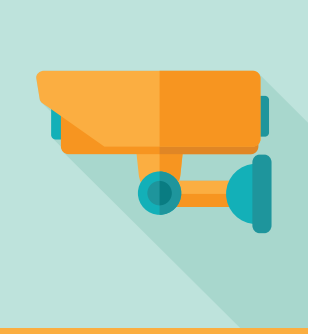
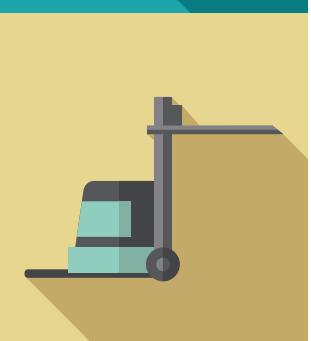

2:0





BY BARRY BRANDMAN
PRESIDENT
DANBEE INVESTIGATIONS

SUPPLY CHAIN SECURITY: PLAYING IT SAFE

DOES YOUR CURRENT ASSET-PROTECTION PLAN PROVIDE A FALSE SENSE OF SECURITY?

Protecting today's corporate supply chain is a complex challenge. The more than 20 million conveyances arriving to the United States each year, and the number of times these shipments are handled both internationally and domestically, create many opportunities for illegal activity to take place. Professional crime rings, dishonest employees and contractors, and terrorist groups are all real threats that we must take seriously.

Organized crime groups that target logistics companies are responsible for hundreds of millions of dollars of loss annually, while employee-related theft is estimated to exceed $10 billion each year.

Since Sept. 11, 2001, terrorist organizations have made numerous attempts to penetrate the commercial supply chain, and recent geo-political events indicate that this risk may increase. Should a terrorist group manage to smuggle a biological, chemical, or nuclear weapon of mass destruction into a shipment, the ramifications could be catastrophic in terms of loss of life, as well as the financial consequences for the victimized company.

Today, the majority of importers, freight forwarders, consolidators, distributors, carriers, and manufacturers understand the importance of mitigating their exposure to these threats. Despite the emphasis on having effective asset-protection safeguards in place, why is it that so many companies are still victimized each year?

Tight security controls can prevent a breach, such as narcotics being hidden inside cartons of finished goods.

REALITY CHECK

Here's a simple truth when it comes to supply chain security: Most business asset-protection plans look much better on paper than they actually work day to day.

Many companies that have not been victimized, or were just not aware that they were having security problems, were lulled into complacency. As a result, they wrongfully assumed that their loss-prevention program was far more effective than it really was.

Only after having a major security breach that couldn't be ignored were a large percentage of these companies forced to face the harsh reality that their safeguards were nowhere near as robust as they had assumed they were. Unfortunately, learning this after a significant security breach can be an extremely costly lesson.

One example involved a distributor that experienced a break-in while its facility was closed. This resulted in an inventory loss of more than $8.2 million. Professionals carried out the theft by entering the building after cutting a hole in the distribution center roof, climbing down a rope ladder, and then dismantling the control panels of all the electronic security systems. The distributor only became aware of the theft when the day shift employees reported to work and found that all the inventory had been removed from several aisles of racking that were full just eight hours earlier.

Company executives were shocked because their facility had never suffered a loss in 17 years at this location. They assumed that their alarm and video systems were more than adequate for preventing this type of unauthorized entry.

The reality is, they were simply fortunate that a professional crime ring had never targeted their facility prior to this event. When their luck ran out, however, they were rudely awakened to the deficiencies of their electronic security systems, which the thieves had easily compromised.

Not only did a vendor sell the distributor the wrong security technology, but the forensic investigation also determined that the vendor had improperly installed and programmed some of the equipment. The professionals who attacked this distribution center had no difficulty circumventing the intrusion detection equipment and cameras, and spending several hours inside the facility loading the distributor's inventory into their tractor-trailers.

Another example of a victimized

Product tampering, terrorism, smuggling, and diversion are just a few security threats that can negatively impact not only a company's reputation, but also its bottom line.

company having a false sense of security involved a foreign freight forwarder that had a shipment seized when narcotics were found hidden inside cartons of finished goods. We were asked to conduct a post-event security assessment; one of the primary objectives was to determine how the forwarder's controls were breached and what it should do to prevent a reoccurrence in the future.

