



Good Management Trumps Good Luck When It Comes to Security

Protecting your supply chain
in a post-9/11 world requires
proactive preparation.

By Thomas A. Cook

My business is helping companies compete in world trade and I have been engaged in this activity since 1971. While my practice has witnessed change over the past thirty years in how global sales, customer service and supply chains operate, there remains a basic premise that holds true today in a post-9/11 compliance and security trading environment. Call it 'Cook's Law': it is that those firms that are "proactive versus being reactive" in how they deal with the *inevitable* will do better in not only being successful but in creating a better foundation to manage global trade in.

The events of 9/11 changed how all of us think about security. For starters, it made the American Government, led by various agencies like Homeland Security, Customs Border and Protection, Bureau of Industry and Security, and The Transportation Security Administration to name a limited few, to more carefully scrutinize the global supply chains affecting trade to and from the United States.

In the wake of these post-9/11 scrutinies, it became very evident to the government that the security of supply chains needed to be prioritized and more importantly, tightened up. Correspondingly, we've seen a host of new regulations and initiatives. There's the Patriot Act, Export Administration Act, Bioterrorism Act, 24-Hour Manifest Rules, Focused Assessments, Free and Secure Trade Initiatives, and a veritable litany of acronyms like

C-TPAT, FAST. No surprise, some of these have been carefully thought out and others more hastily conceived in a kind of administrative 'knee jerk' response.

It awaits the test of time to see if compliance with these efforts will work. But regardless of one's opinion, these new regulations are here and they affect how we manage our supply chains. Which brings me back to Cook's Law.

Those of us engaged in supply chain activities have choices, both as individuals and as corporations, about how we want to respond. If we are 'reactive' to the regulatory climate that now prevails, we will be captives to the process with unknown consequences and uncontrollable costs. By doing only what is required one risks being limited to minimal standards of acceptability. On the other hand, if we are proactive--if we tailor compliance programs to respond not only to explicit security considerations but also to improve the performance of supply chain processes as well--we will better control the destinies our imports and exports and seriously reduce the costs, the exposures, the fines and penalties and the ultimate loss of the supply chain becoming disabled.

Amidst the extensive discussions and analyses of security compliance, there is a more fundamental question running through the conversation: do you choose to run your company by "good luck" or run it by better management?

In over thirty years of helping companies compete effectively in importing and exporting, it is clear to me that

The 8 Step Best Practices for Managing Risks of Terrorism

1. Awareness

Supply Chain executives must become aware of what all the issues are and how they might affect the specific import and export supply chain for which they are responsible. Being reactive after the fact will cause delays, potential fines and penalties and extra costs, typically unanticipated nor budgeted. Awareness means having a consistent inbound flow of information and developing resources to know what the issues are, the most recent modifications and ultimately what options of response are available.

2. Information inflow

Information inflow is as important a skill set as knowing how to get goods cleared by Customs in China or dealing with the FDA in the United States if we bring in food, pharmaceuticals, or related merchandise. An enterprise needs to be able to drill down deep enough into its global supply chain to be able to identify lower tier suppliers, all of whom can have an effect on the security of the flow.

3. Senior management support

Compliance, security and terrorism issues cross all the boundaries of a corporation. Finance, legal, customer service, operations, logistics, traffic management, inventory, purchasing, manufacturing, and even marketing have a stake in securing the supply chain.

The nature of most organizations is to resist change, even when such a

vital issue is at stake. Thus it is imperative that senior management sponsor and support security initiatives to break down internal resistance. Simply stated, those supply chain initiatives that carry senior management support will have a much more likely opportunity for successful implementation than those that do not.

4. Analysis and review

The process to determine actual conditions and exposure is to conduct a facilities review, detailed analysis and mock audit of your supply chain and operations. Typically, this is best accomplished by engaging an independent consultant—an objective third-party analysis without specific internal agendas is most likely to generate valid “benchmarks” for where your company is. A facilities review can also access the relationships to vendors, providers, carriers, forwarders and brokers.

In conjunction with this review is the development of a “blueprint” for actions to be taken. The review and scrutiny also satisfies the government’s requirement of exercising due diligence, reasonable care, and supervision and control.

5. Individual and team responsibility

Irrespective of the size of the corporation or the complexity of its supply chain, one identifiable person should be responsible for managing the risks of terrorism, compliance and security. This person can be part of any profit

or cost center (logistics, manufacturing, purchasing, legal/regulatory, etc.) as long as they have the skill sets necessary to manage the job.

We recommend, though, that this person work within a team context drawing on members from all profit

a written format, which clearly outlines how a company will function in its supply chain; they then become a benchmark to meet the government’s requirements of exercising due diligence and reasonable care; and they provide

“Compliance, security and terrorism issues cross all the boundaries of a corporation. Finance, legal, customer service, operations, logistics, purchasing, manufacturing and even marketing have a stake in securing the supply chain.”

and cost centers, divisions and disciplines.

This will best be accomplished by creating a *plan of action*.

6. Action plan

Once the analysis is done and the compliance person chosen, an action plan with appropriate monitoring techniques will have to be developed. There are variations on task management programs, but we advocate a simple four-column approach that lists the action, the date to be completed, the responsible party, and the current status. The action plan flow chart needs to be accessible to all members of the team in order to align collaborative efforts.

7. Standard operating procedures

The importance of SOPs are three fold: they commit the process to

guidelines for subsequent personnel to follow.

In addition, these guidelines will contribute to a public company demonstrating its compliance with Sarbanes-Oxley Regulations.

At various government websites (www.cbp.gov and www.bis.doc.gov) are guidelines established by agencies put forward as starting points and benchmarks for creating SOPs.

