MARCH 1, 2006 | CIO MAGAZINE

SECURITY COMPLIANCE

Customs Rattles the Supply Chain

The government wants you to secure your supply chain. Right now, its program is voluntary. It won't stay that way for long. And the responsibility for collecting the data Uncle Sam wants is going to fall on—you guessed it—the CIO.

BY BEN WORTHEN

Between 2002 and 2005, the Department of Homeland Security spent $75 million to track several companies' cargo containers coming into the seaports of Seattle/Tacoma, Los Angeles/Long Beach, and New York/New Jersey. The project, called Operation Safe Commerce, used GPS technology and radio frequency identification to monitor cargo from a handful of major importers (including Sara Lee and Motorola) as it made its way from overseas factories to its final destination in the United States.

The goal of Operation Safe Commerce was to identify weak links in the global supply chain. A report summarizing its findings was due more than a year ago, in February 2005. To date, for a variety of reasons, no report has been released. But sources close to the project have told CIO that Operation Safe Commerce revealed that companies actually know very little about what goes on in their supply chains.

Among common unsafe practices identified by these sources were: truckers dropping off containers without ever encountering terminal security, containers left in unsecured areas, and containers bypassing a port that's considered safe (even if scheduled to pass through that port) and traveling instead through a country that poses a greater threat—without either the company or U.S. Customs and Border Protection being informed.

CIO to Go

Don't have time to read? Listen to the **audio version** of this article. Download: **Customs Rattles the Supply Chain**.

According to Steve Schellenberg, a senior consultant at the trade advisement company IMS Worldwide who worked on Operation Safe Commerce for the port of Seattle, the project "showed us that there needs to be a quantum leap in the information we possess about the supply chain."

Companies will have to find a way to make that leap—possibly within the next year—because soon the government will make sharing this information a cost of doing business for every company that engages in international commerce.

The mechanism for the government's initiative is already in

place: the Customs-Trade Partnership Against Terrorism, or C-TPAT, which requires that companies take responsibility for the security of their supply chains. C-TPAT is currently voluntary, but program members say that the benefits of compliance—which include reduced wait time at borders and fewer inspections—will make participation an unavoidable cost of doing business.

"There's really very little that Customs can do to speed things up," says Schellenberg. "But they can sure as heck slow you down."

The Story Continues...

For updates on the Dubai Ports story, stay in touch with **CIO News Alerts**. Read our **ANALYSIS: Selling U.S. Ports to Dubai**.

Furthermore, members of the trade community believe that the government will eventually make C-TPAT participation mandatory, although a spokesman for Customs disputes that. CIOs need to begin preparing now, or they could find themselves facing a massive last-minute hurry-up, comparable to their Sarbanes-Oxley travails, if they don't want to watch their company's containers get held up at Customs while their competitors' crates sail through.

"There's no doubt that this is going to happen," says Kevin Smith, general director of global customs for General Motors. "This is an inevitability."

THE NIGHTMARE SCENARIO: WHEN, NOT IF

Right now, information about any given supply chain is hard to come by. And that's by design. The goal of supply chains is to get something that's needed—a part, a product—to where it's needed as quickly and cheaply as possible. If a container arrives too late to be loaded onto one ship, it's rerouted and loaded onto another. And as long as the container arrives on time—or close to it—no one need be the wiser. In fact, historically, each person or entity that handles a shipment collects and shares information only to the extent necessary to guard against liability.

Similarly, Customs was created to enforce tariffs and calculate import taxes. And while Customs' role expanded to combat drug trafficking in the 1980s, regulating trade was the department's primary job until September 11, 2001. Now, says Robert Bonner, former commissioner of U.S. Customs and Border Protection (he resigned in November), "The priority mission of U.S. Customs is national security."

The Stories Containers Tell

Technology can make the cargo talk.

