

**at a glance**

This article looks at industry efforts to improve maritime security through technology.



# Failure

## *is not an option*

As the scope of regulations widens, it's still unclear exactly who will be paying for heightened maritime security

by Perry A. Trunick

We have no accurate estimate of the cost of maritime security, but we know the price of failure is unacceptable.

If you could sum up the comments of maritime industry executives, security professionals, logistics experts and others, that's about as close as you can get to a price tag for [security initiatives that continue to evolve](#) in the maritime sector. This is despite the fact that last month President Bush signed the \$28.9 billion **Homeland Security Appropriations Act** (for fiscal year 2005). The funding legislation includes nearly \$420 million for border and port security activities.

"The U.S. *Coast Guard* has estimated necessary security improvements will cost over \$1.1 billion just this year alone," says Jay Grant, director of the *Port Security Council of America*. The newly formed group further estimates the port industry will require \$7.4 billion over the next decade just to comply with mandates contained in the **Maritime Transportation Security Act**, which went into effect in July 2003.

That's on the port and infrastructure side. Dawn Russell, a professor of supply chain management at *Pennsylvania State University*, reviewed a number of sources and came up with a further cost to the U.S.

economy of \$151 billion per year. Those costs include logistical changes in the supply chain, new costs related to workplace security, information technology security, contingency operations, employee travel, insurance and liability, etc. Furthermore, an estimate in the 2003 *State of Logistics Report* indicates that businesses might end up carrying as much as 5% more safety stock to buffer against delays, representing a \$75 billion increase in working capital.

The U.S. isn't alone in calling for heightened security on the seas. The *International Maritime Organization* (IMO), made up of 164 countries, has

adopted the **International Ship and Port Facility Security Code (ISPS)**, which contains detailed security-related requirements for governments, port authorities and shipping companies. The IMO has called for member governments to put into effect the legislative, administrative and operational provisions needed to give effect to the ISPS.

“The whole idea of the ISPS Code is to reduce the vulnerability of the industry to attack, thus countering the threat and reducing the risk,” the IMO states.

The ISPS requires ship, port and terminal operators to develop detailed security plans. It also requires that a shipboard security alert system be installed on every ship over 500 gross tons.

There’s a direct benefit to the industry that has nothing to do with terrorism, says David Menachof, a professor at London-based *City University Business School*. It’s not something that you hear much about, but [pirates operate in some trade lanes](#), he notes. They’ll board a ship and hold the crew hostage for ransom. Though they do not pose a threat from the standpoint of either theft or terrorism, they add risk and delay.

Global asset control tracking and monitoring systems have helped ocean carriers with fleet management, but they have also been applied to containers, rail cars and trucks, notes Brent Winsor, marketing manager for *SkyWave Mobile Communications*. SkyWave claims an installed base of 33,000 terminals, which include an antenna, satellite transceiver, global positioning system (GPS) and control capability. These systems are the underlying communications technology supporting a number of applications as disparate as vessel monitoring, tuna buoys and the Phase 2 demonstration project for **Operation Safe Commerce** (see below).

*Pole Star Space Applications Ltd.* uses the SkyWave technology to provide a web-based ship tracking product for 600 clients. In 1998, Pole Star was working with *Sea-Land* (now part of *Maersk*) to use satellite technology for container tracking, says Julian Longson, vice president of development. “It proved to be a [very hard nut to crack](#), technically,” he says. The issues were the size of the equipment and the power requirement.

“Those elements are still a very problematic area in terms of tracking individual containers via satellite technology,” continues Longson. So, Sea-Land began tracking the ships, reasoning that if it knew which containers were aboard, it would have de facto container tracking at sea. The business case at that time was to track containers to provide better customer service to shippers and forwarders.

That thinking has changed. The security alert system mandated by law allows a ship captain or security officer to activate a covert panic alarm which signals a flag administration such as the U.S. Coast Guard. Pole Star is working with container seal manufacturers to expand that concept to provide an alert if a container is opened, closed, or otherwise tampered with at sea.

Additional input terminals on the satellite communications units allow a variety of sensors to be used. Parameters such as temperature or carbon dioxide levels can be monitored and reported when threshold levels are exceeded. (Carbon dioxide

sensors are used at the French entrance to the Euro-Tunnel and other border crossings to detect human stowaways in containers.)

