C-TPAT Part II: strategies for obtaining and keeping C-TPAT certification

Editor's note: *This is the second installment in a two-part series on C-TPAT, the Customs-Trade Partnership Against Terrorism. Part One looked at the origins and evolution of the security initiative, under which U.S. importers agree to continuously police their own supply chains in return for a host of benefits, including reduced cargo inspections. This installment discusses strategies for obtaining—and keeping—C-TPAT certification.*

C-TPAT MAY HAVE ITS CRITICS (SEE "IT MAY not be perfect, but C-TPAT's here to stay," *DC VELOCITY*, November 2005), but that hasn't slowed its momentum. As of last April, more than 9,000 importers had applied for C-TPAT certification. And new applications pour in every month.

But obtaining (and keeping) that certification got harder last March, when the Bureau of Customs and Border Protection (CBP) introduced new and stiffer standards. These new standards, which apply to new applicants and current C-TPAT members alike, mean they must now be able to confirm, among other things, that foreign suppliers, vendors and contractors are performing seven-point container inspections, documenting their procedures for issuing keys , changing passwords, and an array of other best security practices.

As part of the program, CBP requires C-TPAT members to prepare a Security Profile that outlines the steps they're taking and to conduct ongoing internal audits to ensure that their employees, vendors, suppliers and trading partners actually follow enhanced policies and procedures. Though it doesn't require existing members to provide proof of compliance, CBP isn't relying entirely on the honor system either. For that, it has established what it calls a "validation" process, whereby CBP supply chain security specialists meet with company representatives, and visit foreign and domestic sites to verify that everyone in a company's supply chain is following the practices outlined in the member's Security Profile. If the inspections reveal significant problems, CBP can suspend or even revoke the importer's benefits.

To avoid putting your C-TPAT certification at risk, you must establish an ongoing program to assess how well your security program is being carried out and identify new areas of risk that require remedial action.

But who should conduct this assessment? Many times, companies assign this task to logistics or customs compliance personnel, who tend to use boilerplate security checklists to identify vulnerabilities. That's a dangerous practice. This is no ordinary compliance task; an in-depth security assessment requires specialized expertise.

By definition, the global supply chain is a sprawling network of domestic and foreign partners that manufacture, pack, load, consolidate and transport merchandise to the United States. Each of those partners follows a unique set of processes, and those varied processes represent almost limitless potential for security breaches. Auditors who don't have an in-depth under-

standing of the various ways to circumvent security safeguards have no hope of identifying all these risks or knowing how to remedy them effectively. Whether you opt to use in-house resources or bring in an outside security specialist, make sure you're using a qualified and knowledgeable professional with extensive experience in logistics security.

Avoid the traps

Deciding who will conduct their security assessments isn't the only problem importers face, however. There are plenty of other ways to get tripped up in the process. What follows are some tips on avoiding several common missteps:

■ Make sure nothing gets lost in translation. When working with partners in foreign countries, there's always the danger that cultural differences and language barriers will lead to miscommunication. To prevent that, we use customized supply chain security questionnaires that ask key questions several different ways, each worded differently. If respondents answer "yes" and "no" to the same question, that's a signal that they either didn't understand the question or weren't providing accurate responses.

It's also a good idea to confirm the information these partners provide through follow-up e-mails and conference calls. More often than not, we find that the feedback foreign companies provide during these exchanges differs from their original answers. That's not to say they're deliberately trying to mislead us; it may be a simple case of misinterpretation arising from language differences. But whatever the cause, you can't afford to be misled. Foreign suppliers tend to be one of the most vulnerable links in the supply chain today; it's imperative that nothing gets lost in translation.

■ Emphasize the need for candor. It's not only foreign partners who may provide misleading information, of course. Domestic partners and even personnel at your own facilities may be reluctant to expose and document inadequacies in their security practices and programs. Your challenge will be to convince everyone to be open about security weaknesses. Let them know that while there's no shame in exposing vulnerabilities, the failure to disclose a known security breach could result in your supply chain's being compromised.

