Better Business
Means Safer Business

A Call to Action for Global Trade

A VISCO White Paper

291 Wall Street
Kingston, NY 12401
(845) 383-3800
www.viscosoftware.com

Fallout…

The fallout of a Brooklyn race riot in 1973 continues 32 years after the incident: Ralph Alini, of Staten Island, was charged with murder of Jose Colon in October, 2005, 32 years after the fatal shot was fired. The indictment and arrest was not the result of cold case detectives who worked leads until they found their man. The police had always known who pulled the trigger and he had already pleaded guilty and served time for reckless endangerment in connection with the shooting. So why did it take 32 years to bring the murder charge? The answer is horrifyingly simple: it took 32 years for Mr. Colon to die of an infection caused by the bullet.

The fallout from 9/11 continues.

If you think your business has survived the September 11th attacks, you should think again. The attacks were a wake-up call heard around the world. We learned how vulnerable the air transportation system was, and anyone involved in the global trade industry knew that vulnerabilities in air transportation were minor compared to those of maritime shipping. Five years later, not enough has changed.

From beginning to end, foreign-sourced supply chains have vast stretches that are unmonitored. We move goods around the globe in much the same way they did during the 18th Century. Our global trade system isn't the result of a grand design; the "system" has evolved based on business needs. We move goods as quickly as possible, with the acceptance that a significant amount of loss (theft) is a cost of doing business. With little or no perceived business benefits, and no real governmental requirements, the development of robust security technologies and procedures has remained a low priority for more than 200 years.

The attacks also demonstrated that despite having all the technological capabilities of the information age, government agencies had no means to share information that could have prevented the hijackings. We learned of the competition and distrust that was pervasive between some of the government entities created to protect us. We've seen similar issues in our own industry in the relationship between government and the trade.

The fact is the world has changed and the global trade industry must change in response. We know the global supply chain is not safe. We can do nothing and hope the threat will pass, or we can answer the challenge with the most powerful weapon at our disposal; our entrepreneurial and economic ingenuity.

We can do better.

Fortunately, where global trade is concerned, better business means safer business. The same tools that are improving the bottom lines of importers throughout the industry can also be used to improve security by providing key data about inbound shipments.

What would happen to your business?

September 11th showed that our industry needs to change drastically or risk being used as a far more powerful weapon than the aircraft used in the attack. Surely if airplanes could so easily be turned into weapons, shipping containers must be under consideration for future operations. The 9/11 Commission estimated that the attacks on America cost less than $500,000 to execute. How many containers of cheap goods could be imported for

$500,000? And it will only take one success to bring the entire global supply chain to a dead stop.

We know Al Qaeda was aware of the potential economic impact of the "planes operation". US losses connected to 9/11 are estimated to be from $2.5 billion - $2 trillion, depending on who is asked. What would the losses be if every US port were simply closed for a week? What would our store shelves look like? What would happen to consumer confidence? What would happen to the world-wide economy? What would happen to your business? We must assume the potential for this kind of havoc would be nearly irresistible to terrorists. Our industry must take action.

Customs and Border Protection

US Customs is now Customs and Border Protection, and is part of the Department of Homeland Security. CBP's primary mission is now homeland security and the agency has taken steps to make the supply chain more secure. Not all of the initiatives have been effective or popular but this is a process. Newly appointed CBP Commissioner, W. Ralph Basham, has pledged to continue the agency's commitment to balance security and trade facilitation. One of their greatest challenges is enlisting the expanded cooperation of the trade. But just as with some law enforcement agencies, trust has never been a hallmark of the relationship between trade and government.

We have to change that. The trade must engage with CBP to find ways to provide the information they need in a way that will protect the proprietary information that forms the foundation of an importer's business. This kind of cooperation between government and trade would be ground-breaking. We can build a 9,200 TEU container ship; surely we can apply the same level of technological and economic ingenuity to information sharing.

