http://www.hstoday.us/blogs/best-practices/blog/knowing-the-contents-of-cargo-containers-before-they-arrive-at-us-shores/2be539ee4f914b6d3d66f7553de2ae06.html

DHS TODAY WEEKLY BRIEFING
HSTODAY.US
Programs, Policies and Technology

Best Practices

BEST PRACTICES Readers share their knowledge and expertise to provide the newest, most creative means of solving homeland security issues. Comments on any of these pieces are welcome. To provide articles in this area please send to Akimery(at)HSToday.us.

Knowing the Contents of Cargo Containers Before They Arrive at US Shores

February 25, 2013

By: Dr. Jim Giermanski

A recent comprehensive report by Anthony Kimery, *Homeland Security Today's* Online Editor and Online Media Division manager, outlined the issues of not knowing whether radiation is present in shipping containers arriving at 22 US maritime ports.

While his report focused on problems, costs, function and effectiveness of portal monitors for scanning containers, it also made the reader realize that Customs and Border Protection (CBP) simply doesn't know what is in a shipping container, and worries about it "after" it arrives at a US port, not knowing from origin the contents, and not knowing what happened to it during its voyage.

Kimery's report forces the question: What does CBP really know about any shipping container's cargo, least of all whether it contains a radioactive material or nuclear weapon? But what is even more startling about this issue is that real human-factor

processes and off-the-shelf technology exist right now that can be utilized to solve the problem of verifying container contents and detect, without scanning, the presence of radiation in an arriving shipping container …surpassing the ineffective, expensive and time-consuming scanning equipment and process that World Customs Organizations and US trading partners refuse to endorse.

The real question, then, is how do we know what's in a shipping container on its way to the United States? There are really only two ways to do this, First, a person informs us, and second, technology senses it. Both, however, have inherent weaknesses. While no one system is ever 100 percent effective … or reliable, both necessarily need to be used. Just as in flying across country, there is no 100 percent certainty that the plane will land safely, even though that's clearly the desired outcome.

In the case of shipping containers, though, the government and the private sector want as close as 100 percent knowledge of a cargo container's identification, quantity and condition as possible, and reassurance that it has not been tampered with, removed, replaced or in some way denigrated or contaminated during its movement. The human factor involves the use of a presumably trusted, uncorrupted person. The technology component equation involves the use of container security devices (CSD). Each serves both business and government.

Business and government use of trusted agents

The business reasons for knowing what's in a container are very clear and relate to the risks associated with buying or assuming liability for the product during its movement. International sellers are expected to ship what has been ordered. And to insure that that happens, the global community has business entities that physically inspect and verify the cargo that's stuffed into shipping containers. But there really are only five available options for verifying a container's contents.

First, a government customs inspector verifies loadings at origin – but, obviously, that is impossible.

Second, a government 3rd party inspector verifies the contents, which is possible, but not affordable for governments.

Third, a non-government 3rd party is contracted by the seller or buyer to verify content and quantity. This, too, is doable, especially in light of international commercial terms and rules embodied in the new Incoterms 2010 international rules for buyers and sellers with respect to carriage, liability, etc., that went into effect in January 1011. Examples of firms already conducting such inspections are SGS, Cotecna and Intertek.

Fourth, an identified, vetted and authorized company employee at the container's origination point confirms cargo and quantity through documentation. This option, while not the strongest, is also a doable, realistic method of knowing a container's content.

And the fifth and best option is the integrated use of a vetted company person or non-government 3rd party firm, coupled to the use of electronic Container Security Devices (CSD) affixed to the interior of the container that can monitor access, the container's internal environment, and the movement of the container through electronic and logistics data, including cargo and container identification -- all within the capacity of the CSD's software to transmit as programmed when the authorized agent personally arms the CSD and seals the container at origin. However, CBP mandates neither the human factor nor the use of CSD technology. Consequently, it doesn't really know what's in a container.

To remove any doubt about what CBP knows about a shipping container's content, I inquired about the matter with a number of authorities who report manifest information through the Automated Commercial Environment (ACE) system. According to CBP, ACE is the commercial trade processing system that's being developed by the agency to become the "single window" through which international traders will electronically provide all information needed by federal agencies for the import of cargo. ACE is the enabler of further collaboration between the US government and the trade community to enhance the security, safety, compliance and flow of international trade.

My questions focused on the knowledge of authorities who report manifest information through ACE regarding the actual content of containers at the time they reported it to CBP using ACE. These ACE users -- or trusted agents – deal with both sea and land shipments into the United States. The sample included only two categories of trusted agents, US Customs Brokers and national motor carriers who communicate through ACE. Since no trusted agent in the ocean-borne cargo area responded to my questions, the following is an example of the responses I received from ACE-qualified US Customs Brokers and carriers handling land shipments across our borders.

Question: How do you know what is in a container or trailer if you never opened it to inspect the cargo? (Note: Unless loading themselves, all brokers and carriers responded that they do not know the contents of trailer or container. An LTL carrier stated that when receiving fully loaded trailers, it relies on the documentation stating what's in the container).

Example of Responses: "We really don't know and neither does CBP. We rely on information provided by the shipper. When receiving a full trailer load, we rely on the shipper's load and count and/or annotated on the bill of lading. If the trailer is pre-loaded and sealed at a shipper, we have no way of knowing if there is anything in the trailer …"

Question: Do you assume the veracity of the documentation accompanying cargo? (All said that they simply depend on the documentation they are provided).

