A Costly

By Barry Brandman

This west coast distributor had never experienced any cargo theft, which was why they were shocked when two loaded containers parked in their yard vanished in broad daylight. We were called in to investigate and came away convinced that, as with many cargo theft cases, it was an inside job.

We arrived at this conclusion after determining that nearly all of the trailers that were stored in their truck yard were empty on the day of theft. However, the thieves knew which two trailers were fully loaded, despite the fact that there were no visible markings on the outside of the containers. Additionally, the stolen trailers were only vulnerable for 90 minutes because they were placed in the yard at 2:00 p.m. and were scheduled to be picked up by an outside carrier at 3:30 p.m. that same day.

Even in states with chronic cargo theft, the odds of an outside theft ring having two available tractors and randomly stumbling across these two loaded containers within a 90-minute window of opportunity were so remote as to be beyond the scope of possibility. Upon further investigation, we subsequently determined that the thefts were indeed set up by one of the distributor's supervisors.

Epidemic

Explosive Growth

Unfortunately, this and other forms of cargo theft are becoming more commonplace. Industry experts now put the cost at $10 to $20 billion annually in the United States and in the ballpark of $50 billion globally.

One of the side effects of a healthy U.S. economy is that more product than ever before is being shipped to warehouses, stores, and consumers via truck. As a result, criminals now have found that there is a fortune to be made by stealing these "warehouses on wheels."

Once the exclusive domain of old established organized crime families, dozens of new cargo theft rings have sprung up across the country. While the major gangs who commit these thefts on a nationwide scale are based in south Florida, the New York metropolitan area, and southern California, in the last several years law enforcement has witnessed the growth of regional crime rings in areas such as Dallas, Houston, Chicago, Atlanta, and Oakland.

Attracted by the number of trucks on the road transporting valuable goods, lax security controls utilized by many warehousing and transportation firms, the low probability of being caught, as well as the huge market for "discounted" black-market product, cargo theft has turned into an underground economy.

The relatively lenient criminal penalties given out for cargo theft, which are nowhere as severe as the sentences handed out

to convicted drug traffickers, is one of the reasons why some of the cargo theft rings were formally involved with the distribution of illegal narcotics. As a result, they have the needed personnel and distribution pipelines to sell stolen product domestically as well as internationally.

Among the most sought after products targeted by cargo thieves today are consumer electronics, cigarettes, computers, cosmetics, fragrances, jewelry, pharmaceuticals, and food.

Different Forms of Cargo Theft

There are two types of cargo theft. *Internal theft*, which involves drivers working in collusion with employees at the shipping or receiving docks, and *external theft*. The latter type typically takes one of three forms:

- Theft by deception,
- Theft of an unattended truck, or
- Forced hijacking.

An example of theft by deception is best illustrated by a company that was recently victimized for $480,000 when a trucker dressed in full uniform and having a company photo ID arrived at a distribution center to pick up a waiting order. This driver calmly walked up to the dispatch office window, presented his ID, and obviously knew that there was staged product waiting to be loaded. Neither the dock guard nor the dispatcher had any indication that they were being scammed until the real trucker showed up for the same order two hours later, only to be told that this shipment was already picked up earlier that day. These types of "bogus driver" thefts have been increasing in the last few years, especially in the northeast.

Trucks that disappear while parked at truck stops, rest areas, or diners, as well as armed hijackings are not always as they appear. A number of these thefts are either set up or personally committed by employees or contractors with knowledge of what is inside the containers, the routes they'll be traveling, and the security safeguards that are in place.

Because many of these cases are not solved, insurance companies have been hit hard in recent years and premiums are on the rise, which is another costly ramification of this problem. However, because many insurance companies have significantly raised their premiums or declined to insure carriers with a history of cargo loss, trucking companies and distribution firms have been forced to find more effective ways to protect the product that they transport, realizing that the buck now stops with them.

Protecting Assets while in Transit

While there are no easy or quick fixes, following is a sampling of some of the essential components of a successful asset protection program.