Customs-Trade Partnership Against Terrorism

The purpose of C-TPAT is to protect the people of the United States from terrorism by protecting our ports. We tend to think in terms of radiological and biological agents, but this fight is so much more complex than that. It's true that we owe it to the people who live and work in and around our ports to keep them safe, but the biggest impact of a major incident at a port would be on our economic well being. It is imperative that we protect our way of life by protecting the economy, at home and abroad.

The story goes that there was an exchange between an executive at Target and a US Customs official shortly after 9/11, during which the Target executive asked if it would be helpful if US Customs knew what Target was buying in advance of shipment. This was the birth of the Customs-Trade Partnership Against Terrorism. The labor pains didn't hit until later. The question of what information would be shared, from whom it would come, and how it would be transmitted has been in question ever since.

The most important aspect of C-TPAT is the concept of partnership between government and trade. The American Heritage Dictionary defines

partnership as: "A relationship between individuals or groups that is characterized by mutual cooperation and responsibility, as for the achievement of a specified goal: Neighborhood groups formed a partnership to fight crime."
A successful partnership is one where each entity contributes and each benefits. In the case of C-TPAT, the partnership may not be as effective as we'd hope because the nature of the partners' needs is seemingly at odds. CBP wants more information from the trade, but the trade needs to protect the very same information in order to stay in business. We haven't gotten a lot further than that.

Many in the trade feel that the benefits of the partnership are just not there. CBP has not gone far enough to ensure the program does indeed have demonstrable benefits. Without significant, tangible benefits, a voluntary program cannot succeed.

Legislation.

Trying to build a partnership between tens of thousands of importers and a governmental bureaucracy is difficult enough, but on top of all this is the issue of dealing with politicians, the public, and the press. We learned during the Dubai Ports World controversy that a little bit of knowledge can be very dangerous. We can

disagree about the intentions of politicians who call for safeguards we know to be impossible, but if we have no meaningful industry-wide strategy with which to answer, we are the real problem. The global trade industry must take the lead in dealing with port and container security, or we will be doomed to follow the lead of those who are engaged in the issue, no matter what their experience in the industry may be. It is as simple as that.

Once signed into law, the recently passed Port Security Improvement Act of 2006 (H.R. 4954; S 2008), will require the collection of advance, non-manifest data, if the importer is to receive any benefit from C-TPAT. It will be the responsibility of the importer of record to provide this information. While this may send chills down the spines of importers of record nation-wide, there are ways to achieve this will satisfy C-TPAT requirements, and lead to increased profitability for the importer.

What's possible today.

While the idea of advance submission of data may be relatively new, the technology to submit this critical data about inbound shipments – from customer quote, through delivery to final US destination (including manufacturer, vendor, product, shipping information, and much more) – is already in use today, and is driving up revenues of user companies. Software is being used to build bridges between logistics, sales & purchasing, warehouse/inventory, and finance departments, allowing users to understand the entire supply chain from all perspectives. User companies know where their containers came from, where they're located, where they're going, what's in them, and even how much profit they can expect on any particular shipment.

Under the best of circumstances, importing is a barely controlled form of chaos. Importers must have detailed information about inbound shipments easily available as early in the process as possible. This helps importers make better decisions and leads to increased profits. Obviously, the systems that were developed to provide this kind of return on investment had nothing to do with terrorism. But this same technology, available and in use today, could easily be used to transmit relevant data to CBP, at little or no additional cost to the importer.

Focus on the Bottom Line, Not on Stopping Terrorism.

The private sector is driven by revenue. It will never be motivated by the same issues as government.

A quick look at the selling of C-TPAT to the trade shows that the effort has been focused largely on an appeal to a company's sense of patriotism ("C-TPAT offers trade-related businesses an opportunity to play an active role in the war against terrorism."). Although there has been an attempt to talk about business benefits, these efforts can go further. A benefit should have a monetary value attached (or at least a way for companies to gauge a monetary value). Consider this hypothetical:

The CFO of a chemical importing organization has been asked to investigate what C-TPAT might mean to the company. The CFO visits the CBP Web site and clicks on: C-TPAT Frequently Asked Questions. Here's one of the benefits listed on the actual Web site:

- A reduced number of CBP inspections (reduced border delay times)

That will imply some level of benefit for the CFO, but consider what defining the reduction as a percentage would do:

- C-TPAT participation can reduce container inspections by up to 75% or more.