Examples of Responses: "Yes, we are led to believe that the information provided by the exporter is accurate. We assume the veracity and rely on the information provided. We also perform verification of piece counts, but we do take the counts on the Bill of Lading. We can only go on what the drivers transmit …"

In other words, the only source of real knowledge about conveyance content must come from an identified person at loading who certifies the cargo, its quantity and condition, and then seals the conveyance for its monitored movement to the United States.

There is one more significant business concern for accurate knowledge of conveyance contents. In September 2009, the United States became a signatory to the United Nations Convention on Contracts for the International Carriage of Goods Wholly or Partly by Sea (Rotterdam Rules). When signed by President Obama with the "Advice and Consent" of the Senate, the Rotterdam Rules supersede the Hague, Hague-Visby and Hamburg Rules … replacing the previous US Carriage of Goods by Sea Act (COGSA).

COGSA currently obligates the vessel carrier to a "tackle-to-tackle" mode wherein liability for the cargo begins at that moment that the goods are laden into, and discharged from, the vessel to a new "door-to-door" mode. According to the UN General Assembly, the Rotterdam Rules is a "…uniform and modern global legal regime governing the rights and obligations of stakeholders in the maritime transport industry under a single contract for door-to-door carriage."

Essentially, the new rules now put the legal liability for the cargo on the vessel carriers themselves -- from the origin of the shipment. In other words, from where the shipping container originally was stuffing with whatever is in it.

Business and government use of technology

In addition to the human factor, there also are technical options. However, the technology options have greater offerings than just identity, quantity and condition of the cargo at loading. New container security devices can electronically incorporate a container number, booking, bill of lading and manifest data along with the identity of the authorized agent who verified the cargo at the time the shipping container was stuffed.

Additionally, CSDs can incorporate specific sensors that can detect the presence of explosives, chemicals and even shielded highly enriched uranium (HEU). They also can detect and report any unauthorized entry into any part of the conveyance, even if it went off-course during its movement to the United States, and all well before the conveyance arrives.

For instance, ConSearch, LLC, a small South Carolina-based company has developed technology composed of a chemical and radiological detection system to determine the presence of contraband (e.g.: nuclear weapons, illegal drugs, chemical weapons, explosives, concealed humans, etc.) in shipping containers, which include ISO "dry box" containers, rail cars and trucks. The detection system will automatically perform radiological and chemical analyses for contraband materials while the containers are in transit.

The detection system is interfaced with a CSD that can report any anomalies at any point along the shipping route, including containers in transit on container ships, stored in ports

or anywhere else in route (by rail or road) that are destined for distribution into the US supply chain.

Since the analyses and the reports of the analyses are performed and reported during the "dead time" of the container's transit process, the smooth and unimpeded flow of containers through US ports or across international borders is assured. Detection of contraband or other abnormalities are reported instantaneously at any point during the progress of the container.

This technology has already been successfully demonstrated for the European Union's tax authorities, and, at Department of Homeland Security (DHS) facilities. Yet, it still isn't being used. Instead, DHS continues to put money and time into the major corporations involved in the development and use of scanning technology that simply do not work, as Kimery's report clearly articulated.

The role of CSDs and their multiple offerings to both business and government cannot be overestimated. CSDs with sensors such those used by ConSearch LLC, along with additional CSD applications that are able to provide a complete end-to-end "Chain-of-Custody" system, in effect accomplish everything that DHS and CBP have not been able to accomplish with shipping container scanning technology, draining millions -- perhaps billions -- of tax dollars toward the development and purchase of ineffective government-supported technology.

Current off-the-shelf (COS) private-sector technology offers DHS, CBP, shippers, carriers and importers with real-time knowledge about shipping container content long before it arrives at a US seaport or land Port of Entry, and, ultimately at its final US destination.

Conclusion

There's little question that the integration of both human and technological factors in the identification of cargo, its quantity and condition is available. There's also little question that either or both can be compromised. Yet, this integration of human activity and technology in knowing what's in conveyance content far exceeds what DHS and CBP have developed to know shipping container content prior to its arrival in the United States. And both exceed what the official practice is today, which is reporting through ACE what the conveyance is "said to contain" -- the very term that's not permitted to be used for the identification of container or trailer content.

The reality is that those trusted agents who have never seen the cargo that's actually loaded into the conveyance, officially report its identity and quantity without knowing what it is. Currently, they simply take the word of a carrier who picked it up … or the word of a shipper about whom they know little about.

As I have said before, CBP plays a "let's pretend we know" game, when the reality is we can really know. And that, is *no* game.

Known as the "Paul Revere of cargo security," Dr. Jim Giermanski is chairman of Powers Global Holdings Inc. and a former Regents Professor and past director of Transportation and Logistics Studies, Center for the Study of Western Hemispheric Trade, at Texas A&M International University. He also served as an adjunct graduate faculty member at the University of North Carolina at Charlotte. Giermanski is a former Air Force Colonel who, as a special agent in the Air Force Office of Special Investigations, concentrated on counterintelligence and clandestine base penetrations. He also is a former FBI agent and worked with Customs and Border Protection on drug intelligence development. His new book, Global Supply Chain Security, was published by The Scarecrow Press, an imprint of The Roman & Littlefield Publishing Group.