To overcome some of the limitations imposed by the power requirement, the satellite communications units can be set up to communicate with readers positioned inside the hold of a ship and at the end of each gantry. The readers can communicate wirelessly with electronic cargo seals that include **radio frequency identification (RFID)** technology. This allows a unit with visibility to a satellite to communicate with a number of containers and issue alerts as needed.

**Operation Safe Commerce** is a demonstration project that started before the September 11 terrorist attacks. A goal of the project — now in its second phase — is to use currently available and affordable technologies to secure an entire supply chain.

The first phase involved lighting manufacturer *Osram Sylvania*’s supply chain from Eastern Europe to the U.S. In Phase 2, the U.S. government asked to expand the scope and increase the scale using multiple, realistic supply chains, says Iraj Tavacoli-Shiraji, chief technology officer for *Innolog*, a participant in two of the demonstrations. At press time, the final shipments were being delivered and the review of the projects was underway.

Seventeen primary supply chains were selected at three load points: Seattle-Tacoma, Los Angeles-Long Beach and New York-New Jersey. The purpose of the project is not to show the government a lot of gadgets to impress them, explains Tavacoli-Shiraji, but rather to develop end-to-end solutions with existing technologies — including policies, procedures and assessments. So, Operation Safe Commerce is designed not only as a technology demonstration but a means to apply current tools, and uncover, assess and address gaps and vulnerabilities in the supply chain.

“We started with an assessment that included visiting every component of the supply chain,” says Tavacoli-Shiraji. “We took them through a very detailed assessment looking at physical security, the personnel and the processes they had in place.”

The next step was to identify, rank and quantify security issues before deciding on a solution.

“A consortium of technology providers put a solution together that fit the requirements of the assessment and the vulnerabilities we had identified,” notes Tavacoli-Shiraji. That solution included active and passive RFID tags and satellite mobile tracking through the intermodal supply chain — truck, rail and ocean. Passive RFID tags and readers met established Class 0 electronic product code (EPC) guidelines.

At the center of the solution, says Tavacoli-Shiraji, was a data fusion center. The technology components installed along the entire supply chain provided real-time status on the subject containers from origin to destination.

Innolog also worked with 60 to 70 textile/garment suppliers in mainland China. Cargo was screened and consolidated at the port of Hong Kong, including radiation scans. Data on the shipments were relayed real-time to the data center.

Security assessments included the warehouse and personnel in Hong Kong to ensure that each shipment that arrived was properly identified, stored, managed and monitored before consolidation and loading. RFID tags provided real-time input of what was being loaded into the containers, and this was matched to the unloading detail at destination to ensure that what was unloaded in the U.S. was the same as what got loaded in China.

[Real-time tracking of the moving asset](#) was a critical element of the demonstration, says Tavacoli-Shiraji. The SkyWave satellite communications terminals were connected to intrusion alert devices, providing full visibility of what was happening to the containers enroute. Reporting cycles for the tracking system varied based on risk. During more vulnerable legs of the journey, reporting was constant. On lower-risk segments, reporting could be every few minutes or even every half hour.

Any intrusion alert would have triggered an immediate message. In fact, when a container was opened at the U.S. port for inspection, the data center received an alert. Operators were able to determine immediately that the location and timing coincided with the expected customs clearance.

One very important point made by the participants in this demonstration project is that [shipments aren’t automatically safe once they are at sea](#). In fact, the days a container spends on the water provide ample opportunity for undetected intruders either to steal cargo or to conceal contraband in the container. This equates to a compelling argument for the ISPS and Operation Safe Commerce initiatives which are aimed at securing the vessel during this vulnerable period as well as the other efforts of the **Container Security Initiative** and **Customs-Trade Partnership Against Terrorism (C-TPAT)** to screen and secure other elements of the supply chain.

Solutions to maritime security range beyond technology, but technology is a key element in securing extended supply chains. Though the technology to accomplish this exists, the barrier to entry is the massive infrastructure in terms of the volume of containers, numbers of ships and portside facilities, says PoleStar’s Longson. “There are so many stakeholders,” he notes, “but no single stakeholder is willing to fund the whole thing.”

What could develop is a system where the technology companies and container owners and lessors charge a service fee for container tracking. But even with that as a model to cover the cost of implementation, the real driver is likely to be more widespread regulatory requirements, like the ISPS. At this point, only the U.S. appears to be pushing hard on security initiatives. **LT**

Copyright © 2004 by Penton Media, Inc.