Read More

Experts say that Bonner, who was sworn in at Customs on Sept. 24, 2001, was right to change the agency's focus. Most agree that the likelihood of terrorists attacking the United States through the global supply chain is so high that it's a matter of when, not if. Such an attack (most analyses focus on a dirty bomb) won't primarily be designed to kill a lot of people, but to cause panic. "It isn't the event but the sudden lack of faith in the system that it causes," says Stephen Flynn, senior fellow for national security studies at the Council on Foreign Relations.

If a bomb goes off, Flynn says, there will be huge pressure on the government to close all the nation's ports until every container on every site in the country is inspected. An October 2002 war game that mimicked that scenario found that closing the nation's ports for as many as 12 days created a 60-day container backlog and cost the economy roughly $58 billion. "Any incident would shut down commerce," Sen. Patty Murray of Washington told CIO. Murray is the ranking member of the Senate Appropriations Committee Subcommittee on Transportation, Treasury, the Judiciary, Housing and Urban Development and Related

Managing the Terror Risk

Should Customs focus on preventing an attack or responding to one?

Read More

Agencies.

Securing the Supply Chain: Sox and C-TPAT

Customs has developed a two-pronged strategy to prevent the dirty-bomb scenario. First, it's asking companies to assume responsibility for their supply chain security.

Legally, a company is responsible for a container only when it formally purchases it, which—precisely for that reason—usually doesn't occur until it reaches a port, either in the United States or abroad. Target, for example, typically does not legally purchase the clothes it orders from China until they arrive in the terminal. But the government wants importers to take responsibility for everything that occurs prior to purchase, even if the container is in the custody of a trucker in China or a longshoreman in Rio de Janeiro. The principle vehicle for this is C-TPAT. This so-far voluntary program gives certain benefits, such as reduced inspections, to companies that can show they meet a minimum level of supply chain security. The better a company's security (as judged by Customs auditors), the more benefits it receives. There are currently three tiers of C-TPAT compliance, and containers belonging to members in the top tier sail through Customs virtually uninspected.

If C-TPAT is the carrot, then the Sarbanes-Oxley Act (Sox)—which requires that companies put in place reasonable safeguards against events that could materially affect the company's value—is the stick. There's little doubt, experts agree, that events in the supply chain fall under the Sox umbrella.

With both C-TPAT and Sox, IT's job is the same: Secure the data, make sure that purchasing and security have access to one another's information, and collect more data about what is happening in the extended global supply chain.

The second prong of Customs' strategy is to collect as much information as it can about what's happening in the supply chain so that, through data mining, it can spot anomalies. The key to this is the Automated Commercial Environment, or ACE, a $3 billion-plus trade processing system begun in 2000, which Customs plans to complete by 2010. ACE has modules that do everything from serving as Customs' ERP system to targeting containers for inspection. Within the next six months, carriers entering the United States through land-border crossings in seven states will be required to send close to 100 data elements to Customs, including information about the vehicle, its driver and its cargo. If they don't, they don't get in. Customs is also piloting an ambitious ACE add-on called the Advance Trade Data Initiative (ATDI), which requires importers to share with Customs every bit of information about a shipment, including the purchase order, which ports it passes through, proof of delivery and its final destination within the United States.

"ATDI will make companies collect information that they haven't collected before, share information they haven't shared and provide information earlier than they've been required to provide it before," says GM's Smith. For example, it's the rare company that knows where on a ship its container is located, but ATDI will require it.

Eventually, experts say, Customs plans to make ATDI participation a requirement for tier-three C-TPAT certification. (Customs says that ATDI participation qualifies participants for tier-three

Sox and the Supply Chain

A bomb in a box would have a "material impact" on a company's value

Section 404 of the Sarbanes-Oxley Act (Sox) requires companies to establish controls that provide reasonable protection against preventable events that could have an impact on a company's value. For CIOs, this meant making sure that employees couldn't use a company's systems to commit acts of fraud. While the Securities and Exchange Commission did not focus on it during the first year of Sox compliance, the same logic applies: Companies

status, but that it will not be a requirement.) Soon, companies that achieve this level of compliance will be rewarded with a Green Lane designation—essentially a "get out of Customs free" card that will do for borders what E-ZPass does for highways.

