Supply Chain Security Demands Greater Focus

Today's supply chain security threats are radically different than in the past

Crimes involving the theft of products, merchandise and other hard and soft goods continue to plague the logistics sector. "There is an absolute increase in the number of occurrences taking place every single year, leading to devastating financial consequences for warehousing companies, 3PLs, carriers, manufacturers, wholesalers, and retailers," confirms **Barry Brandman,** president, Danbee Investigations.

The estimated loss attributed to supply chain theft, according to government statistics, is $35- to $40-billion per year. However, this figure (emphasis on estimate) represents only a small fraction of the actual total loss, according to Brandman, because most companies experiencing a loss from theft do not publicly report their supply chain losses for a variety of commercial, financial, and/or competitive reasons.

Then there's also the various indirect, or peripheral costs, associated with product disappearance. These indirect charges easily can amount to large multiples of the original loss amount. Among these are fees and charges associated with the risk of product tampering, compromised price integrity, replenishment costs, and legal and investigative costs. Also, for 3PLs in particular is the potential loss of customer confidence.

Warehouses remain as top targets

"Logistics facilities are perfect environments for theft to occur," Brandman declared at the 2019 WERC Conference. He explained: "You have thousands of cases of finished goods coming in and out your facility at a rapid and sometimes chaotic pace. Unless you're sitting at the door doing case-by-case or pallet-by-pallet reconciliation to the manifest of what is supposed to be going out or coming in, it's almost impossible to discern the difference between everyday legitimate activity and collusive theft."

Develop an effective security program

Brandman advises: Realistically evaluate your security safeguards. Take a realistic look at what you're doing right now. Does it really work? Does it look better on paper than it operates in actuality?

"Most security programs are not that effective," he maintains. "They tend to look a lot better from the distance, but when you get close up and start to probe deeply, that's when you find where the lapses are located." Find your weaknesses before others can exploit them, he urges.

Once you identify how good your program is, create and maintain an effective auditing program so whatever upgraded loss prevention safeguards are implemented can be regularly checked and evaluated. "If you don't verify and that verification process is missing, I can guarantee you that whatever controls you set up, over time will start to dissipate and become loose and sloppy," Brandman warned.

- **Establish effective hotline program.** One key to success is to offer complete anonymity (not just confidentiality) to the caller. Brandman explains: "We never ask the caller for their name. Without their name we can't in any way accidentally or otherwise breach their identity. Instead, we give them a code name or code number." This is what gives individuals the courage to come forward and provide the tips on behalf of the client.

He also recommends outsourcing the hotline. Outsourcing always will work more effectively than insourcing because employees, again, don't want their voices recognized when it comes to reporting a security problem.

Theft related loss is getting worse, because employee theft is a high-gain, low-risk proposition.

Using his formula, Brandman explained why:

The value of the product continues to increase + there's a low-risk factor of being caught + the problem of ineffective security practices and programs + an "inadequate criminal justice system," = a high-gain, low-risk situation.

"What's made this problem even worst is the Internet, which has become the ultimate hi-tech flea market for dishonest workers and professional thieves," he declared. Stolen merchandise is being routinely sold quickly domestically and internationally by the sellers without fear of apprehension because they can conceal their identities on the Internet via bogus names and websites. Further, thefts are also being regularly perpetrated by organized crime groups that specifically target logistics companies using such techniques as fictitious driver pick-ups and warehouse break-ins.

For those who operate international supply chains, there's also the growing threat from terrorists who continually attempt to infiltrate these supply chains. Brandman attests to the "hundreds of attempts by terrorist organizations and rogue governments hostile to the U.S. that have been caught trying to ship weapons, manpower and cash into the U.S. through commercial supply chains." He recommends companies with international supply chains become C-TPAT certified and adopt AEO (authorized economic operator) standards within the WCO framework of standards to secure and facilitate global trade.

Brandman insists to make certain that a co-worker cannot be wrongfully punished. "The way we do that is very simple: no one is punished solely based on a tip we receive," he says. "The information has to be independently investigated and verified before anyone receives a disciplinary action."

- **Introduce an undercover operation.** This is a very interesting concept and one that many companies use to determine what is really happening on the warehouse/DC floor. Typically, logistics companies will contract with security or investigation firms who will place the undercover operative within the organization.

As effective as the undercover initiative is, Brandman insists that three strategies be consistently followed:

Use undercover information as intelligence, not proof. "Once the reports start to come through and you start to read about some of the things taking place in your company, your knee-jerk reaction is to do something about it," Brandman notes. "I caution you not to do that."

Don't overreact to information. Reacting too quickly or overreacting will reduce the probability of learning about the problems taking place. "And the odds are that the first problem that comes to light through an undercover investigator is not the only problem, or the most significant problem that is taking place within the company," he maintains.

Undercover is not a short-term solution. Undercover takes time because there is no substitute for naturally and gradually developing relationships and rapport with fellow workers. Undercover investigator needs to build their trust and confidence.

- **Consider cybersecurity.** Protecting integrity of data and network is another area of critical concern. While there are many areas for concern, Brandman focused on four: Encrypt sensitive e-mail; require password standards; safeguard sever rooms with card access, alarm and video technology; and have your system penetration tested.
- **Minimize cargo theft risk.** There are six proven strategies that are "tried and proven" and are "extremely effective" that Brandman recommends:

1. Don't react passively to loss. Aggressively investigate each case.
2. Utilize GPS with mobile geo-fencing, panic buttons, and disabling devices.
3. Use state-of-the-art technology to enhance yard security.
4. When shipping directly from one facility to another, utilize effective seal procedures.
5. When working with logistics partners, establish sound security standards. Test these safeguards on a regular basis.
6. Digitally record all truckers picking uploaded containers. Once this information is in your system, use it for verification purposes.

> "Unless you're sitting at the door doing case-by-case or pallet-by-pallet reconciliation to the manifest ..., it's almost impossible to discern the difference between everyday legitimate activity and collusive theft."
>
> Barry Brandman