

June  
July  
2003

the  
**NET  
BEST  
THING**

iSource  
BUSINESS

As Seen In

**iSource**  
Intelligent Solutions for the Enabled Supply and Demand Chain **BUSINESS**

# Building the Secure Supply Chain

BY ANDREW K. REESE

The threats may be new, but the tools and processes for ensuring your company's supply chain is secure are the same solutions you have been using to keep your goods moving efficiently through the chain.

Supply chain security is nothing new for The Neiman Marcus Group, Inc. (NMG), according to Jimmy Howell, the [www.neimanmarcus.com](http://www.neimanmarcus.com) company's vice president of transportation and logistics. "As an importer and retailer of high-end, luxury goods, NMG has always focused on the security of our merchandise as it moves through our supply chain," Howell explains. But now, facing a new set of threats not only to the company itself but to society at large, Neiman Marcus and other major U.S. importers are finding that the tools and processes they used in the past to keep their goods secure are also helping them deal with the realities of the post-9/11 supply chain.

## A Monumental Challenge

To get an idea of the scope of the supply chain security challenge for a nation as tied to imports as the United States, consider a few statistics from the U.S. Bureau of Customs and [www.customs.gov](http://www.customs.gov) Border Protection (CBP): more than 48 million full cargo containers

move between major seaports around the world each year, and more than 6 million of those containers arrive in U.S. ports by ship, comprising nearly half of the total value of goods imported into the country. That doesn't count the more than 11 million trucks and 2 million rail cars that arrive in the country each year, which bring in approximately another 10 million containers. In all, more than \$1 trillion worth of goods flow into the country annually.

Physically inspecting every single container entering the country would be a monumental task. As Michael Laden, president of Target Customs Brokers, a subsidiary of retailer Target [www.target.com](http://www.target.com) Corp., noted in testimony before Congress in December 2001, "Given the technology and resources available today, it is impractical and impossible to search or examine 100 percent" of the cargo coming into the country. In fact, the International Mass Retail Association and the West Coast Waterfront Coalition, in a joint statement to Congress for a hearing on container security in March 2002, estimated

that inspecting just 10 percent of the total number of containers entering U.S. ports on an annual basis not only would require hundreds of millions of dollars in additional funding but also would take 37 years.

On the other hand, the risks of not improving the physical security of importers' supply chains are clearly too high to ignore. The greatest menace is that a "dirty bomb," a chemical or biological threat or some other weapon of mass destruction could slip into the country inside a container. But even smaller disruptions could have a devastating effect on importers, too. Should an explosion inside a single container at one port prompt the federal government to shut down all U.S. ports temporarily, even a brief closure could cause significant economic hardships; witness last year's West Coast port closures, which, according to economists' estimates, cost the nation \$2 billion a day. At the extreme end of the imaginable-risk spectrum, South Carolina Senator Fritz Hollings, in a statement issued [www.boozallen.com](http://www.boozallen.com) in March, cited a Booz Allen

## New Rules of the Game

Government and private initiatives relating to supply chain security include:

- **24-hour Manifest Rule (24-hour Rule)** — U.S. Customs rule requiring carriers to submit a cargo declaration 24 hours before cargo is laden aboard a vessel at a foreign port.
- **Automated Commercial Environment (ACE)** — Update of outmoded Automated Commercial System (ACS). Intended to provide automated information system to enable the collection, processing and analysis of commercial import and export data, allowing for moving goods through the ports faster and at lower cost, as well as detection of terrorist threats.
- **Customs-Trade Partnership Against Terrorism (C-TPAT)** — Private-public partnership offering supply chain security guidelines. By complying with the voluntary guidelines and submitting to inspections, importers can qualify for expedited Customs clearance for incoming goods.
- **Container Security Initiative (CSI)** — U.S. Customs program to prevent global containerized cargo from being exploited by terrorists. Designed to enhance security of sea cargo container.
- **Fast and Secure Trade (FAST)** — U.S. Customs program that allows importers on the U.S./Canada border to obtain expedited release for qualifying commercial shipments.
- **Smart and Secure Trade Lanes (SST)** — Private initiative of the Strategic Council on Security Technology, an assembly of executives from port operators, major logistics technology providers, transportation consultancies, and former generals and public officials. Aims to enhance the safety, security and efficiency of cargo containers and their contents moving through the global supply chain into U.S. ports.

For more information on government security programs, go to [www.customs.gov](http://www.customs.gov) or [www.dhs.gov](http://www.dhs.gov).

Hamilton analysis concluding that “the economy would collapse within 20 days following an attack on a U.S. port.”

