RFID JOURNAL
THE WORLD'S RFID AUTHORITY

International Cargo Conundrum

How much investment in security is enough?

Feb. 6, 2006—What must be done to provide an "adequate" measure of cargo security? Are electronic freight container seals (e-seals) a good investment?

These questions were debated at **eyefortransport's North American Cargo Security 2005 Forum**—held in Washington, D.C., in December—by representatives from such large importers as **Boeing** and **Procter & Gamble** (P&G), as well as transportation and logistics companies, and information and cargo seal technology vendors. Not everyone agreed on the answers, but they did concur that the U.S. government must invest more to step up private investment.

Tectonic Shift in Cargo Security Since 9/11

Corporate supply chain security managers speaking at the conference described grappling with the change in cargo security emphasis since 9/11—from prevention of theft and contraband to terrorism. The new threat is exceedingly difficult to evaluate. Clearly, weapons of mass destruction, slipped in by terrorists into U.S.-bound cargo shipments, could cause catastrophic loss of life and harm to the economy. Still, the U.S. has not had a major terrorist incident since 9/11, and multiple speakers acknowledged that complacency was growing. Some are starting to see their company's security budget reduced in response to unremitting cost-cutting pressure.

Supply Chains More Vulnerable Than Ever

The increasing resistance by U.S. companies to spending on cargo security was especially worrying to attendees, who believed that—despite post-9/11 efforts to improve security—the vulnerability of U.S. companies' supply chains was increasing. Why the increase?

First, global trade is increasing at a 10 percent annual rate in recent years. The quantity of shipping containers, used to transport 90 percent of the world's cargo, have also been increasing, at 7 percent annually. What's more, U.S. imports continue to grow faster than exports. More than 10 million containers entered U.S. ports in 2005, and some experts predict that this number will roughly double by 2010.

Second, an increasing proportion of U.S.-bound containers are arriving from developing countries, where security practices are less reliable. "Security is different in different cultures as you go around the world," remarked Jeff White, director of asset protection at **Kmart**, a company known for its attention to supply chain integrity. "In some countries, a good security system may be a dog behind a fence."

The biggest security gap exists between the overseas factory or distribution center, where containers are filled, and the port where they are loaded onto ships. U.S. importers have limited ability to close this gap because of national sovereignty and the number of cargo handoffs obscuring the chain of custody.

Referring to his company's "Secure Commerce Roadmap"—a novel guide to assessing the investment-worthiness of various cargo security and tracking technologies—Ted Langhoff, director of supply chain security group at **Unisys**, pointed out that the sheer complexity of the global supply chain poses a huge challenge to security: "In addition to international jurisdiction, the typical international shipment involves 20-plus handoffs, 25-plus documents, 200-plus data elements, and public/private sector integration."

Four New U.S. Programs Since 9/11

Since 9/11, the U.S. government has moved to create a baseline of regulation within its jurisdiction, and to work with other governments toward creation of a worldwide baseline.

Customs organizations play a central role in enforcing such regulations. The World Customs Organization's recently developed "Framework of Standards to Secure and Facilitate Global Trade" calls for national programs that recognize authorized economic operators (AEOs)—shippers and transportation service companies volunteering to comply with the country's cargo security guidelines. These companies and their supply chain partners are considered "trusted," with their cargo marked to receive expedited handling at the country's borders. Such classification enables customs authorities to focus on higher-risk cargo from non-qualifying organizations.

Consistent with WCO's framework, the U.S. Department of Homeland Security (DHS), through its Bureau of Customs and Border Patrol (CBP), has introduced four main programs since 9/11: (1) the Customs-Trade Partnership Against Terrorism (C-TPAT), a voluntary program for shippers, freight forwarders and carriers involved with U.S. importation; (2) the Container Security Initiative (CSI), a port-centric, customs-to-customs program; (3) the Smart Box program promoting technology for securing containers; and (4) the Advanced Trade Data Initiative, requiring shippers to send CBP manifests in advance of shipment to the U.S. Together, the programs specify the collection of more information about supply chain partners and shipments; CBP's use of advanced analytical tools to identify potentially hazardous shipments and its use of noninvasive detection systems (e.g., X-ray and Gamma-ray) to inspect such shipments; and the development of new technology to track and seal cargo containers, and to detect intrusion or any dangerous materials within them.

The December eyefortransport conference largely centered on C-TPAT. Companies apply for C-TPAT certification by completing a standardized evaluation of their own supply chain security practices, as well as those of their suppliers. One of the required practices is securing cargo containers with C-TPAT-specified seals. Currently, these seals are mechanical, not the newer electronic seals. However, CBP encourages use of the latter and may require them in the future.