"A huge number of containers come into our country," says Sen. Murray—about 9 million a year. "Right now, we don't know what's in them, who's handled them, if they've been opened."

need to have controls that protect them against an adverse event within a supply chain. There are other sections of Sox that indicate that the supply chain will become an area of emphasis in the future as well. Section 401 requires companies to account for risk in their off-balance-sheet transactions, such as their supply chains. And Section 409 requires companies to report "on a rapid and current basis" events that could have a material impact. One can assume that a bomb in a cargo box would have such an impact.

If the government gets this information, it can clear most containers before they even reach the United States. This will allow Customs to focus its limited resources on the containers it knows the least about.

As Murray puts it, "We're trying to reduce the size of the haystack."

THE SECURE 10,000

After 9/11 there were calls by some members of Congress to inspect each and every one of those 9 million containers coming into the country. But the vast majority of those containers are filled with legitimate goods from legitimate sources heading to legitimate companies. "The question we faced was, Can you risk-manage for terrorism?" says Bonner. "If the answer is yes, you can spot-inspect." (For more on the issue of risk-managing onetime events, see "Managing the Terror Risk" .)

In July 2002, Bonner unveiled C-TPAT, which, by shifting that burden onto the importers, was designed to reduce the need for the government to inspect containers. Since then, over 10,000 companies have applied for C-TPAT membership. In 2005 C-TPAT members accounted for 42 percent of all imports by volume.

There are three tiers of C-TPAT membership, each of which comes with progressively fewer inspections. The first level simply requires an attestation that your company has performed a risk analysis of its supply chain and has taken steps to mitigate any vulnerabilities. So far, 5,757 of these attestations have been accepted by Customs. Tier-two members have had this attestation validated by Customs officials. Right now, 1,511 companies have achieved tier two (another 2,273 validations are in progress). Tier-three members are companies that Customs has determined follow supply chain security best practices (although Customs has not yet defined any). These are the companies that will be eligible for the Green Lane. Only 126 companies to date have qualified for tier three, including Boeing, General Motors and Target.

HOW TO GET YOUR GREEN LANE TICKET PUNCHED

Securing your supply chain data is the most obvious step to reach at least tier-two C-TPAT status (although eventually, sources say, there will be only a tier three; everyone else will be treated the same—poorly). And no one should be surprised that it's important to encrypt and protect information about the schedule and location of your shipments. But securing supply chain data goes beyond that. Importers have to attest to their partners' security. "We had an audit [at a partner's factory] in South Africa, and they grilled them about IT security," says Jim Wigfall, VP of supplier management for Boeing Shared Services. Customs auditors checked the partner's firewall, backup systems and access controls. (The company passed.) Now Boeing does the same every time it vets a potential partner against C-TPAT requirements.

It's also important to limit access to supply chain information. "If the bad guys know that IBM is going to ship products from point A to B on a particular Tuesday, it gives them a leg up," says Debbie Turnbull, IBM's program manager for supply chain security. A bad actor inside a company could alter the information attached to a container from Karachi, Pakistan (which might raise an alarm), so it looked like it was coming from a factory in Hong Kong (which might not). Or that bad actor could pass scheduling information to a crony outside the company. IBM uncovered one such plot a few years ago. A worker in a plant in Mexico noticed that one container he was about to load was 53 feet long on the outside, but only 50 feet long on the inside. Upon inspection, it was found that the container had a false back, behind which was hidden several million dollars in narcotics.

While it's important to keep information about shipments from people who don't need to know, it's equally important that the people who do need to know the details have access to them. For CIOs, this means integrating the systems used by the purchasing and supply chain organizations, and making sure that the system can capture information such as a country's security profile. The integration benefits both departments, says Ron Miller Jr., Customs compliance coordinator for P&G's Global Cross Borders Group. Making purchasing information available to the supply chain group allows it to identify low-risk partners and pass that information on to Customs for C-TPAT validation. If, for instance, you can show that something is a regular shipment from a secure business partner, it is less likely to be inspected, says Miller.

