Supply Chain Security

by Joe Mullich / 18 November 2013 / for Wall Street Journal

As supply chains become more globalized and complex, so do the risks to organizations.

Consider some recent headlines: In 2012, $2 million worth of copper ingots were stolen from a facility in Arizona. More than $1 million in vodka was stolen from a warehouse in Florida.

Supply chain risk affects every part of the world. In Mexico, thieves were reported to have boarded trains and tossed products to the side of the tracks for their partners in crime to collect. And according to Brazil's National Association of Cargo Transport and Logistics, stolen food/drinks, electronics, tobacco and pharmaceuticals wind up in consumers' hands via the black market as well as legitimate retail outlets.

Incidents such as these that occur throughout the supply chain can have severe implications for a company's reputation as well as its bottom line. The global adoption of social media has made it nearly impossible to sweep an unfortunate event under the rug. Today, news from halfway around the world can catch on like wildfire.

"The 24-7 social-media environment we live in raises the bar on supply chain theft," says Don Hsieh, director of commercial and industrial marketing for Tyco Integrated Security. "If someone steals your food products, fails to keep them in the cold chain and people become sick, that could have serious repercussions on your brand."

Locking down the supply chain is difficult because much of it is beyond your control. For example, "If you are sourcing from a foreign country, you want to know that the facility that your truck enters within the port is secure," says Bill McBeath, chief research officer for ChainLink Research. "That can be difficult to do for all routes and all products."

Transportation security is critical given that 90 percent of cargo thefts involve trucks. "A growing threat is fraudulent pickups, where the thieves know the pickup schedule ahead of time, show up with false IDs and simply drive out with the merchandise," says Hsieh.

Video surveillance technology on-site can go a long way to help deter this rising threat with systems that can record the license plate number of vehicles and rapidly perform analytics to determine whether or not the truck is legitimate. Video technology can also be used to evaluate internal threats—ensuring that employees are adhering to proper security procedures.

Other strategies that can be implemented include equipping trucks with GPS tracking devices, which can identify whether a vehicle is off route. If so, the truck can be remotely and safely braked to a complete stop at 10 mile per hour increments.

According to McBeath, one ingenuous approach is to make the cargo less inviting to thieves. One anecdote: A shoe manufacturer sent shipments of left shoes and right shoes in separate

trucks using different routes. “Thieves realized there isn’t much of a point in stealing one those shipments,” he notes.

Annual Audits Address Vulnerability

Ensuring the physical security of your supply chain starts with an annual audit, where you assess both your own facilities and those of your suppliers to ensure that they are addressing key areas of vulnerability.

“For distribution centers, the physical security has to be done in layers,” says Glenn Master, chairman of the International Supply Chain Protection Organization (ISCPO), an industry group. “A retail store may only have one layer of protection, but distribution centers have perimeter fencing, multiple access points available to certain people and human elements that need to be taken into consideration.”

The physical security review includes the building materials of the structure, guard gates, alarm systems, perimeter lighting, locks on all doors and windows, and access control technology, which restricts entry to certain areas through mechanisms such as card metrics and biometrics.

“You need to determine that facilities are limiting access not only to visitors, but also to employees in certain areas,” Hsieh says. “For example, the mixing area for food presents the opportunity to contaminate a large batch of food, so you want to make sure only authorized people are allowed access there.”

Master says the inspection should home in on seemingly small details that can have big implications for security. “You could have a good security system that doesn’t work adequately because you failed to clean or maintain it,” he says. “Sometimes people turn off the alarm and forget to turn it back on. A lot of companies have systems in place for years without ever testing whether they are still working.”

Hsieh points out that some studies have shown security procedures are only followed 50 to 80 percent of the time. But, he says, “If you do randomized audits and use remote video auditing as a tool for training employees in proper procedures, compliance has zoomed up above 95 percent.”