What Are the Incentives to Complying With C-TPAT?

Complying with C-TPAT necessitates the gathering of information worldwide, as well as process changes and occasional supplier changes, all of which can pose considerable expense. A recent study indicated that "Canadian carriers alone have spent $400 million," noted conference speaker Stephen Evans, vice president of loss control and regulatory compliance, for Alberta, Canada-based H&R Transport.

So, what are the incentives to participate? CBP has described at least four possibilities: fewer inspections of inbound cargo; "green lanes" to expedite handling of C-TPAT-compliant cargo at border crossings and ports; "restart priority" in the event of port closure due to disaster; and paperless information exchange. To date, the only incentive implemented has been reduced cargo inspections.

Without question, avoiding inspections would save most importers money. According to Container Security Inc., an exhibitor at the conference that makes RFID-based security and tracking systems for intermodal containers, one major U.S. retailer estimated that avoidance of a noninvasive inspection saved $300 in cost—that is, $300 in savings accrued from moving cargo faster through the port, and reduced time spent by the retailer's personnel or its appointed cargo handlers. Likewise, avoidance of an invasive inspection saved $1,000. The retailer stated that 20 percent of its containers were inspected.

But does C-TPAT compliance actually translate to reduced inspections? Some speakers from C-TPAT-certified companies confirmed that it had. Others remained unconvinced, though all agreed that, if widely available, green lanes would make a difference. However, green lanes have been implemented only at a few border crossings, and no ports. With border crossings and ports already severely congested, creating green lanes would require expensive infrastructure upgrades or ultra-creative ways to utilize existing infrastructure. A former DHS official told attendees, "Green lanes are like sex in my old high school—everybody talked about it, but no one knew how to do it!" A CBP speaker who followed confirmed not to look for green lanes anytime soon.

Congress may come to the rescue. Irv Varkonyi, president of Supply Chain Operations Preparedness Education (SCOPE)—who filled in for ailing conference chair, Michael Wolfe of North River Consulting—informed this author about the "Greenlane Maritime Cargo Security Act" introduced in November by Senators Patty Murray (D-Washington) and Susan Collins (R-Maine). "Congress knows that appropriations will be needed to support even a modest implementation of green lanes," he said. "It has to walk a fine line between promising things to industry that can't be paid for, and offering no meaningful incentives to compliance." He predicted passage "in some form" next spring.

Looking For Rewards From C-TPAT Compliance—But Not From CBP

Given the paucity of incentives offered by CBP, why would a company sign up for C-TPAT? Speakers from Procter & Gamble (P&G), Boeing, Starbucks, and Kmart emphasized that doing so makes good business sense. In addition to the "moral obligation" to secure cargo, they cited the need to "protect the brand." A terrorist incident, or product tampering causing harm to consumers, would have devastating consequences for globally recognized products.

Despite this, only about 4,000 of some 50,000 U.S. importers have applied to join C-TPAT. Not all companies have high-value products or brands, and many are small and reluctant to dedicate the necessary resources. This poses a risk. "The supply chains of noncompliant companies are especially vulnerable," observed Ray McGuire, former vice president of Saks Fifth Avenue and Kellwood.

Does Spending on Cargo Security Bring Supply Chain Efficiency?

Making the case for investment in cargo security would be considerably easier if it could be shown that the investment contributed to supply chain efficiency. Several speakers had already made that case, pointing to their companies' recent investments in cargo security and tracking technology. Representatives from P&G and Starbucks spoke about the synergy their companies had experienced in piloting electronically enabled cargo-tracking systems. Ron Miller, on the customs-compliance team at P&G (a company that mandates C-TPAT compliance by all its suppliers) noted: "RFID not only ensures chain of custody, but also reduces the need for handling. 'Touches' mean cost; our cost per case is driven by touches."

Starbucks has been utilizing "talking smart containers" to ensure the purity and freshness of "green" (unprocessed) coffee and tea used in its high-demand "holiday blends." Furthermore, a product exhibitor at the conference pointed to a recent survey of the top 100 U.S. importing and exporting companies indicating that supply chain efficiencies gained from automatically tracking containers—reducing inventories and out-of-stocks, minimizing lead-time variance and increasing manufacturing uptime—were estimated to save $1,150 per container.

