Supply Chain SECURITY *in a* high-risk world

An Interview with Barry Brandman of Danbee Investigations

Logistics Management's sister publication, *Supply Chain Management Review (SCMR),* interviewed security expert Barry Brandman in its July/August 2003 issue, not long after the creation of the Department of Homeland Security. The threats to the security of supply chains have certainly not abated since that interview; if anything, they have only intensified.

So now seems to be the perfect time to revisit the subject of supply chain security. And, once again, Barry Brandman is the go-to guy. Brandman is president of New Jersey-based Danbee Investigations, which provides professional investigative, auditing, and security consulting services to hundreds of major companies.

Brandman has developed a particular expertise in logistics and supply chain management. He's a frequent speaker at industry conferences such as CSCMP and the International Conference on Cargo Security. He also has authored articles on supply chain security for a wide range of publications.

The underlying message in this current interview with Brandman is clear: In a high-risk world, companies must be proactive when it comes to supply chain security; to be otherwise, invites a host of serious and potentially devastating consequences. *SCMR*'s Editorial Director Francis J. Quinn conducted the interview.

Q: *Since our last interview almost seven years ago, have North American companies become more proactive about supply chain security? Or, are they still largely in a reactive mode?*

A: I see companies being more proactive today, especially those that have been victimized in the past. When a company has a major theft, fraud, product tampering incident, or any other type of security problem, the human and financial resources needed to deal with it are usually quite significant. It's not a good experience and most executives want to do everything possible to avoid having history repeat itself. Being proactive is the best way to do that.

Q: *As supply chains grow larger and more complex, what added pressure does this put on cargo security integrity?*

A: Security today has become a greater challenge because there are more opportunities in a complex supply chain for theft, smuggling, and product tampering. The objective is to develop, introduce, and then diligently maintain asset protection continuity within each link of your supply chain. This isn't easy or simple to do when you're working with a global logistics network.

One major problem in this regard is that many foreign entities don't accurately represent what their supply chain safeguards really are when questioned by American importers. This is sometimes due to language barriers and other times the result of not understanding how to properly implement security safeguards.

One overseas manufacturer, for example, had assured our importer client that the ocean containers they were shipping to the United States were being properly sealed in accordance with the security standards we had designed for them. While conducting a security audit at their site, however, I witnessed shipments leaving the manufacturing facility without a security seal being affixed to the containers. When I questioned the shipping manager, he explained that because Chinese customs officials occasionally detached the security seals for cargo inspections, the manufacturer simply began handing seals to the drivers and asked them to attach the seals after they passed through China Customs.

While the manufacturer believed that they were adhering to our policy, these shipments were vulnerable to theft and smuggling because drivers had uncontrolled access to the cargo area of every container. Although China Customs only inspected approximately 5 percent of their shipments, this manufacturer completely abandoned the security practice they had previously agreed to follow—instead of consulting with us for a better solution. Consequently, a huge vulnerability existed.

Our client obviously didn't know that truckers were affixing the security seals until they received our audit report. It was no coincidence that shipments from this manufacturer were regularly arriving to U.S. distribution centers with shortages. Not surprisingly, when we changed their sealing practices, the shortages immediately stopped.

Q: *What are the security threats that companies typically overlook or pay insufficient attention to these days: physical theft, cyber theft, product integrity, terrorism?*

A: Today, successful companies are genuinely concerned about all aspects of their security. Theft of property or proprietary information, product tampering, inventory theft, fraud, sabotage, and terrorism can dramatically affect a company's profitability and reputation in the marketplace.

The problem is that executives oftentimes assume that their company is far better protected than it actually is. Unfortunately, only after they've been victimized do many companies learn how vulnerable they actually were.

Q: *What are some warning signs suggesting that a manufacturer, distributor, supplier, or a logistics provider may be vulnerable when it comes to their security practices?*

A: I find that companies experiencing security problems typically have made one or more of these three mistakes.

One: They have security assessments performed by people who are lacking in any meaningful expertise or experience

PHOTOGRAPHY: GARY PEYTON

in logistics asset protection. As a result, they fail to detect areas of risk and therefore cannot remedy their vulnerabilities.

Two: Their security audits are conducted using generic checklists. Most security programs look better when viewed from a distance. Prior to Sept.11, 2001, security at American airports appeared adequate. There were guards, video cameras, metal detectors, and other components in place. However, if you had examined the real effectiveness of these safeguards, you would have exposed a number of weaknesses. These vulnerabilities were exploited then and on several occasions since 9/11.

This appearance versus reality problem exists in the private sector as well. Using checklists to superficially evaluate the effectiveness of a company's security program is not a good practice. And many companies have paid the price for failing to recognize this.

A *third* major trouble signal is a failure to make regular improvements—or even conduct basic reviews—to the company's security program. In such cases, the company is not utilizing the very best security practices, and what safeguards that may be in place are typically ineffective.

"No technology acting alone will adequately protect a supply chain—regardless of how sophisticated it may be."

Q: *Can you give an example of how these missteps play out in the real world?*

A: A good illustration of how they can get a company into trouble can be seen in the litigation between a third party logistics warehousing company and their customer. The customer in this case was a major manufacturer that had become aware that its inventory was being sold in large volume on the black market.