The company's senior management had always believed they had tight security policies and procedures in place. They pointed out, for example, that they kept the cartons of finished goods that contained the concealed drugs in a secured section of their building with access strictly limited to only a few highly trusted employees. Additionally, when the product was shipped to the local seaport, the cargo containers were always secured with high-security tamper-evident seals. Consequently, they were puzzled as to where and when the smuggling could have occurred.

CAUGHT UNAWARE

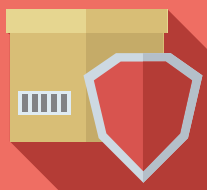
However, an investigation revealed several breaches in security policies and procedures that the forwarder was unaware of.

The managers were convinced that the high-security area of the warehouse was well protected with an electronic lock that required an access control card to open, and only three highly trusted workers had the ability to enter this area. An investigation found, however, that for convenience, these employees repeatedly left the entrance gate open for long periods, and had also dismantled the prop alarm on the gate because they found the siren annoying, thereby neutralizing any benefit that the access control system provided.

Consequently, other warehouse employees had the ability to enter the high-security area. That's exactly what was taking place, and was one of the ways that the drugs were being hidden inside the product cartons.

No one in management was aware of this because the video cameras monitoring the high-security area provided poor clarity and were seldom viewed. Although uniformed guards patrolled the facility, the officers became friendly with many of the

Loss Prevention Best Practices

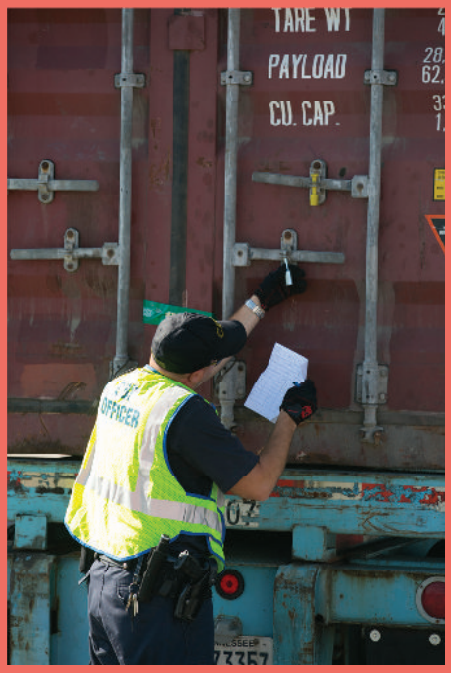


The most successful loss prevention programs incorporate the following best practice strategies and tactics:

Implement a security program that is far more proactive than reactive. It's not a question of whether an incident will occur; the real questions are where it will take place and how costly it will be. That's why focusing on effective safeguards that prevent problems from occurring, rather than reacting after an incident, is typically a more cost-effective approach to protecting a company's assets.

Design your supply chain security program with multiple checks and balances. There is no silver bullet. The truth is, no one solution, whether a practice or type of technology, will protect your supply chain from risk. World-class security programs always utilize a layered approach, with numerous checks and balances in place in the event that primary safeguards fail or are compromised. In some high-risk countries, or when handling product that is extremely valuable, you'll find not one but multiple checks and balances embedded into the chain of custody controls.

Companies importing shipments from Mexico to the United States, for example, should have as many as six, eight, or even 10 backup safeguards in place, with each acting as a safety net in the event the others are circumvented.



Best practices, such as using durable cargo seals, can ensure that goods get to market safely and without interruption.

Combine the right technology with your policies and procedures. If you find and utilize the right technology, and integrate it into your asset-protection program, it can provide significant value. Some examples include covert GPS devices that are hidden inside shipments, and high-definition digital cameras that can be remotely viewed from anywhere in the world. Exercise caution, however, as some security equipment vendors will over-hype their product's capabilities and/or offer technology that is not applicable to your specific needs.