The CFO routinely pays nearly $9,000 per month for container inspections (the company brings in approximately 300 containers per month and has an average inspection rate of 10%, or 30 containers).

- Each inspection costs the importer $300.
- Participation in C-TPAT can eliminate container inspections by 75%.
- That saves $6,750 per month, or $81,000 per year in inspection fees alone.

That is a business benefit that a CFO can quantify and use to generate excitement about C-TPAT within the organization.

Business benefits from C-TPAT participation.

There are three tiers of C-TPAT certification.

Tier I is attained upon application and submission of the company's security profile documentation. This documentation includes not only your company's security profiles/procedures, but those of the entities that make up your entire supply chain as well. For instance, if you buy from a vendor in China, you must require that they submit documentation of their own internal security procedures to you. If their security were lacking, you would advise which areas need strengthening and ask for a revised policy and documentation. This documentation would become part of your supply chain security documentation.

There are published guidelines to work from, and DHS assigns a C-TPAT Supply Chain Security

Specialist who will work with your company to validate and enhance security throughout your company's international supply chain.

Tier II is attained once the supply chain security has been validated. CBP aims to have this validation complete within one year of the initial registration for C-TPAT. There are limited additional benefits to Tier II certification, including priority processing and reduced ATS scores.

Tier III, or "GreenLane" designation, is attained when companies "demonstrate a sustained commitment beyond the minimum requirements for participation in C-TPAT." One of the most crucial requirements for Tier III is the transmission of non-manifest shipment information prior to a container's loading on a vessel in a foreign port.

There are tens of thousands of importers in the United States. Less than two hundred of them are C-TPAT Tier III certified companies.

Why only two hundred Tier III companies?

Many companies see participating in C-TPAT as unaffordable. They feel that the time and money spent becoming certified is a luxury. Would they like to help in the war on terror? Of course they would. But this is seen as a tremendous burden, and companies feel it is CBP's job to protect our ports & borders. They also fear that they could put themselves at a competitive disadvantage if they participate while their competitors do not.

There are ways to address this concern:

1. Make C-TPAT certification mandatory. This is a horrible idea because it would alienate the trade and could put many, many companies out of business. Additionally, more needs to be done to understand the ramifications of participation before we legislate compliance.
2. CBP could work to be more effective in the selling of C-TPAT. Selling is not the core competency of CBP, but there is no reason there is not an active sales campaign geared specifically to various sized companies in multiple verticals.
3. CBP and the trade could work together to design C-TPAT in such a way that companies will realize obvious benefits and will want to participate in the program.

The third choice is entirely possible and the program could begin almost immediately. Word-of-mouth is the most effective sales technique, and if there were quantifiable benefits, and monetary assistance for companies that have legitimate needs, the program would sell itself. If each side approaches C-TPAT as a work in progress, we will be able to design a system in stages that will benefit business and secure the supply chain.

ATDI: A Dual Benefit Program

The Advance Trade Data Initiative (ATDI) is an Automated Commercial Environment (ACE) program developed to receive the advance shipment data described above. ATDI was conceived as a way for non-manifest shipment data to be shared with CBP well before the goods are

placed on a ship in a foreign port. Information on the manufacturer or vendor, inland drayage, importer, shippers, even product information like certificates of origin and certificates of analysis are obtained by the importer during the normal course of business and transmitted to CBP. CBP presumably feeds the information into its Automated Targeting System, and ATS uses the data to identify higher-risk containers for closer inspection.

But remember, the importer needs the same information as early in the transaction as possible to ensure the financial success of the transactions. This level of understanding of the supply chain will allow importers to run leaner inventories, eliminate errors caused by multiple data entry, understand exact costs, and see profit and loss at the shipment level. It will help importers make better decisions and better decisions will lead to increased profits.

This business model achieves a dual benefit; higher profits for the importer and better information for CBP (ATDI is a C-TPAT Tier III best practice). It is a classic win-win formula.

How does ATDI work?

