the present day, there is a developing global consistency in the collection, storage, and electronic transmission of trade and manifest data from the stuffing of the container at origin to the opening of the container at destination. However, although this is occurring, common sense tells us that the reality or really knowing with 100% accuracy the contents of the container is a matter of statistical probability. This is due, as it is in all security and intelligence matters, to the human factor, often the lowest common denominator in security. There are really only 5 available options in verifying actual container contents.

   a. A government Customs Inspector to verify loadings at origin - Obviously that is impossible.
   b. A government 3rd party inspector to verify - Possible but not affordable for governments.
   c. A non-government 3rd party paid for by the seller or buyer to verify content and quantity - Very doable especially in the light of international commercial terms and rules embodied in the new
Incoterms® 2010 (4), which went into effect in January 1011. Examples of firms already doing these inspections are SGS, Cotecna, and Intertek.

d. An identified, vetted, authorized company employee at origin who confirms cargo and quantity through documentation. This option, while not the strongest, is also a doable, realistic method of knowing the real content.

e. Finally, the best option is the use of this vetted company person or non-government 3rd party firm coupled with the use of electronic Container Security Devices (CSDs) attached to the interior of the container that can monitor access to it, its internal environment and movement of the container carrying electronically, logistic data, including cargo and container identification, all within the CSD armed when the authorized agent personally seals the container at origin.

These electronic data must be generated at the shipper’s site and be transmitted as soon as the container begins its initial travel to destination. Data may include divergent information depending on unique government requirements, circumstance of product, mode of carriage, country of origin, history of shipper and consignee and more. Derived from the Bill of Lading and/or Booking confirmation and/or Dray Order, CSDs can carry information such as:

1. Identity of the Authorized Person supervising stuffing and arming the system at origin;
2. Document Number;
3. Booking Number;
4. Shipper/Exporter;
5. Forwarding Agent and License Number (e.g. FMC No.);
6. City or Point of Origin (Stuffing);
7. Date of Departure from Origin if Known;
8. Consignee;
9. Notify Party;
10. Place of receipt by land carrier;
11. Exporting Carrier (vessel line);
12. Sea Port of Loading (Origin Sea Port);
13. Loading Pier or Terminal if known;
14. Sea Port of Discharge (Destination Sea Port);
15. Declared Value;
16. Container ID Number;
17. Gross Weights in Lbs. or Kgs or measurements; and
18. Description of Goods (6 digit tariff number).
Required Customs Forms may add to this list by requiring:

1. IMO number;
2. Nationality of Ship;
3. First Port or place where carrier takes possession;
4. Name of vessel;
5. Name of Master;
6. Last foreign port before U.S.;
7. Marks and Nos. (container numbers);
8. Bill of Lading number;
9. Driver’s identification; and more.

2. Focusing on the Individual

The focus on the individual varies depending on the operations of the firm. In the large corporate world of publicly traded companies, the U.S. government has influence in the corporate ethics issue through legislative action embodied in the Sarbanes Oxley Act of 2002 (SOX) which is changing the face of corporate governance and corporate responsibility starting at executive levels by making the CEO and CFO as “signing officers” personally responsible for establishing and maintaining internal controls embodied in rules, documentation, and disclosures (5). SOX is applicable to both U.S. and foreign firms publicly registered and traded in the United States.

A. Individuals within the SOX Corporate World

Inventory, alone, can be used to manipulate and distort a financial picture of a firm. Therefore, if there is no transfer of ownership, there is no sale. One problem in international business, given the distances, and options available to buyer and seller, involves the locus of exchange for control or ownership. For instance, does a U.S. importer take ownership in the foreign nation, aboard the vessel in route, when it is discharged from the vessel or when it reaches his or her warehouse in the United States? If it is someone else’s merchandise until it reaches the U.S. destination, who has the security risk and liability? Where does the merchandise become the inventory of the buyer? Are assets determined on the sale or on custody? How are these inventories reported? The bottom line for SOX is honest reporting of inventory, value, revenue, and ownership. Most of this ethical reporting constitutes honest corporate reports made by honest employees, all of which bear supply chain security implications (6).

B. Individuals within Smaller Firms

Ownership and control are also related to security. Since September 11, 2001, the United States has become more and more concerned about the potential linkage of terrorism and trade.

The Patriot Act, the Trade Act of 2002, the Maritime Port Security Act of 2002, the creation of the new Department of Homeland Security and the Department’s Bureau of Customs and Border Protection (CBP) demonstrate this concern, especially from the potential threat imposed by inbound traffic to U.S. seaports and land ports - thus, the development of two major CBP programs applicable to all sizes of companies, CIS (Container Security Initiative) and C-TPAT (Customs Trade Partnership Against Terrorism). Although voluntary, participating U.S. importers must comply with C-TPAT mandates, for instance:
Importers must conduct a comprehensive assessment of their international supply chains based on the following C-TPAT security criteria. Where an importer outsources or contracts elements of their supply chain, such as a foreign facility, conveyance, domestic warehouse, or other elements, the importer must work with these business partners to ensure that pertinent security measures are in place and adhered to throughout their supply chain. The supply chain for C-TPAT purposes is defined from point of origin (manufacturer/supply/vendor) through to point of distribution -- and recognizes the diverse business models C-TPAT members employ (7).

