Cargo Container Security Navigates the High Seas

Adoption rates for electronic systems aren't as fast as many expected -- and here's why

Crest Electronics:
SIW's CCTV Section Sponsor
The Latest from SIW

Tyco International Announces Acquisition of Trident Tek, Inc. Deal will strengthen its American Dynamics PortfolioNavigating Network Video Recording TopographiesWhile NVR systems offer a number of benefits, decentralized network storage can help integrators & end users achieve goals The Security Week That Was: 11/09/2007Threat to Malls DownplayedTAC Americas Veteran Steps Aboard as Pelco COOTamron USA Names New G.M., Reexamines CCTV Optics Market

Geoff Kohl, editor
SecurityInfoWatch.com

A week ago at a GE Security press conference held during the 2007 ASIS International Seminars and Exhibits, GE Security's Vice President and General Manager for Americas Commercial Greg Burge, explained why an initiative to enable the cargo container industry with electronic security devices hadn't been as spectacular as GE and many port security experts had believed it might be. "The fact is there is lots of legislation that is still in the works, and everyone is concerned about the standards that this legislation could bring," said Burge. "They're scared that if they invest in a technology before the standards are completed, then what they invested in might not meet the standards." GE Security, which was one of the early vendors of a cargo container security device, has reason to be concerned. The Safe Port Act of 2006, was a piece of legislation that had been reappearing in Congress for years without much success until it was passed and signed into law by George Bush in 2006. While the bill doesn't specifically set technology standards, it's clear within the industry that standardizing of container security technologies is a sticking point and possibly on the horizon.

It's no wonder that there is an issue in technology; this is an industry which has traditionally used basic mechanical seals which simply ensured that if the seal wasn't broken, then the doors had not been opened. Those simple mechanical seals weren't fully effective, as many shippers learned that organized crime was sometimes even going to such extremes as removing the heavy steel doors as a pair from their hinges so that the seal never was broken. It was a classic case of criminals beating out low-tech security, since those seals only tell the shipper that the doors hadn't been swung away from each other. Then came newer technologies from vendors steeped in electronic security systems for businesses and commercial assets. Generally, these were intrusion alarms that could notify an integrated security system either via RFID scanning, or by radio/cellular or even by satellite.

Still other systems looked at GPS tracking of containers on top of intrusion detection to give shippers and shipping agents a real-time operational view of the containers as well as the security status. The problem, of course, was that maritime and port environments aren't exactly technology friendly, with moisture and corrosion almost always the first two ingredients for technology failure in maritime environments. Additionally, signaling is challenged by the massive nature of some container yards and by the difficulty in signaling when containers are buried in stacks. The industry has often focused on the choke-point model for scanning and retrieving RFID-transmitted data stored in the electronic devices, but detractors of that model argue that it doesn't tell you about a breach until it's too late and the cargo is gone or the bomb is already in there.

But, according to Luke Ritter, author of the book "Securing Global Transportation Networks," CEO of Trident Global Partners and principal on global security for Tom Ridge's new consulting firm Ridge Global, the acceptance of such electronic security technologies isn't just about whether there are standards or not. For Ritter, the issue of acceptance of the electronic container security devices gets down to cultural challenges.

"Transportation is still a labor-intensive business," explains Ritter. "The first reaction to problem solving in this in-

dustry can be to throw more people at the problem versus reaching for technology solutions." Even more challenging, adds Ritter, is that when the industry adopts technology, it often doesn't do so as an early adopter.

"Finally," says Ritter, "the complicated and critically important cost/benefit justification associated with an investment in cargo container screening devices is still being developed."

Jim Giermanski, Ph.D., professor and director of International Business Studies at Belmont Abbey College and a former Regents Professor at Texas A&M International University, agrees that money is the big hold-up for the industry.

"The private sector is not going to invest in anything until it sees a return," says Giermanski, "and the government is not providing incentives." He points out that the Safe Port Act of 2006 provided for so-called "green lanes" to speed up container processing for companies that met C-TPAT requirements and the requirements of the Container Security Initiative that were outlined in that Act. The problem is, says Giermanski, "green lanes at seaports still do not exist."

"Look at the 100 percent scanning requirement or the new RFIs coming out of DHS," adds Giermanski. "The government really doesn't know what we mean by smart container and what it can do."

If Giermanski is correct, then the only hope for better use of relevant technologies to protect our supply chains is going to have to come from within the private industry. Ritter thinks that's where it has to be driven, but he also believes the solutions have to be positioned as not simply another security alarm, but as an end-to-end supply chain security solution.

"Some of these devices have the potential to provide additional visibility in the supply chain, particularly for goods in transit," says Ritter, "and visibility is one of those critically important issues in global trade where business process improvement and enhanced security/resiliency can intersect to create real return on investment."

That bottom line advantage is what will drive these technology offerings, but ROI and bottom-line advantages aren't as easy to spell out as they seem at first. However, Giermanski -- who is a big advocate of satellite-enabled smart container communications -- says that the technologies can prove themselves without the supply chain or security executive trying to divine ROI numbers. He cites a trial of a GPS-based solution where criminals were actually apprehended during the test breaking into one of the containers. On the same trial, the shippers lost one of the cargo containers, and the satellite system was able to locate it.

And while neither Ritter nor Giermanski could point to a specific cost point where container security devices would prove their value unequivocally, Ritter says that "there is a per unit price point that justifies (or nullifies) most return on investment calculations in business, and cargo security is no exception."

Therefore, if businesses can define that value, the adoption of these technologies will happen - with or without any standards defined by DHS or the European Union.

Giermanski, however, is not so optimistic about near-term adoption of container security devices.
"It's a combination of a private sector that doesn't see the benefits," laments Giermanski, "and the government that doesn't know how to show the private sector the benefits."

Fortunately, the market isn't altogether afraid of the conditions. As GE's Greg Burge noted in their ASIS press conference, there may be difficulties and challenges in the cargo container security market, but there's still business to be done.

Article from: SecurityInfoWatch.com