Similarly, purchasing people need to have data on the security of the factories and countries to which they plan to source. If they don't have this information, a cheaper product may end up costing more when delays for inspections are factored in.

"We were sourcing computer components from Singapore," says IBM's Turnbull. "Someone in purchasing made the decision to source the same components out of Indonesia. The exact same part from Singapore, with no inspection, got stopped when it came from Indonesia." Making this information accessible to both parties requires constant updating.

Assuring that your suppliers are handling your cargo in a secure way will require greater visibility into what is actually happening in the supply chain. Someday, this will be done through RFID, smart containers and other emerging technologies (see "The Stories Containers Tell"). But right now, many of these technologies are still too immature or expensive to work in the real world. Until then, companies will need to integrate systems with their overseas suppliers so that they can risk-manage the supply chain by spotting anomalous activity as it happens. Even secure processes "can be compromised," says Ken Konigsmark, Boeing's C-TPAT program manager. "[Overseas workers] get paid peanuts, and it would be very easy to bribe them." CIOs need to be able to tell when a truck driver leaves a factory and when he arrives at a port. The CIO can then alert Customs if a four-hour trip turns out to take 12.

This is a major challenge when the supply chain is global. "The things we take for granted may be very difficult for a coffee producer in Colombia," says P&G's Miller. For factories and freight forwarders that cannot send EDI messages, CIOs may need to set up Web-based access to their supply chain systems. And they better start soon, since Customs is going to want that information, sources say, as early as next year.

CUSTOMS' ACE IN THE HOLE

Since the late 1990s, Customs' Automated Targeting System (ATS) has identified which containers to inspect by feeding the information it possesses about a shipment into an algorithm designed to calculate risk. Last summer, the DHS inspector general released a report critical of ATS, saying it didn't have the information to accurately identify suspicious containers. The report made no reference to the Advance Trade Data Initiative, the targeting system that Customs is currently

piloting.

ATDI has its roots in a conversation that took place shortly after 9/11 between Mike Laden, then president of Target's custom broker division, and the late Assistant Commissioner of Customs Bonni Tischler. "We were talking about the information that Customs needs," recalls Laden. "Finally I looked at her and said, 'Do you want to know what we buy? Heck, sometimes we know months in advance.'" Shortly thereafter, Laden gave Customs a file with 1,000 purchase orders—data that included a description of the goods being purchased, their price and their factory of origin. Customs set out to learn what it could from the data.

Pre-9/11, Customs' first encounter with a container was when it entered a U.S. port. The only information it had about the container was the manifest, describing its contents and port of origin. Tom Bush, director of targeting and analysis systems in Customs and Border Protection's IT office, says that from Customs' point of view, containers simply materialized in an American port.

"Sometimes we may think a container originated in a safe port, when it could have come out of Karachi," says Bush. On the other hand, "a purchase order gives you insight into the actual point of origin, as well as the buyer and seller relationship." In early 2003, Customs began to build a system that was capable of combining commercial information like purchase orders and shipment notifications with intelligence reports and other counterterrorism information.

Today, Target and around 30 other companies are participating in the ATDI pilot. (Participation currently means entering into an understanding with Customs and doesn't necessarily include sharing data.) Once past the pilot stage, ATDI participants will need to send Customs a copy of a purchase order as soon as one is filled out and a copy of the shipping notification they receive from a factory when their cargo ships. Customs also plans to collect information about overland transport, a container's location within a terminal and where on the ship a container is located, as well as notification when a container reaches its final destination in the United States.

One problem for importers is that they rely on third parties such as truckers and shipping companies for most of this information. Bush says that companies will need to share only what they're capable of sharing. But importers are concerned that just as C-TPAT requires companies to be responsible for parts of their supply chains for which they are not legally responsible, ATDI will eventually demand that they provide all of the information Customs is seeking. One place to look for clues to how all this will work out is the ACE e-manifest program that Customs is piloting on the Canadian border in Washington state and Detroit, and at the Mexican border at Nogales, Ariz., among others.

