



# supply chain strategy

## Look Beyond Compliance for Supply Chain Threats

A mandate to scan all import containers might give you a read on where supply chain security is heading

**A**S THE THREAT OF TERRORIST ATTACKS has gone up in recent years, so has supply chain security become elevated on corporate to-do lists. But much of this effort is driven by expedience—the need to avoid supply delays by complying with new security requirements—rather than a fundamental rethinking of security as a strategic objective.

Legislation signed by President Bush this August could provide a wake-up call to companies that securing supply chains means more than short-term tactical gain. The mandate requires all maritime cargo containers to undergo security scanning at foreign ports before entering the United States. As yet, the measure may only represent a faint trace on your radar screen, but the debate it has provoked highlights the broader supply chain implications of a changing security regime.

### Widespread Doubts

The 9/11 Commission Recommendations Act requires 100% scanning of imported maritime freight containers before they are shipped from a foreign port to the United States. The most obvious risk presented by the mandate is that it will slow the flow of the six million or so containers that enter the country annually, disrupting international supply chains and ultimately damaging economic performance.

Comprehensive scanning operations will impede cargo flows, particularly in large facilities that are served by multiple feeder ports, believes Dan Purtell, president, supply chain security services, First Advantage Corp. “Just the logistics of setting up multiple scanners in ports, especially megaports, will slow the exporting process down,” he said.

In addition, many security experts worry that such a draconian measure is not the best use of anti-terrorism resources. “Someone has to look at the scanner data,” pointed out Jim Rice, director of the MIT Integrated Supply Chain Management Program, at MIT’s Center for Transportation & Logistics, Cambridge, MA. That’s a tough challenge, given the sheer number of images that will have to be processed. “People are talking about 100% scanning but not 100% analysis,” Rice added.

An overarching issue is whether concentrating so many resources on inspecting cargo coming into the country via well-known ocean routes is misguided. Rice argued that a terrorist, whose overriding aim is to smuggle a weapon into the country with maximum chances of success, may find the relatively porous northern border with Canada a better point of entry. “If our back door is open, why would anyone want to go through the front door?” he said.

Many experts advocate a layered approach to security that relies on a number of strands, including established programs such as Customs Trade Partnership Against Terrorism (C-TPAT), existing requirements including advance manifest reporting, and scanning. “No one layer is foolproof; it is the combination that makes it less likely that something bad will happen,” said Bill Tenney, group manager, International Assets Protection, at retailer Target.

But another fear is that 100% scanning will deter companies from investing in these other security measures on the assumption that the U.S. government’s scanning efforts are sufficient.

### Spread the Risk

“Can we get to a point where we are talking about risk-based scanning?” asked Tenney. Under this system, there is a risk component and a vulnerability component. Countries such as Pakistan and Indonesia would be relatively high on the risk scale. China would be rated less risky but score very highly on vulnerability since shutting down supply lines from that country would cause major business upheavals. The level of scanning would vary according to these factors.

In principle, the concept of scanning at foreign ports does

#### [Key Takeaways]

- » Companies need to cast supply chain security in a much broader light than simply a way to comply with the latest trade regulations.
- » A recent mandate that requires all import freight containers to be scanned is a good indication of how the security landscape is changing and the strategic implications for supply chain management.

offer important advantages since these facilities are a “natural chokepoint” at which security efforts can be focused, believes Tenney. Also, such an approach “begins to address the central question of what’s in the box—or more importantly, what’s not in the box,” he said.

## Planning Ahead

The mandate brings home how difficult it is for supply chain managers to plan for such measures given the many doubts over the future direction of security policy. Moreover, it comes at a time of general uncertainty in the trade arena. Recent quality problems associated with products from China, a backlash against globalization, and the vagaries of a forthcoming presidential election year during which security will be a hot-button issue compound the uncertainty. In combination, these developments may even give senior executives pause for thought when contemplating expanding overseas.

“I don’t think supply chain strategies will suddenly change, but companies might start thinking about revisiting their strategies given these problems,” said Rice. CEOs should be asking for assessments that look three to five years out, he maintained. One approach is to look at different trade scenarios such as what will happen if only 100% scanning is imposed or if there is full scanning plus improved product reliability out of China, he suggested.

The ways in which companies counter security-related disruptions, such as slower goods flows and maintaining higher inventory levels, may be unpalatable but necessary. Companies may need more working capital to support higher inventory levels over longer periods, adversely affecting the availability of time-sensitive goods such as fashion items.

Providing such assessments “is a conundrum,” acknowledged Tenney, one reason why Target, in collaboration with CTL, has developed a security model for supply chain risk management (see *Supply Chain Strategy*, June/July 2007). The model positions security as central to protecting a firm’s economic viability and helps companies assess where their supply chains fall on the security scale.

On the tactical side, supply chain managers have a number of options at their disposal to reinforce supply lines against the bad guys. “Cargo is at greatest risk between the manufacturer, container stuffing location, and the port, so it’s critical to understand who you are doing business with,”

said Purtell. Of particular concern is that C-TPAT member companies should focus on the dynamics of the supply chain prior to stuffing, the country of origin, and whether or not their suppliers comply with security criteria outlined in the C-TPAT program. As he pointed out, a small supplier in a high-risk country such as Indonesia can represent the lion’s share of risk that a company faces. Mitigating that risk involves actions such as making sure that the supplier complies with relevant security mandates such as C-TPAT. “We are finding that corporations that vet business partners/suppliers are probably only at a 10% C-TPAT compliance rate at best,” he said.

Companies such as Intel are drawing on their experience of protecting extremely valuable cargo from theft. “Contingency planning is essential, irrespective of the event that causes the disruption,” advised Steve Lund, director of security, Intel, because snafus inevitably crop up when moving goods internationally. “And you should be pulsing those contingencies on a continuous basis,” he said, since even best-laid supply chain plans are still likely to go awry.

Scanning is a welcome added layer of security, but not a silver bullet, stressed Lund. “Solid intelligence is critical to an effective prevention capability; you have to know what’s going on out there to target and intercept shipments where necessary.” Mandated scanning does not guarantee that companies will conduct that activity with appropriate due diligence or allocate their resources appropriately.

## More Heat Than Light

Perhaps the trickiest variable to account for is the political one. Securing the supply chains that support the U.S. economy is an emotive issue that lends itself to communication by sound bite—particularly when politicians who do not understand the complexities of global trade are looking for quick-fix solutions. Scanning every freight container that enters the country is a clear, simple solution that appeals to an uninformed public. That puts the onus on the industry to fill the information gap.

“Get involved,” advised Earl Agron, vice president of security for ocean carrier APL. The general drift of supply chain security legislation is to encourage more collaboration between the public and private sectors. But professionals should present a common face through trade and industry associations if they are to have a good chance of influencing the future direction of security measures, recommended Agron. ♦

This article was originally published in IOMA’s monthly newsletter, *MIT Supply Chain Strategy*, and is republished here with the express written permission of IOMA. © 2007. Further use of, electronic distribution or reproduction of this material, unless specified in a copyright agreement, requires the permission of IOMA. For more information about IOMA or to subscribe to any IOMA publication, go to [www.ioma.com](http://www.ioma.com). For information about copyright permissions or any other form of content license, please call Jonathan Wentworth Ping at 6212-576-8741, or email: [jpings@ioma.com](mailto:jpings@ioma.com).