Carriers at the conference, however, emphasized the need for technology developers to distinguish between cargo security requirements and the supply chain management goals of protecting and efficiently utilizing assets. One individual referred to the World Shipping Council's work in defining these divergent needs. In a 2004 advisory paper, the council emphasized: "E-seals, designed to discourage unauthorized entry into a container, must be 'read-only and not reusable.' The security vulnerabilities would increase significantly . . . if, as some have suggested, the e-seal were to also have the capability to upload and store supply chain management data such as cargo manifest and other consignment-related documentation."

The council went on to explain: "E-seals, like manual seals, will be frequently broken in transit for legitimate reasons, typically by foreign customs officials, to allow access to the container and its contents. Adding a 'write' capability to an e-seal—which would be necessary to re-seal a reusable e-seal after opening—would create, rather than reduce, security vulnerabilities, e.g., security credentialing of all persons with 'write' capability, the impossibility of monitoring whether unauthorized persons obtained the write capability, and potential manipulation or alteration of the data already entered into the device, as well as other cyber security-related vulnerabilities. In addition, it would significantly increase cost, with no identified security enhancement benefit."

Global Standards Critical to Container Security Technology Adoption

The WCO has endorsed a set of specifications for mechanical seals developed by the International Organization for

Standardization (ISO), ISO Publicly Available Specification (PAS) 17712. Though not yet ratified, ISO PAS 17712 has effectively become a standard. Consistent with WCO, CBP has made the use of ISO PAS 17712-conformant seals a requirement for C-TPAT certification.

Although e-seals are not yet required, some companies are using them. Recently a group of high-profile companies, including Boeing, conducted e-seal trials at the request of CBP. Ken Konigsmark, C-TPAT program manager at Boeing, told attendees that his company had tested two different e-seals on marine cargo: "a 'homegrown device' and GE Security's CommerceGuard product." He indicated that CBP would be releasing the results of this and other trials in the first quarter of 2006.

E-seals clearly have numerous advantages over mechanical seals. They can be used to identify containers and report intrusions automatically, while mechanical devices cannot. Furthermore, e-seals can be connected to sensors that detect movement, intrusion through any of the six container sides, and radioactive, biological and chemical hazards.

International e-seal standards have not yet been issued, however, with several ramifications: First, no uniform frequency for e-seals has been adopted across all countries. "The WCO needs to harmonize," said McGuire. Second, the interoperability of different vendors' products is not assured. Finally, most terminals at ports and other facilities where containers are handled have not had the financial justification to deploy readers and related infrastructure.

As a result, no e-seal product can be used worldwide. "To make large investments in e-seals and supporting technology today would not pay," stated several speakers. Furthermore, with no worldwide consensus on functionality, "some container security vendors are hedging their bets by morphing disparate technologies into 'Swiss Army knife' solutions that are not practical or cost-effective," noted Randy Mullett, vice president of government relations for supply chain solution provider CNF.

ISO's E-Seal Standard Not Imminent

ISO has been working for six years on a standard for electronic freight container seals, ISO 18185. It falls under the ISO 18000 standards, "RFID for Item Management." ISO 18185 will likely conform to ISO PAS 17712, the standard for mechanical seals, but will electronically evidence tampering or intrusion through the container doors. It is read-only and includes both passive and active protocols to support a range of costs and capabilities. The passive protocol will probably use the 862 to 928 MHz frequency range. The 433 MHz frequency, long used by the U.S. Department of Defense for container tracking, has been proposed for the active protocol. However, the U.S. and most other countries outside Europe have not yet approved the allocation of 433 MHz for freight containers.

While significant progress was made in 2005, the release of ISO 18185 is not yet imminent. Some relative newcomers to ISO Technical Committee 104 ("TC 104")—the group responsible for freight container technology standards—have questioned a number of provisions in the standard, including the lack of support for data security (encryption) and data integrity. Testing has been extended to address those concerns.

An ISO standard for automatic freight container identification (for tracking) already exists. Developed in the early 1990s, ISO 10374 uses passive, read-only, dual-frequency RFID (850-950 MHz and 2.4-2.5 GHz). Although container tracking does contribute to container security, this is not a container seal standard and has not been recommended for use by the WCO or the CBP. Today, only a fraction of the world's containers carry ISO 10374-conformant tags. ISO is revising the standard in response to demand for an RFID tag that would survive the life of the container without maintenance. Also in progress is ISO 17363, a rewritable RFID container tag standard for use by shippers and consignees in supply chain applications.

When the ISO 18185 E-Seal Standard is Released, Will Containers Be Secure?

Conferees acknowledged that having this standard will be a good first step, but that much more remains to be done. First, ports and other cargo handling facilities need to invest in readers and the supporting infrastructure. Interoperability testing, funding and the politics that will accompany these public agency purchases could draw

the process out for the remainder of the decade—or longer.