Since 2005, additional mandates have been added. And like SOX, "Importers must have written and verifiable processes for the selection of business partners including manufacturers, product suppliers, and vendors" (8). C-TPAT is also available to foreign manufacturers (9).

Besides C-TPAT, there is a Homeland Security Presidential Directive 12 requiring certain workers connected to the supply chain to have secure identification and have undergone security background checks. For Federal contract employees they must undergo background checks and in some cases clearances. However,

Recent studies have shown that as many as half of corporate security officers believe their corporations have inadequate background checks, and that they are less involved in the vetting process than they should be. The ISO 17799 reviews the writers have conducted within the financial industry support similar conclusions. One could argue that 20 to 25 percent of critical employees do not receive adequate background investigations. (10)

For all firms, the ultimate, bottom-line necessity must be the use of genuinely vetted personnel being identified as the ones verifying the cargo, securing the container and being subject to legal and personnel action if what arrives is not what was shipped using a chain-of-custody CSD with its built-in safeguards to protect the cargo and the authorized persons verifying stuffing at origin, and opening the container at destination. This process is likely to start with non-government 3rd party vetted agents or the seller's own vetted personnel identified for legal retribution if and when necessary.

Additionally, good personnel selection, training, and follow-up review limit fraud and cargo loss at terminal and distribution sites worldwide. Although the private sector does not have access to the data mining and integrating software used by intelligence and law enforcement, good background, criminal, and credit checks must be made on all personnel, especially for firm involved with handling cargo in a global supply chain. Supply chain risk management is fundamentally an issue of control.

CONCLUSION

What is absolutely clear is that the "human element" is the essential core component of supply chain security. Global supply chain and container security systems are inextricably linked to personnel selection, their competence, and performance. Controlling risks in any international supply chain must begin, be executed by, and end with the human component. Therefore, that combination of direct control in personnel selection, and the use of technology, especially CSD chain-of-custody technology, should be the main focus of managing risk within the global supply chain. It is the human element and its quality combined with CSD technology that can only increase the reality and statistical probability of knowing what's really in the container. (11)

About the Author
A former Regents Professor at Texas A&M International University, Dr. Jim Giermanski is now Professor of International Business and Director of Centre for Global Commerce at Belmont Abbey College. He has been chosen as the International Educator of the Year by the National Association of Small Business International Trade Educators and has been appointed to the graduate faculty at the University of North Carolina at Charlotte. In conjunction with the Professional Examination Service (PES) and Bradley University, he is a member of the International Practice Analysis Committee of the NASBITE Task Force to develop a national International Trade Specialist Certificate. He is also a reviewer for the Transportation Research Board, U.S. National Research Council. He served as Director of Transportation and Logistics Studies, Center for the Study of Western Hemispheric Trade at Texas A&M International University.

Dr. Giermanski consults often on international transportation and transportation security, border logistics, and trade matters involving Mexico. He has frequently given invited testimony on NAFTA, transportation, and other international business issues before the U.S. Senate and House, the Texas Senate and House, EPA, and the U.S. International Trade Commission. He served as the co-chairman of the Texas Transportation Committee of the Task Force to prepare for NAFTA, sat for 5 years on the Texas Office of the Attorney General’s Trans-border Trucking International Working Group, and for three years as a member of the Research Advisory Committee on Management and Policy, Technical Advisory Panel, Texas Department of Transportation. He has been requested to serve as a border expert to assist the Arizona Department of Transportation in developing concepts and practices to improve the border crossing activities on the Arizona Mexico border, and at the request of the White House, Council of Economic Advisors, he provided information on trade issues and barriers on the southern border.

He has authored over 100 articles, books, and monographs and has given over 100 presentations. He has been published extensively on transportation and trade issues and for five years wrote the International Insight column in Logistics Management. In addition to his scholarly writing, he has been published in the Journal of Commerce, El Financiero, Traffic World, Strategic Finance, Transport Topics and most recently, Tax Notes International. He has been interviewed by and quoted in over 50 national and international publications such as the Wall Street Journal, the New York Times, Forbes, the Financial Times, Christian Science Monitor, and has appeared nationally as a special guest on the FOX News Channel’s Special Report with Brit Hume, CNN, NBC, CBS, NPR, BBC, Voice of America and the Canadian Broadcasting Corporation in addition to many local and regional affiliates.

Finally, with his background as a former FBI special agent, OSI special agent and a Colonel in the Office of Special Investigations where he handled counterintelligence matters, Dr. Giermanski is Chairman of the Board of Powers International, Inc. which provides supply-chain security solutions, consulting, and training. He currently provides transportation security lectures on C-TPAT, and other Customs and Border Protection (CBP) programs. Dr. Giermanski has a Masters degree from the University of North Carolina in Charlotte, a Masters from Florida International University, and a Doctorate from the University of Miami. He is a graduate of Air Command and Staff College, and The Air War College while also serving as a visiting scholar at the Center of Aerospace Doctrine, Research, and Education, an Air Force think tank.

Citations

(2) http://www.wcoomd.org/ie/En/Press/WCO%20FRAMEWORK%20OF%20STANDARDS%20June%202021%20Final.pdf

(3) Framework of Standards to Secure and Facilitate Global Trade, Version No. 2.0, World Customs Organization, April 2005, p. 12


(9) Online Application for Foreign Manufacturers, Customs and Border Protection, August 9, 2005, p. 1.