- *Don't react passively to loss.* After a theft has been committed, have it thoroughly investigated rather than simply filing a police report or insurance claim. Because many victimized firms do not aggressively investigate, cargo thieves brazenly strike with little or no concern for being caught. In fact, it's commonplace for the thieves to focus on the same companies, hitting them continuously until they are no longer easy targets.
- *Install global position satellite (GPS) technology in your trucks,* especially if you are located in or transport goods through states prone to cargo theft. The newer versions of GPS and assisted GPS (AGPS) will allow you to not only track your trucks, but the better systems also provide for two-way communication, concealed duress buttons, remote disabling devices, geo-fencing, and notifications if, for example, a trucker isn't at a delivery location at his estimated time of arrival. Newer technology is also on the market that allows for battery-operated covert devices that can be concealed in the cargo area of trailers and ocean containers.
- *Maintain a counter-surveillance program.* One of the methods used by professional thieves is to surveil trucks when they leave distribution centers. In fact, it's not unusual for these trucks to be followed for hundreds of miles by the thieves who wait patiently for the driver to stop for fuel, rest, or food. Routinely monitoring staging points close to the distribution center, as well as following trucks for the first ten to fifteen miles, may expose these criminals before they have the opportunity to strike.
- *Mark the tops of trailers* so that law enforcement can easily identify stolen trailers and containers via aerial surveillance.
- *Utilize an anonymous tip line program* throughout your company. Employees oftentimes learn of security breaches or become aware of suspicious activity but are concerned about coming forward with this information because of "whistle blower syndrome." Providing workers with a risk-free way to report this type of information and rewarding them for confirmed tips is an essential component of a loss prevention program. One good call can easily pay for the cost of the program for years.
- *Always stage high-value containers in well secured storage facilities.* In addition to adequate lighting and fencing, you can enhance physical security be installing digital video systems that record activity 24 hours a day. Sophisticated video technology can be viewed remotely hundreds of miles from a site. Additionally, CCTV can be interfaced with intrusion detection and access control systems for even tighter control.

Trucks that disappear while parked at truck stops, rest areas, or diners, as well as armed hijackings are not always as they appear. A number of these thefts are either set up or personally committed by employees or contractors with knowledge of what is inside the containers, the routes they'll be traveling, and the security safeguards that are in place.

- If you direct ship from one facility to another, *use high-quality security seals* to protect against the driver stealing product from the cargo area of the truck while in transit. However, it's important to remember that unless you consistently adhere to strict seal procedures, even high end, expensive security seals can be circumvented by devious employees and professional thieves.
- If you work with an outside trucking firm, *establish minimum security standards and clarify your expectations.* You want to be sure that the carrier is doing enough proactively, and equally important, will do the right thing if a theft occurs. Many companies assume that if they use an outside carrier, they no longer have to be concerned about the financial consequences of cargo theft. The reality is that there are an array of peripheral costs as well as liability issues that may not be covered by the carrier. In fact, many trucking companies are no longer able to fully insure high-value loads. Consequently, customers are being forced to assume a good percentage of the cost of a stolen container, which can easily run in the mid- to high six-figures.

In the last few years, professional cargo theft rings have expanded their activities, no longer focusing only on trucks, rail cars, and ocean containers in transit. They have found it extremely lucrative to attack distribution centers and manufacturing plants, where they have repeatedly gotten away with millions of dollars of stolen inventory.

Facility Break-Ins

In the last few years, professional cargo theft rings have expanded their activities, no longer focusing only on trucks, rail cars, and ocean containers in transit. They have found it extremely lucrative to attack distribution centers and manufacturing plants, where they have repeatedly gotten away with millions of dollars of stolen inventory. Not bad for a few hours of work.

The truth of the matter is that these break-ins require much more time to set up. It's not unusual, for example, for cargo rings to dispatch advance teams to surveil a target for several weeks prior to their attack. Issues such as the time the facility opens and closes, the number of employees on each shift, the traffic patterns of inbound and outbound trucks, whether there is on-site security and, if so, how and where the manpower is appropriated, the design of the lighting and fencing, as well as the frequency of roving police patrols are just some of the factors that they carefully evaluate.

They have also been known to gain entry inside their targeted facilities posing as vendors, contractors, service people, or sales

representatives. Additionally, they occasionally will have their people apply for jobs. Once hired, they can assess the type and location of all the alarm devices, what type of video system is in place, and the interior physical structure of the doors, walls, and racking. After this information is obtained, and oftentimes photographed using concealed cameras and camcorders, they can methodically plan the most effective way to circumvent the facility's security safeguards.