Beyond the broader economic risks, importers clearly have a direct stake in ensuring that their own supply chains are secure. In a September 2002 report entitled “Trade Security: A Wildcard in Supply Chain Management,” [www.arcweb.com](http://www.arcweb.com) Adrian Gonzalez, a senior analyst with consultancy ARC Advisory Group, writes, “No company wants to see its name on the front page of the Wall Street Journal being linked to a shipping container blowing up at a busy port....” Gonzalez notes that such a company could face financial losses, including a sharp drop in share value, as well as criminal prosecution for non-compliance with trade regulations, in addition to the overall disruption of the enterprise’s supply and demand chain.

### Who Pays for Security?

In the course of the public discourse on trade security, various estimates have surfaced that suggest beefing up supply chain security for goods entering the United States ultimately could cost billions, or even trillions, of dollars. Not surprisingly, much of the discussion surrounding trade security has centered on who exactly is going to cover those costs. “There is a fundamental tension right now,” says Gerald Woolever, a 35-year U.S. Coast Guard veteran who is now senior vice president for homeland security operations at supply chain consultancy INNOLOG, “between the people in the ports, the carriers and transporters, who don’t necessarily want to bear the expense of buying the technology and putting these procedures in place, and the government, which is trying to pass the cost

down to the people in the supply chain.”

Fortunately, as Woolever and others note, many of the processes and technologies that can help companies secure their supply chain against terrorist threats are the same solutions that enterprises have had at their disposal to fight theft and product tampering, to comply with existing customs and other regulations, and perhaps most importantly, to streamline their supply chain. Gerald McNerney, a senior research analyst and supply chain specialist with technology consultancy AMR Research, says that the systems [www.amrresearch.com](http://www.amrresearch.com) companies might use on a day-to-day basis to manage a secure supply chain could include a transportation management systems (TMS), solutions for connecting to trading partners for inventory visibility, international trade and logistics systems, and any tracking systems — such as wireless or radio frequency identification (RFID) devices — that a company uses to collect information on the location of goods in its supply chain, that is, solutions that were likely in place or under consideration before security cast a renewed spotlight on them. (See the sidebar, “New Threats, Same Old Tools,” on page 20 for a run-down of new applications for existing supply chain solutions.)

The change has been one of focus, says Neiman Marcus’ Howell. He notes that the retailer has always focused on the security of its merchandise as it moves through the company’s supply chain. “However, after 9/11 our focus broadened beyond just the physical security of our goods to include an understanding not only of our company’s facility and personnel security procedures but those of our supply chain business partners as well.”

And the company has found that sound security practices are not incompatible with good supply chain processes.

It is estimated that inspecting just 10 percent of the total number of containers entering U.S. ports on an annual basis would take 37 years.

### Security in Practice

For example, after Neiman Marcus implemented a global logistics control system from the software company Qiva (recently purchased by TradeBeam), the new system not only began providing information critical for security, it also just plain made good supply chain sense. “The system provides visibility to supply chain events before the goods leave the foreign country,” Howell says. “This provides much-needed lead time to identify security or other compliance-related issues before the goods reach our border. We believe the capabilities of this Internet-based system will allow us to keep pace with both the logistics and compliance sides of the global supply chain.”

The same principle applies to various supply chain processes, with certain procedures requiring only minor modification to produce heightened security. For instance, for several years Neiman Marcus has visited its foreign business partners’ facilities with a focus on labor and human rights issues. Now the company has enhanced those facility reviews to include security issues as well.

Similarly, Target’s Laden says that security issues were already one component of the company’s education and inspection work with overseas vendors as part of a five-year-old program at the retailer in conjunction with the private-public Business Anti-Smuggling Coalition (BASC) set up by U.S. Customs in 1995. And, in testimony before Congress last year,

Wayne Gibson, Sr., vice president for global logistics at The Home Depot — a company that [www.homedepot.com](http://www.homedepot.com) directly imports from 268 different vendors, sourcing 80 percent of its products from five countries — said the home improvement chain could use its current quality procedures (which include vendor inspections) to improve supply chain security, and that it could supplement its existing anti-theft procedures with anti-tamper efforts to improve container security, another key component of securing the supply chain.

### Toward Standards

Companies like Neiman Marcus, Target and The Home Depot that are taking steps to improve their supply chain security necessarily are funding these initiatives out of their own pockets. However, the government is providing some assistance for importers under the Customs-Trade Partnership Against Terrorism (C-TPAT), a program established last year by the Customs Bureau. Specifically, C-TPAT offers a set of guidelines that companies can follow in building their secure supply chains. The guidelines, which essentially are setting standards for the secure supply chain, cover such areas as procedural security, to ensure against unmanifested material being introduced into the supply chain; physical security of facilities and goods; security education and training; and manifest procedures.