■ Provide in-depth, focused training. The new C-TPAT criteria require that importers establish a threat awareness and security training program. This isn't a quick overview of the basics; this should be exceedingly specialized instruction. Your security depends on workers' ability to recognize potential threats—whether terrorists' plots or internal conspiracies. In order to do this, they'll need detailed information so they'll know specifically what to look for.

It appears that some companies have a long way to go when it comes to threat awareness training. That became evident to us recently when we went out to conduct a C-TPAT training seminar that focused on security seals, one of the most important components of a supply chain security program. During that session, we asked the attendees whether they thought bolt seals could be circumvented. Ninety percent said no, bolt seals were tamperproof; the remaining 10 percent told us they suspected that bolt seals could be compromised, but they had no idea how. That was a troubling response. Bolt seals can, in fact, be circumvented. But if the people responsible for seal integrity don't know that (or don't know how), they're unlikely to detect a breach.

See for yourself

If you want to keep your certification, you will need to have an ongoing security auditing program in place for your facilities as well as those of your supply chain partners. Aside from its being a C-TPAT requirement, it's also a very sound practice.

A C-TPAT compliance audit we conducted at a Hong Kong consolidator confirmed the wisdom of performing adherence audits. Prior to our audit, company representatives had assured us that their personnel diligently followed all of the security procedures we asked them to establish. Among other claims, they told us that their facility had "complete video coverage throughout [its] warehouse" and that our client's goods were "always kept in a segregated, highly secured area."

But when we audited this facility, we found otherwise. Take the "complete" video coverage, for example. True, the facility had a CCTV system in place, but the camera views were of poor clarity and too broad to be of much use. And the video coverage was anything but complete; we found that our client's goods were not monitored from the time they arrived to the time they were reloaded for shipment to the Hong Kong seaport. We also discovered that the system's digital hard drive could archive only seven days' worth of footage, making it impossible to investigate any event that dated back more than a week.

We also uncovered problems with the consolidator's shipment verification practices. For example, although its security policy dictated that only senior personnel would remove an inbound truck's security seal, we found that in reality, seals were being removed by whoever happened to be working on the receiving dock. As a result, workers did

not always take the time to verify that the seal number on an inbound shipment matched the manifest (another policy violation).

Things were no better with the seals used for outbound trucks. We found that these seals often sat unguarded on the shipping dock, fully accessible to employees, vendors and truckers. Because the shipping crew had stopped using seals in numerical sequence, it would have been easy for a driver to steal one of these seals and reattach it to a truck's doors after it left the facility, concealing the fact that the trucker later accessed the truck's cargo area without authorization.

As for the consolidator's claims that it was segregating our client's product in a "highly secured area," we found that the fencing was only eight feet high and had no ceiling to keep intruders from climbing over. We also found that the keypad code to this area hadn't been changed in nearly nine months and was known to most of the workforce (including those without clearance to this area). And the alarm system wouldn't have been much help. We determined that the alarm was only being armed at the end of the workday, even though the area was frequently left unoccupied for hours at a time.

Once we notified the consolidator of these and other security loopholes, it remedied them promptly. But this experience points up how easily your inventory can be exposed to unnecessary risks.

If your company is a C-TPAT-certified company, it's your responsibility to make sure your security safeguards are as good in reality as they appear to be on paper. It's no secret that shipments to certified companies stand a much lower chance of being opened and inspected by CBP inspectors. That makes shipments to C-TPAT-certified companies precisely the ones terrorist cells are most likely to target—underscoring the importance of identifying loopholes in your supply chain safeguards before others have the opportunity to exploit them. Doing anything less could jeopardize your C-TPAT certification and expose your company to the catastrophic ramifications of having a weapon of mass destruction smuggled into your supply chain. □

Barry Brandman is president of Danbee Investigations, a Midland Park, N.J., company that provides investigative, loss prevention and security consulting services to many of the top names in the logistics industry. He is the author of *Security Best Practices: Protecting Your Distribution Center From Inventory Theft, Fraud, Substance Abuse, Cybercrime and Terrorism.* You can reach him via e-mail at bbrandman@danbeeinv.com or (201) 652-5500.