They generally arrive with a team of specialists, including forklift operators, tractor trailer drivers, surveillance personnel to stake out the major access roads for police response, as well as technical experts who know more about electronic alarm systems than many of the companies that install them. The end result is usually a successful heist, with the victimized company not knowing they've been hit until the next work shift arrives.

Most of the companies that find their alarm systems disconnected, the video recorders missing, and several trailer loads of inventory stolen are shocked, not just by the financial loss, but by the efficiency of the perpetrators.

In one recent case, the criminals cut a hole in the roof, descended into the facility via a rope ladder, and disconnected the alarm system control panel and communication equipment. At that point, they located the inventory they wanted and used the company material handling equipment to load the tractor trailers they had brought along with them.

While most victimized companies are surprised by the ingenuity and ease in which their security controls were defeated, the reality is that the professionals have been using the same methods for several years. Disconnecting phone and power lines, cutting through doors (rather than prying them open and activating the magnetic contacts), and entering via the roof or wall vents are standard operating procedure and pose little difficulty for them. While there are always new, innovative methods, such as installing concealed wireless video cameras

When criminals weigh the risk versus reward, it's no mystery why cargo crime has become a multi-billion dollar problem that will most likely continue to escalate in coming years.

outside a building that will record employees entering their alarm codes into the lobby keypad, the professionals tend to stick with the techniques that have historically been very effective for them.

Defeating Security Systems

"I can't believe my security system was so easy to defeat."

We've heard this statement repeatedly, usually accompanied by a dazed expression that can best be described as shock and awe. To appreciate why intrusion detection and video systems have been consistently compromised, it's necessary to understand two realities about the alarm industry.

The first is that most of the sales representatives that design intrusion detection and video systems have very little, if any, direct knowledge of how the professional thieves operate. While this may seem illogical, it's nonetheless true.

When involved in a post-theft investigation, we always meet with representatives from the security system provider. During these discussions, we typically ask these sales representatives if they are familiar with the professional thieves and their standard operating procedures. Ninety-nine out of 100 times, the answer is, "No." However, these same sales reps are the ones that companies typically rely on to select the right technology, strategically position the protective devices, and properly program the systems.

continued on page 52

continued from page 50

The second fact is that alarm companies have little legal or financial responsibility for losses sustained by their customers. Regardless of whether for example, the wrong devices were selected, or if the central station operator failed to properly respond to an activation, alarm vendors have limited liability. If you doubt this, read the small print in your contract and you'll probably find not one, but two or three clauses that stipulate this.

This is not an indictment of alarm and video companies. The reality is that they would not be able to obtain insurance if they assumed this type of responsibility. Because alarm companies could potentially be paying out millions each year, their contracts state that they are not "insurers."

However, without having serious "skin in the game," they don't always understand the need to be absolutely certain that your intrusion detection system is "bullet proof."

The Worst Is Yet to Come

Experts agree that cargo is vanishing with greater frequency. To make matters worse, criminals are becoming more entrepreneurial in developing new outlets for stolen product.

Additionally, we have found that the buyers of large quantities of stolen merchandise are oftentimes businesses that encourage the thieves to steal more volume, and provide detailed shopping lists of what brands and models they are willing to pay top dollar for.

Over the years, we've tracked hot goods throughout the country. However, it's no longer unusual to find stolen merchandise being resold in other parts of the world. As a result, it's becoming increasingly difficult for law enforcement to track and recover stolen merchandise after it disappears.

When criminals weigh the risk versus reward, it's no mystery why cargo crime has become a multi-billion dollar problem that will most likely continue to escalate in coming years. ■

BARRY BRANDMAN is president of Danbee Investigations, a Midland Park, New Jersey, company that provides professional investigative, auditing, and security consulting services to hundreds of major firms. He has appeared on network television and has been a guest speaker nationally and internationally for organizations such as the Council of Supply Chain Management Professionals, the North American Cargo Security Forum, the International Warehouse Logistics Association, the Pharma Secure Conference, the Foreign Trade Association, and the National Retail Federation. The Warehousing Education and Research Council has published Brandman's manual entitled Security Best Practices. *In addition, he has authored articles for numerous publications, including* Corporate Security, Risk Management, Global Logistics & Supply Chain Strategies, *and* Supply Chain Management Review. *Brandman can be reached at 201-652-5501 or bbrandman@danbeeinv.com.*