The ACE pilot asks cargo carriers to share close to 100 pieces of information about their shipments, everything from the vehicle identification number on a truck to the address of the importer. If Customs does not receive all of this data by at least an hour before the truck reaches the U.S. border, there will be various penalties.

"The major difficulty for us was that the information for the driver, vehicle and cargo were in three different systems," says Janet Shearn, director of customs and trade compliance for UPS, one of three companies (along with Brown Line and ABF Freight System) that participated in the pilot program. (The pilot has since expanded to include about 400 companies, 25 of which are now sharing data with Customs.)

UPS had to integrate these three systems in order to send a single timely EDI message to Customs. The information also had to be formatted so that Customs could read it. For example, Customs wanted information that UPS stored as address line one in address line two. In other cases,

Customs wanted information that UPS simply didn't have, such as a driver's passport number. And if any of the information was left blank or entered incorrectly, the truck, hypothetically, could be held at the border until the problem was fixed.

Customs plans to publish requirements for the ACE program within the next few months, which means that companies will have 90 days to comply. It won't be easy. "We had all the systems in place and it still took us more than 90 days," says Shearn.

The ACE program foreshadows how ATDI will likely collect data from companies. One Customs report identifies potential EDI standards companies could use to share information. But Customs' Bush says that be it EDI or XML, "We have the ability to handle data in the way that [CIOs] use it."

Many questions remain about how Customs will protect the information it receives, how it will use it and just how exactly it will carry out such large-scale data mining. "I have a great deal of concern," says Smith of GM, which is advising Customs on ATDI but declined to participate in the trial. "ATDI is about commercial data that has never been given to the government before, and sometimes it is not available when they want it. When you force someone to type data in before it is normally available, you get errors. What good is information when it's wrong?"

Security is another concern. Purchase orders often contain competitive secrets, such as the rates that factories charge importers. Not only would the government have to protect this data from hackers, it would also have to develop a way to protect it from Freedom of Information Act requests.

And even if it solves these problems, there's still the matter of making the system work. "It would take 20 supercomputers chained together just to go through the data from Target, Wal-Mart and Sears," says Laden, who left Target last May to start the consulting firm Trade Innovations. (Bush says the system will work but declined to discuss specifics, citing national security.)

Regardless of the difficulties, Shearn and Laden are convinced that ATDI will move forward.

"Companies need to realize that this isn't going away," says Shearn. "There's a commitment from DHS, and they have the money to make this work."

The ROI of Security

One of the challenges that comes along with securing the supply chain is measuring success. How do you know you've prevented something that hasn't happened? Chuck Winwood, a former deputy commissioner of Customs, now senior VP for border security at the trade consultancy Sandler & Travis, says CIOs should judge how well they are improving security by using traditional business metrics: "Improvements in safety, insurance liability, efficiency—these are outgrowths of a good security program."

The reduction in inspections promised by C-TPAT are another potential source of ROI. Toymaker Hasbro spent just under $200,000 on its up-front C-TPAT compliance and spends an additional $112,500 a year maintaining it. Since it became C-TPAT-certified in November 2002, its inspections have dropped from 7.6 percent of containers coming into the U.S. in 2001 to 0.66 percent in 2003. Given that in 2003 the company imported about 8,000 containers, and that port authorities charge around $1,000 per inspection, Hasbro is saving about $550,000 a year in inspection costs alone, approximately a 5-to-1 return rate.

Members of the trade community expect that ATDI participation will be a requirement for Green Lane status. And while no one has a firm timetable for the merging of ATDI and C-TPAT (Customs says that participating in the ATDI pilot qualifies companies for tier-three status), the funding is in

place. In November, Sen. Murray introduced the Green Lane Maritime Cargo Security Act of 2005; expectations for its passage are high. In all likelihood, CIOs will have between 18 and 36 months to prepare for compliance, but a terror event looms as a wild card. If there's an attack, that timetable could telescope quickly.

Senior Writer Ben Worthen can be reached at bworthen@cio.com

Dated: March 01, 2006
http://www.cio.com/archive/030106/supply_security.html