The manufacturer conducted a confidential investigation of the situation, without the 3PL's knowledge. It found that the 3PL's general manager was directly involved with the theft of truckloads of inventory from the distribution center he was responsible for. The customer was outraged and subsequently sued the 3PL for the stolen inventory and for the investigative and legal expenses incurred, which totaled seven figures.

The 3PL's legal defense was that they had exercised a reasonable standard of care, noting that they had electronic intrusion detection and video systems in place, as well as a guard on premises whenever they were open for business. Plus, they claimed that every time their facility had been audited it had received near-perfect scores for security. On the surface, it appeared that the 3PL had implemented sound protective controls.

The manufacturer's attorneys retained us as their expert witness to objectively analyze the 3PL's security program. What we subsequently found was that their security controls were purely cosmetic and totally ineffective. To begin with, the 3PL's general manager, who was the ring leader, had full control of the intrusion detection and video systems. Because there was no independent inspection of the opening and closing alarm system reports, or independent viewing of archived video activity at this distribution center, the dishonest GM simply eliminated the evidence of all the thefts that these systems had archived.

The guard service proved to be no deterrent because they reported to the general manager. One of the security officers had suspicions about the GM and reported them to his office. Yet the company providing the guard service did not want to make unsubstantiated accusations because it feared that the GM would terminate the contract if the allegations proved untrue.

With respect to the near-perfect internal audit scores introduced as proof that the 3PL's security controls in place were sound, we had no difficulty undermining their real value. In particular, we pointed out that all of the audits were conducted by quality control personnel with no real security experience or specialized training.

Additionally, their auditors were using checklists that glossed over many of the important functions that should have been examined far more thoroughly during the onsite assessments. For instance, two of the questions on their checklist were, *"do you have a working alarm system* and *"are the alarm system activity reports regularly reviewed?"*

Instead of the QC auditors actually knowing how to test the onsite security technology or personally examining the activity reports, which would have revealed that the intrusion detection system had been repeatedly compromised, they simply asked these questions of the GM. Naturally, the GM answered in a less than candid manner. The auditors simply accepted his statements as being truthful and checked off the boxes on their forms.

In short, the audits were nothing more than an exercise in pencil-whipping that gave executives at the 3PL's corporate offices a false sense of security and left their inventory vulnerable to theft.

After the 3PL's attorneys understood the real value of the protective policies and practices that were in place, they decided to make a settlement with the manufacturer rather than risk a verdict in court.

Q: *What technology is available today to accurately track chain of custody and ensure product integrity? How effective is it?*

A: While progress is certainly being made, I've yet to come across an extremely reliable, cost-effective solution that can track cargo moving through an international supply chain. However, I think this technology will become a reality in the future.

Until such time that electronically reliable, cost-effective technology is on the market, companies need to make certain that they combine the right equipment with best security practices. No technology acting alone will adequately protect a supply chain—regardless of how sophisticated it may be. I think that executives sometimes wait with anticipation for new technology to surface, hoping that it will be a cure-all for their security concerns. The reality is that high-tech devices will always need to be supported by smart practices and procedures.

Also, you don't need the latest technology in every aspect of your supply chain to keep it secure. As an example, if a company in Hong Kong is shipping an intermodal container via ocean liner, they can still have very tight chain of custody providing they utilize a high-security bolt seal, make certain that there are diligent seal control procedures in place, and have inspections conducted at each point in the transit route. Just because the seal doesn't have an embedded smart chip with RF communication doesn't mean that your shipment has to be vulnerable.

Q: *What's the connection between supply chain security and customer retention and loyalty?*

A: As a result of several factors, such as compliance with C-TPAT (Customs-Trade Partnership Against Terrorism), the popularity of just-in-time logistics, and the increased risk of theft and terrorism, there is greater emphasis than ever before on protecting a company's supply chain. Today, global logistics is about speed, reliability, product integrity, and cost containment—all of which directly affect profitability and customer retention. The industry leaders have found that having world-class security programs directly benefit all four of these critical areas.

"The reality is that high-tech devices will always need to be supported by smart practices and procedures."

Let's examine what could happen to a company that fails to adequately protect their supply chain. If their security is breached, and law enforcement discovers a large quantity of smuggled narcotics in one of their shipments, this company will likely experience a dramatic increase in the number of government inspections of *all* their imports for an extended period of time. This will not only slow down their supply chain and jeopardize delivery deadlines to customers, but also increase their operating costs. Additionally, this company will incur considerable time and expense interacting with law enforcement officials in the aftermath of this incident.

On top of all this, the publicity that could be generated in the media over the incident can negatively affect the company's reputation in the marketplace as well as their stock price. The end result is that current or prospective customers may not be so eager or comfortable doing business with that company.

Q: *What are the potential supply chain impacts of an attempted or actual terrorist attack on cargo destined for the United States?*

A: Intelligence sources have reported that the commercial supply chain remains a prime target for terrorist organizations because of the volume of shipments sent to the United States as well as the fact that an act of commercial terrorism would have significant consequences.

