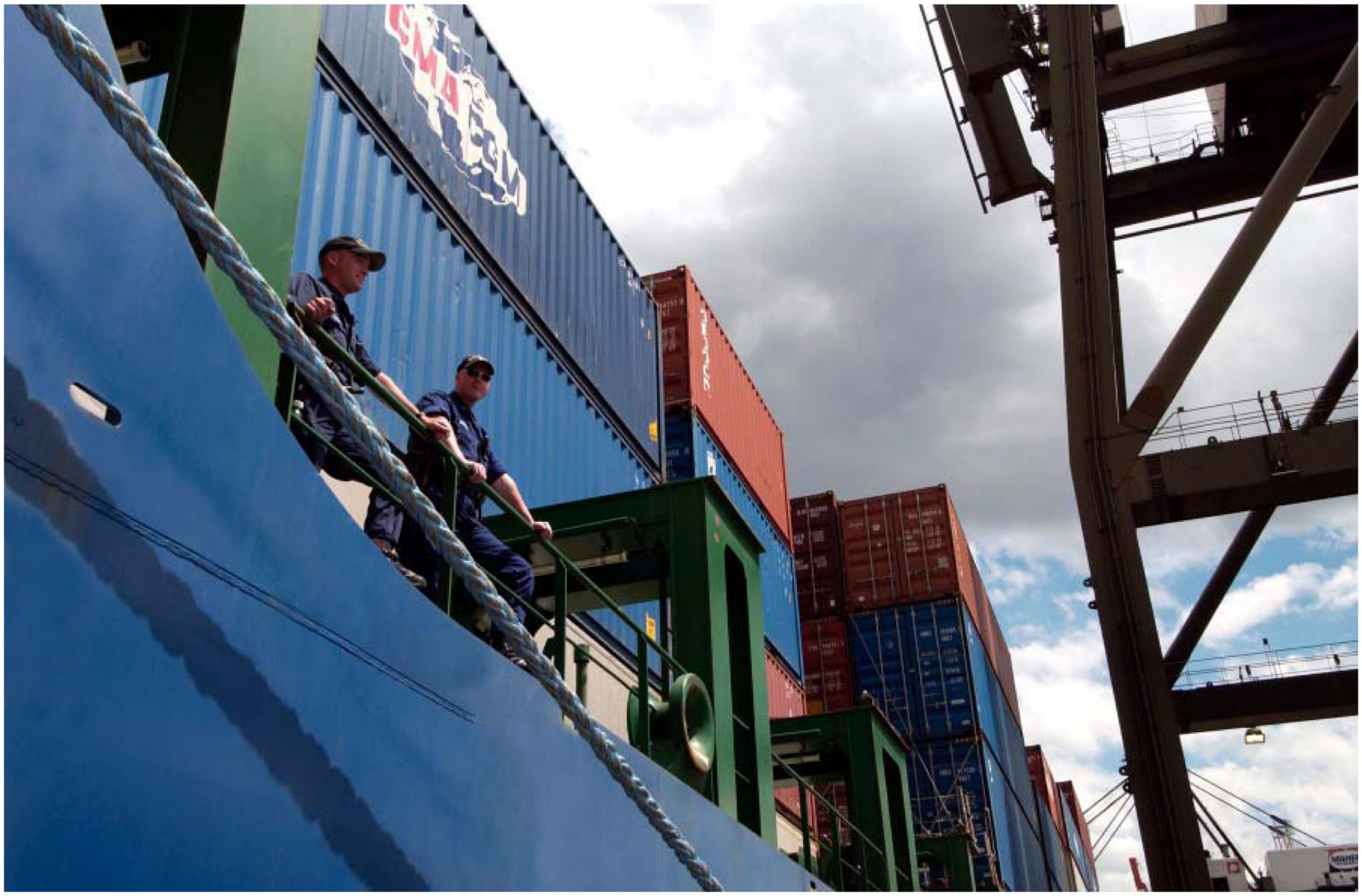
Visibility and the Role of Government in Container Security

David Jacoby, Boston Logistics Group



The problem is still there

A shipper called me this week asking if I could help locate a stolen container that went the wrong direction somewhere in Egypt. The Director of Logistics was very concerned, partly because this was the third container of hers that met this fate recently.

It's not that the theft was bad - the container was carrying T-shirts for pregnant women - how valuable could that be? It's not even that individual containers could be carrying bombs (they could). The greatest concern is that lapses of security can be exploited in a more complex and nefarious plot.

Containers can be used in money laundering schemes. In one case, thousands of units were diverted to a fictitious destination, and by the time the police showed up it was too late to do anything.

Containers can also be part of schemes to dis-assemble and re-assemble components of prohibited and dangerous cargoes. A recent test of security at American airports found that while pretend terrorists were prevented from carrying prohibited devices through security, they managed to dis-assemble contraband articles and re-assemble them on the other side, all within the airport walls. Security recently stopped me in Amsterdam because they thought I might have been used as a pawn in a plot like that.

Terrorists could inflict a heavy penalty on economic growth simply by threatening to plant bombs in containers. The additional screening and inspection that would take place as a result of such as threat would create backups and delays at key choke points in the global transportation network.

But the pain has faded

So container security is important, but it's difficult to make the case for action in the absence of pain.

The practitioners and academics writing about container security are not making a dent in the problem. The theory of risk mitigation is simply not compelling to the individual supply chain practitioner, or even the individual large company. The problem is not that the books are boring. Some of them are very sterile in tone and actuarial in their approach to addressing the problem.

The problem is that the risk of danger to others is more significant than the danger to oneself, which makes security a difficult "sell" to any individual. Security falls mostly in the area that economists call "externalities" - events that affect the public, but which require far too much investment for any individual company to concern itself with. This is the origin of regulation in areas like environmental waste and pollution (double-hulled tankers, for example), noise pollution (night flight restrictions in populous areas), vehicle accidents (mandatory auto insurance), and public health risks (quarantine for SARS victims, for example).

Experience has a half-life. Recent victims of theft have alarms installed, but then forget about the danger over time. We don't like to admit it, but the same thing is true with airport security following 9/11. Security at Logan airport in Boston is lax, and dockworkers across America have barely implemented the Smart ID card, a most basic foundation for security.

Private companies are implementing visibility solutions in a slow and methodical way, but if governments want to accelerate visibility to cargo flows, they may want to consider offering tax breaks for investment in visibility solutions that enhance security.

Building an information shield

How do you develop an invisible fence that won't bother people and doesn't cost too much?

The key is in leveraging information. The solutions are in both the governments' hands and in the private sector's hands.

The governments and related transportation security authorities control programs such as (at least in the US) the Container Security Initiative, Customs-Trade Partnership Against Terrorism (CT-PAT), Advanced Customs Declaration (ACD), Transportation Workers Identification Card (TWIC), and electronic collaboration amongst ports (e-Ports).

Private carriers and intermediaries can implement visibility improvement technologies such as radio frequency identification (RFID), yard management, load planning, and e-Collaboration between trading partners.

Paying the bill

Private companies are implementing visibility solutions in a slow and methodical way, but if governments want to accelerate visibility to cargo flows, they may want to consider offering tax breaks for investment in visibility solutions that enhance security. Examples of such technologies are: active RFID systems for high-risk cargo types and traffic lanes; optical scanning and license plate recognition; and container yard webcams. This still would not eliminate the need to police the ports that everybody knows are dark and dangerous, but it would be a step in the right direction. D

David Jacoby is President of Boston Logistics, a global supply chain economics consulting firm. He can be reached at djacoby@bostonlogistics.com