The preferred way to submit the information has been by converting the relevant import documents to a digital format recognized by CBP's computers. There are two challenges associated with this. The first is that importers are very reluctant to provide copies of their purchase orders and other documents. It's not clear that this is necessary anyway since the systems discussed above could more easily provide the individual data elements without transmitting entire documents.

The second, closely related challenge has to do with the sheer amount of data being transmitted. There could easily be 50 pages of documents from which the data is extracted. Multiply that by 60 million product shipments during the course of a year and it's an enormous amount of raw data. That's an awful lot like looking for needles in a haystack.

A modern importer's software system can provide the needles without the haystacks.
The data is fed into CBP's Automated Targeting System, where it is co-mingled with other data collected by CBP. That data might include intelligence bulletins about specific threats, or products; things an importer would be unlikely to know. The expectation is that ATS will leverage all the data to identify shipments that should receive additional inspection such as non-intrusive scans, and hands-on searches.

OTHER ISSUES

Although C-TPAT has been one of the more successful post-9/11 initiatives, there are still significant challenges to be met. One is each side's understanding of the other's position. For instance, it's one thing to call for the submission of non-manifest data, but CBP has to understand why it's dangerous for an importer to share product sourcing information without iron-clad assurance that the information will be protected. An importer's entire business is sourcing, and when they give up these documents, they give up their most closely guarded trade secrets.

There is also concern that the data may be used by other government agencies such as the IRS, to monitor a company's business practices. Although CBP has stated that the data will be protected from any other use, they must recognize that the PR battle is on-going and devote resources to bringing more companies into the C-TPAT fold.

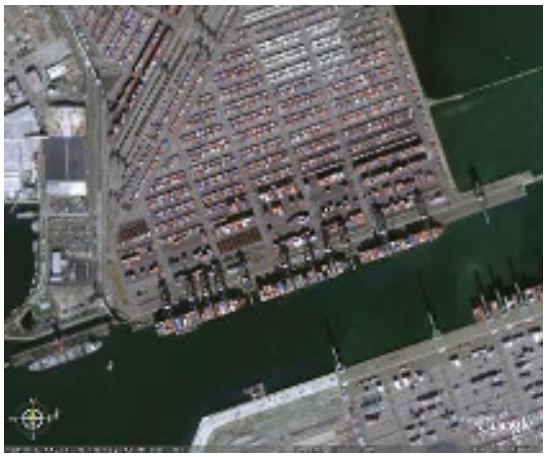
How much would this cost?

Because the most profitable importers are already collecting and managing the exact data CBP needs to secure the supply chain, the costs are negligible for those companies. Companies without the capabilities needed to manage and submit the data would need to upgrade their infrastructure in order to participate with the same effectiveness. Once the infrastructure is there, the program would have a minimal footprint.

Either way, the improved business models would produce a high return on investment even as companies complied with more stringent government regulation (again, a win-win). With hundreds of millions of dollars being spent on container/port security, there are surely resources to continue these programs, and to assist companies as they make the changes we all know must be made.

Next steps.

It is time to bring more companies into the fold through participation in C-TPAT. Since ATDI provides the data deemed crucial by CBP, we must make the program stronger. One essential project



that has been discussed is the creation of a "master database" that would hold information common to all importers. This would allow standardization of information on such things as ports, both foreign and domestic. This information could then be made available to companies preparing for submission of a security profile, simplifying the process and ensuring that information is standardized across the C-TPAT user base.

Profitable compliance through partnership.

It is naïve to think that the global trade community or the government can afford to wait to address the profound vulnerabilities in the global supply chain. The cost of complacency could be nothing less than world-wide depression. We can leave it to politicians and the public to tell us how our business will be run (as was the case in the Dubai Ports World episode), or we can do what we know is right by taking steps to secure the global supply chain now, with the tools that are already available.

But success will take a true partnership between government and the trade. And that will take courage from everyone involved. The tools to secure the supply chain are the same as those needed to increase profits. This could be the first time that more stringent government regulation, or the threat of more stringent regulation as the case may be, leads to increased profits.

Better business is safer business.

www.viscosoftware.com