Second, even if ISO 18185 provides encryption and data integrity (a matter not yet resolved), additional technology and standards development will be needed. E-seals can detect unauthorized entry through the doors, but not the result. By the same token, they can't detect breaches of the container walls. Furthermore, the particular container-tracking data to be reported, and to whom (e.g., government agencies like DHS would like to receive data), must be defined, and the reporting systems paid for.

Finally, container technology is just one of the means necessary to improve cargo security. Equally (or perhaps more) important is the collection of foreign commercial intelligence. "What works," said speaker Sandra Scott, director of international relations for transportation service provider YRC Worldwide (formerly Yellow Roadway), "is gap analysis."

DHS Providing Seed Money For New Container-Technology Development

DHS has initiated several programs to spur the development of cutting-edge container security technology and analytical tools. Several of these programs feature multiphase vendor competitions. One program is the "Advanced Container Security Device," focusing on the detection and reporting of "six-wall intrusion" and dangerous materials. Another, the "Future Smart Container," includes the Marine Asset Tag Tracking System (MATTS) to facilitate universal tracking by finding clear signal paths between containers that are typically stacked tightly together, and satellites for positioning and communications. The "Secure Carton Initiative" aims at monitoring boxes within crates through intermodal transfers.

Responding to market need or DHS incentives, a host of large and small companies have developed electronic products designed variously to lock, track, monitor the contents of, report on and manage containers. At the December eyefortransport conference, four U.S. companies exhibited such products: Container Security Inc., iControl Inc., Sciguard and Safefreight Technology.

More Regulation on the Horizon?

With so many U.S. importers declining to participate in C-TPAT, and the slow pace of container seal and tracking technology standards development, uniform protection of U.S.-bound cargo would seem to be many years away. This, however, could change. "Watch for [CBP] mandates," noted Doug Doan, former business liaison for border and transportation security at DHS. The prospect of mandates is, no doubt, why many container technology vendors are hanging in.

Regulation is Useless Without Enforcement

"Trust, but verify" is a byword at CBP. Conferees agreed that the U.S. government must spend the resources to verify that C-TPAT applicants are actually using the procedures and technology they say they're using. Even after C-TPAT certification, however, some companies, eager to reduce cost, dispense with rigor—and human nature is to seek the most expedient path. "Seals are sometimes given to drivers to affix to containers after they are loaded," remarked one attendee. CBP says it is committed to "revalidating" C-TPAT-certified companies, but has not yet begun doing so.

A roundtable of attendees agreed that, in addition to more public sector investment in enforcement, both the public and private sectors must invest in additional training in order for cargo security technology and policies to deliver results. Even the best-designed e-seals cannot function well unless transportation and logistics personnel are trained to use them. "Installers and inspectors must get hands-on practice testing for likely attack scenarios," observed one member.

And what if disaster is not averted? The final, but best, session at the conference highlighted the critical need for more and better training of public and private sector personnel in managing disasters. The session featured the demonstration of an innovative new crisis simulation product from Crisis Simulations International (CSI). The demonstration was based on a simulation developed by CSI for the city of Portland, Oregon, designed for city leaders to practice managing a crisis involving terrorist attacks on the city's transportation infrastructure. Two

conference attendees acted as mayor and chief of police in coordinating the city's response to a vividly portrayed bridge bombing. The audience, which could see each person's decisions on a large screen, was riveted.

"Typical crisis training exercises in companies and governments require the memorization of a series of steps appropriate to each person's role, and minimal interaction with others in a rapidly changing environment—'If this happens, do that,'" noted Chris Hatzi, senior director at CSI. "They do not sufficiently take into account the surprises that result from the decisions of others. Our simulations, which utilize our patent-pending DXMA, allow for unanticipated outcomes which better represent the kind of real-world chaos that senior leaders must respond to in real time."

Cargo Security is a Collective Obligation

Eyefortransport's North American Cargo Security 2005 Forum evidenced no clear consensus on how much investment would "sufficiently" protect cargo. However, all concurred that much more needs to be done—and that the U.S. government must play a central role. "Shippers and logistics companies are willing to assume their fair share of responsibility," observed YRC's Scott, "but the fact is that the cargo security challenge is enormous. In the increasingly competitive and congested international shipping environment, more government assistance with priorities and cost sharing is key."

*Leslie Downey is a principal and founder of **RFID Revolution**, a Washington, D.C., firm providing RFID marketplace consulting services to RFID vendors and end users. She can be reached at 301-589-9791 or **LDowney@rfidrevolution.com**.*

| Back to normal page view | Send this article to a friend |