8. Training and education

A cornerstone of any compliance and security program is having all the supply chain personnel specially trained, at a minimum, in the basics of compliance and security. Among the categories that require training and education are classification, valuation, record keeping, red flag management, documentation and denied party screening.

those enterprises able to assess their situations and then proactively deal with a range of potential impending disruptions are those that do well. On the other hand, companies that seek to falsely economize by cutting corners and being blind to the real-world implications of current events by being reactive to their environments are likely doomed to uncompetitive supply chains, loss of revenue and profits in the short-term and in the long-term even the ability to operate viably.

Here are some vivid examples.

Take the hundreds of companies that receive tens of thousands of dollars in fines every year for selling goods to overseas entities that are on the Department of Commerce List of Denied Parties. They had a choice

to be responsible and check the list prior to engaging in the export transaction or get caught and suffer the consequences (fines, loss of revenue and possible loss of export privileges).

Take the hundreds of companies that are audited by Customs and Border protection that receive millions of dollars in fines and penalties for violating common practice errors in valuation, record keeping, classification or documentation. They had a choice to exercise reasonable care and due diligence or suffer the consequences.

Take the over twenty thousand companies that are eligible to participate in Custom’s trade program C-TPAT, Customs-Trade Partnership Against Terrorism, but have not yet executed applications. What will happen to these

companies following another terrorist attack? The borders will close for all companies, but might only open for those who are C-TPAT Certified (meaning that those who are not are rolling the dice when it comes to their supply chain).

In all fairness, the issues are not simple. I currently see a growing concern among global supply chain executives in how best to deal and manage all these post-9/11 compliance and security regulations and initiatives. My best 'guesstimate' is that a third of them are going to be proactive, leaving two-thirds either complacent or non-reactive at all. The implications for the latter two-thirds strike me as particularly dire.

RFID, radio frequency identification, is a good example. There is a "charge" being led by many large retailers to have all vendors provide RFID capabilities that interface with their supply chain IT capability. RFID adds significant cost to the supply chain, specifically to the product unit and the technical infrastructure to maintain a RFID system. Many companies are reluctant to make such an investment, particularly in the absence of viable "business models" that can show a return on investment.

We have studied this matter the last 15 months and have identified numerous potential security and compliance benefits to RFID. We have also observed the government (specifically Customs Border and Protection, Coast Guard, Homeland Security) who are testing RFID advancements to potentially incorporate this technology into Global Supply Chain security. In addition, many pharmaceutical companies now believe that RFID can assist them in product trailing and preventing tampering. In addition, cargo seal manufacturers are working with authorities to see if RFID can provide a better security seal for ocean freight 40' and 20' steamship containers.

We believe there are hidden benefits in terms of supply chain security which provide an added opportunity for return on investment which might not show up in more conventional ROI analyses.

Most professionals feel the window of opportunity to initiate proactive steps to secure the supply chain remains open—perhaps for another 12-18 months. By then, however, the probability of disruption is likely and, with it, rigid control of supply chain activity for non-compliant companies. As I travel around the country, I see more and more companies recognizing their vulnerabilities and primed to engage in compliant security initiatives.

That's the good news as the process unfolds. The 'less

Where to Get Help

We are observing more companies creating positions in supply chain or import/export compliance and security than at any other time. To facilitate this process, the Professional Association of Import and Export Compliance Managers, www.compliancemaven.com, based in New York City with representation throughout the United States, has developed a program of seminars, testing and certification of supply chain managers. This association teaches the skill sets for personnel who have compliance and security responsibilities and offers instruction to help companies meet the standards of exercising due diligence, reasonable care and internal training and education.

"As I travel around the country, I see more and more companies recognizing their vulnerabilities and primed to engage in compliant security initiatives."

good news' is that many enterprises remain uncertain what they should do or how to begin. The Professional Association of Import and Export Compliance Managers (PACMAN, www.compliancemaven.com) reports a doubling in membership and certification of its membership in the last 12 months. The World Academy (www.theworldacademy.com), based in New York City, reports a four-fold increase in student census in all their classes on compliance, security and import/export supply chains.

I firmly believe that the more astute supply chain executives that I have interfaced with representing such companies as Pall Corporation, Amgen, Engelhard, Estee Lauder, BMW, Bobst Corporation and Linens 'n Things, have identified significant benefits in improving the efficiencies of their supply chains in tandem with compliance and security initiatives. Various proactive steps they have initiated in compliance with security regulations have actually enabled their supply chains to run better, more cost effectively and more responsibly.

Every study we have done suggests that there are certain typical steps in the security compliance

process, which enable the supply chain not only to be safer but also to operate better. The U.S. government agencies engaged in managing compliance and security all require companies to exercise "due diligence and reasonable care."

The importance of self-audit

The ultimate goal of this whole process outlined in the Eight Steps is for an enterprise to run its global supply chain compliantly and securely on an independent basis. This means that the company can self-audit import and export operations and feel confident that its personnel, SOPs and operations will run in accordance with the new post-9/11 regulations.

Customs has put forth an initiative called the ISA, or Importers Self Assessment program. Upon demonstrating a capacity to self-audit and self-regulate in compliance with U.S. Customs and Border Protection's standards, the firm is granted ISA status. Such status will significantly reduce the extent to which the firm will be scrutinized on a day-to-day basis by Customs. **wt**

Thomas A. Cook is Managing Director of American River International, Ltd., and can be reached at tom@worldest.com

For reprints of this article, please contact Jill DeVries at devriesj@bnpmedia.com or 248-244-1726.