Companies signing onto the

voluntary program provide self-assessments of their supply chain security and agree to submit to CBP inspections. Importers that meet Customs’ guidelines and recommendations for security improvements can take advantage of faster processing for their shipments coming into the country, assuring a smoother, more predictable flow of goods through their supply chains. C-TPAT members also gain access to the coalition’s membership list, helping to establish a pool of best practices around supply chain security.

Other U.S. government initiatives around supply chain security may impose additional burdens on importers, but these initiatives, too, could come with benefits. The Container Security Initiative (CSI), for example, is a CBP program that calls for identifying so-called “high risk” containers and inspecting them at the port of origin in order to prevent a shipment containing, for example, a weapon of mass destruction from reaching U.S. shores before being subject to inspection. Some observers have questioned whether this system, initially targeted for implementation at the world’s top 20 ports shipping to the States, could produce logjams at foreign ports, but the potential benefits would include faster processing of shipments on arrival and less risk that a transport ship might be diverted or delayed due to concern about a single container onboard. (See the sidebar, “New Rules of the Game,” for a summary of government programs for supply chain security)

## Strategies for a Secure Supply Chain

The standards that these and other government initiatives are establishing will evolve, of course, and companies looking to build a secure supply chain must incorporate sufficient flexibility into their processes and systems to accommodate changes in regulations as well as new threats.

For instance, importers recently had to begin complying with the so-called "24-hour rule," a regulation requiring carriers and non-vessel operating common carriers (NVOCCs) to file a cargo declaration 24 hours before cargo is loaded aboard a vessel at a foreign port. Failure to comply with the rule could result in fines and denial of entry for the vessel's cargo. "That's a very big change to a process that has been fairly antiquated for a long time," AMR's McNerney says, "so it's a big leap for companies to meet that expectation." The analyst says that many companies have become accustomed to putting a container together at the last minute and delivering it to a loading dock. That may no longer be an option. In addition, some companies lack the electronic infrastructure to be able to provide the necessary data to Customs, so they will have had to work closely with their freight forwarders and carriers to ensure compliance.

The good news is that the government has not specifically defined what a secure supply chain is, says Beth Peterson, a 20-year logistics veteran who is now vice president of product solutions with Open Harbor, a [www.openharbor.com](http://www.openharbor.com) provider of global trade management solutions. "That means that companies can apply their own interpretation to their operations and their product type to define what is secure," she says.

In general, Verle Hammond, president and CEO of supply chain consultancy INNOLOG, recommends that companies view security not as a separate goal in and of itself, but as part of the larger supply chain environment. "The understanding of the end-to-end nature of the supply chain on the one hand, and the understanding of security on the other hand, have really been separate concepts," says Hammond. That disconnect has prompted some companies to focus more on implementing point solutions to shore up security in one particular aspect of their supply chains — such as implementing RFID tags to track containers while they are in transit — rather than looking at the movement of goods all the way up and down the supply and demand chain. "You have to understand everything that happens from beginning point to the point of ultimate use," Hammond urges.

Can a supply chain ever be totally secure? Hammond, a veteran of 28 years as a logistician in the U.S. Army and a supply chain consultant for 14 years, since he founded INNOLOG, doesn't think so. He notes that many nodes through which goods pass employ outmoded asset management and inventory processes that need to be revised. "You need to update those processes, otherwise all the technologies that you can implement won't guarantee that you can reach that 100 percent secure and efficient supply chain," Hammond concludes. □

Reprinted with permission from  
iSource Magazine,  
June/July 2003

## New Threats, Same Old Tools

While terrorism presents new threats to the supply chain, many of the technologies that companies can use to secure their own supply chains already exist. Here's a rundown of security-related applications for some existing solutions:

Existing Solution	Application
Supply Chain Process Management (SCPM)/Network Connectivity	Connectivity with trading partners; "real-time" visibility to inventory, demand; enables companies to respond to disruptions.
Logistics Resource Management	Up-to-date intelligence on global shipping regulations; connectivity to government systems; a central repository for all shipping documentation and activity.
Global Trade Management	Restricted party screenings; compliance with trade regulations and documentation requirements.
RFID Tags, Wireless Networks	"Real-time" tracking of inventory, conveyances and assets; detects tampering of sealed containers.
Network Design, Strategic Sourcing	Reconfigure supply chains and perform "what if" analysis.

**Source:** Adrian Gonzalez, "Trade Security: A Wildcard in Supply Chain Management," ARC Strategies, September 2002. Mark W. Vigoroso, "Vessel Manifest Rule Underscores Importance of Logistics Visibility," May 5, 2003, Aberdeen Group.