The last thing any of us want, of course, is another 9/11. The loss of life is obviously everyone's number one concern. However, I believe that an act of terrorism also has the potential to ignite a global financial crisis, especially in these economic times.

To illustrate, let's say the United States government closes our ports for an extended period of time in response to a terrorist act, and imports are kept waiting in limbo on ships, trucks and planes at our borders, as well as at ports throughout the world, because they cannot offload their cargo in the States. This would result in a domino effect that would directly affect foreign manufacturers, consolidators, and carriers as well as U.S. importers, distributors, and retailers. In essence, the supply chain would become frozen and the economic consequences would be felt immediately.

Q: *Is mandatory screening on all cargo coming into the United States inevitable?*

A: It's not easy to find the right balance between security, cost, and facilitation. The TSA (Transportation Security Administration) has been attempting to find this balance for the flying public for nearly 10 years and it is still struggling to come up with the right equation. Remember, the U.S. imports over 20 million conveyances each year. Even if we reach the objective of 100 percent cargo screening, the real question becomes how thorough and effective would that screening process actually be?

Q: *Has C-TPAT succeeded in its goal of keeping harmful shipments out of the U.S.?*

A: The C-TPAT program has been extremely successful in two critical areas.

First, there has not been a weapon

of mass destruction smuggled into the United States as a result of the commercial supply chain being breached, despite efforts by terrorist organizations that are determined to do so. I think C-TPAT justifiably deserves a good deal of the credit for this accomplishment. Second, because of C-TPAT, thousands of companies have been motivated to re-evaluate their supply chain security programs and continue to seek ways to better protect their goods. This not only safeguards these corporate entities, but also the American public.

in wage freezes, reduced shift hours, overtime being eliminated, and layoffs. Stock options are worth less and retirement accounts have lost value. Faced with financial pressure, less income, and the threat of job elimination, company loyalty has been negatively affected.

Some of the dishonest workers (both white collar and blue collar) that Danbee Investigations has apprehended over the last two years had no misgivings whatsoever about stealing from their employers, rationalizing that they were simply taking what they were entitled to. In some cases, there was resentment about the austerity measures that had been put in place, and these employees adopted an "us against them" mentality.

"If C-TPAT didn't provide tangible security, logistical, and financial benefits, it wouldn't be replicated by so many other countries and embraced by the business community."

C-TPAT offers an array of financial and logistical incentives, which is why 10,000 companies have joined the program to date. C-TPAT's annual conference is sold out within hours of registration being opened and mutual recognition agreements are being signed with other countries who are adopting C-TPAT-like programs.

Very few companies have voluntarily given up their C-TPAT certification and walked away from the program. In fact, most of the firms that are no longer in the program have had their certifications suspended or revoked.

If C-TPAT didn't provide tangible security, logistical, and financial benefits, it wouldn't be replicated by so many other countries and embraced by the business community. Remember, C-TPAT is a voluntary program. So 10,000 members in less than 10 years is impressive.

Q: *You have said that employee loyalty has become a greater problem these days. What's the reason for this and how is this related to security?*

A: Most security experts agree that one of the reasons for the spike in both white and blue collar crime over the last two years is the recession. The economic downturn has resulted

Q: *What's the single most important action that companies can take today to improve their security and minimize the threat of supply chain disruption?*

A: I think there are actually two key actions.

The first is to become more proactive, rather than being reactive. Don't wait to be victimized to learn that your security safeguards can be circumvented. The most successful companies today are having comprehensive risk assessments and audits performed to expose their security vulnerabilities before others have the opportunity to exploit them.

Second, I would advise companies to be more realistic in terms of assessing the quality of their existing loss prevention programs. There's a difference between not being victimized because your security program is very good versus not being victimized simply because you've been fortunate. Just because you haven't had a problem doesn't necessarily mean that you have an excellent asset protection program. In today's high risk world, relying on luck is not a smart security strategy.

Q: *What can supply chain managers do to jump start the conversation—and action—about better supply chain security in their organization?*

A: I think that reducing overhead and increasing company profitability are always compelling points to raise in advocating better security. The example I previously gave about the company having their supply chain breached and unknowingly having their shipments used to transport narcotics is an actual case we handled for a large American importer. The costs associated with all the remedial actions they ended up taking—the legal, consulting, and investigation expenses as well as the interruption to their supply chain—were all unexpected and unbudgeted. Their bottom line took a hit that fiscal quarter.

Much of the same financial exposure exists if a company's product is stolen or tampered with. Consequently, companies almost always find that being reactive is much costlier than being proactive. Proactive security equates to risk mitigation, the value of which most executives fully appreciate. No one cancels their fire insurance because none of their facilities have recently burned down. They accept the fact that protecting their company from unexpected risks like fire or flooding is a necessary cost of doing business. When you analyze it, that's exactly what an excellent supply chain security program does while also allowing a company to operate more profitably and with greater efficiency.

In this competitive business environment, the chances are that one or more of your major competitors already understand this and are taking the needed steps to make sure their assets are well protected. If you want to remain competitive, you'll need to do the same. □

Barry Brandman can be contacted at bbrandman@danbeeinvestigations.com