Take an MRI of your company. If you have reason to suspect security problems, or simply want to know how your business is really operating, undercover has proven to be a good solution. Seeing your company from the perspective of an insider can provide comprehensive intelligence on a number of issues, including internal theft, workplace substance abuse/distribution, lax supervision, non-adherence to company policies and procedures, and morale issues.

An undercover investigation can also provide insight on the effectiveness of your safeguards by identifying exactly where security deficiencies exist.

workers and were reluctant to write them up for security violations such as lax adherence to the access control policies.

The investigation also exposed significant vulnerability in the transportation controls. Although the executives explained that every container moving to the seaport was secured with a high-security bolt seal, the investigation found that the dock supervisor routinely handed the seal to departing drivers, and allowed them to secure it to the rear door of the container.

Further investigation revealed that one dishonest driver was surreptitiously pocketing the seal the dock supervisor gave him, and affixing a different seal (one that he arrived with) to the container door. After departing the facility, the driver parked in a deserted area, removed the substitute seal he had affixed, entered the cargo area, and concealed contraband inside certain cartons. He then closed the rear container doors and applied the high-security seal he had been given by the dock supervisor—the one that should have been affixed at the shipping dock before he departed. Although the seals were of good quality, the freight forwarder's procedures for controlling and handling them were weak, and therefore able to be circumvented.

COSTLY MISTAKES

Victimized companies are often guilty of making certain mistakes that result in significant security breaches.

One of the biggest missteps is to assign responsibility for conducting loss prevention audits to personnel who lack meaningful asset-protection experience. If auditors don't have expertise in logistics security, chances are slim to none that they will be able to find the weak links in a company's supply chain. Just because individuals have quality control or safety auditing experience does not mean they are qualified to conduct security audits.

Another common mistake is for those conducting security audits to use generalized, over-simplified checklists that they find on the Internet. Using these types of checklists typically results in a cosmetic, rather than in-depth, examination of a company's security policies, practices, and technology.

It's important to keep in mind that the objective of a security audit is to expose and remedy vulnerabilities before those with bad intentions can exploit them. The only way to accomplish this is by going beneath the surface, because when it comes to security deficiencies, the devil is often in the details. Audits need to dig deep in order to expose these deficiencies, and this cannot be accomplished by simply pencil-whipping a generic checklist.

Another costly mistake is allowing an asset-protection program to grow stale. Most supply chains are dynamic, and logistics and security threats are constantly evolving. Unless a company perpetually analyzes and updates safeguards, ensuring that the latest best practices are in place, its risk factor will be much higher than it should be.

A wide range of risks threatens the security of freight moving into and out of seaports; shipments moving on more than one mode are particularly vulnerable. A successful asset-protection program addresses these risks and outlines steps to avoid them.

REAL-WORLD SOLUTIONS

Today, successful companies are concerned about all facets of their security programs. Inventory loss, fraud, terrorism, product tampering, diversion, counterfeiting, smuggling, the theft of proprietary information, and cybercrime are threats that can negatively impact not only a company's reputation, but also its bottom line.

There are numerous reasons to invest in protecting your supply chain, which is why successful companies make asset protection a top priority. The benefits derived from a world-class security program include:

- **Not jeopardizing your C-TPAT certification.** A current C-TPAT certification is essential for any eligible company that wants to stay competitive in today's marketplace. To date, more than 3,400 companies have been either suspended or expelled from the C-TPAT program, a consequence that is far more likely to happen to companies with deficient safeguards.
- **Significantly reducing your risk of internal theft and cargo.** Nearly every dollar saved goes back onto your bottom line—where it belongs.
- **Mitigating your exposure to costly litigation and negative publicity.** Some companies that suffered major security breaches had to spend six figures on legal representation, and damage control and public relations consultants.
- **Avoiding insurance premium increases.** Insurance carriers are typically interested in doing business with, and offer more competitive rates to, companies with good histories, i.e., those without security-related claims.
- **Having a marketing advantage over competitors that don't have a robust security program in place.** Most buyers of finished goods and logistics services today will evaluate how effectively their prospective business partners protect their supply chain from loss, disruption, product tampering, and smuggling. Companies that don't have world-class asset-protection programs often lose out on contracts to competitors that do. ■