LOOKOUT is proud to have with us Mr. Lawrence, VP of Pinkerton Consulting & Investigation, in a sharing of his expertise for the issue. Being in Law Enforcement and Security Operations for over thirty-five years, his global experience ranges from guard force management, operations management, fire protection and prevention, investigations, executive security, crisis management, and even technology. The essence of his career is carried in this piece of elaborate and comprehensive write up on optimizing supply chain and logistics security.

LOCKING IT DOWN

Issues, considerations and best practices for optimum supply chain and logistics security

JOHN H. LAWRENCE
Vice-President
Pinkerton Consulting & Investigations

In today's increasingly interconnected and interdependent world, supply chain security is arguably more important than ever. With so many manufacturing operations utilizing a "just-in-time" inventory model, a single kink in the supply chain can have a crippling impact not only on the manufacturer, but cascading on down to their customers, as well. To illustrate just how vulnerable an entire "ecosystem" of businesses can be to a single adverse event, we need look no further than the 2011 tsunami in Japan. With increasingly centralized manufacturing in a variety of industries, the loss of a single major supplier's facility can bring the global supply chain to a standstill.

In that sobering context, understanding the issues, considerations,challenges and best practices for optimum supply chain and logistics security should be a key priority for any organization that transports goods or relies on materials that need to be moved from Point A to Point B. Decision makers and security personnel should be fully cognizant of today's supply chain and logistics security challenges, as well as the steps that can be taken to overcome those challenges, reduce exposure and mitigate risk: from conducting a comprehensive risk assessment, to implementing appropriate physical security standards, to putting policies and procedures in place that will maximize supply chain security going forward.

Risk vs. Threat

The first piece in the security puzzle is a comprehensive and sophisticated risk assessment. But because the nature of the supply chain and logistics security threat can vary so dramatically, making that assessment meaningful can be challenging. Damaging crime ranges from opportunistic pilferage of a couple cases off the back of a truck, to highly sophisticated and organized hijackers who may even use refined tactics and technologies (such as handheld jammers that can jam a GPS signal) to help them commit their crimes.

The key is to understand your risk, and while that might sound straightforward, it is surprisingly common to see this mishandled or misinterpreted. A big part of the problem is the tendency to mix up the notion of risk with that of threat. Threat is just one part of abevy of factors that goes into a risk profile. To assess risk, we must take into account threat, vulnerability, and potential consequences. For example, if a facility is located in a high-crime environment, the threat level may be high. But if that same facility is secure, with the right policies, tools and systems in place to optimize security, the level of vulnerability is comparably low. And if that facility is one of many that produces or transports a particular product, the consequences of a disruption if something were to happen are not especially dire. In other words, the overall risk level associated with that facility is low.

Compare that to a similar facility in a relatively safe, crime-free region of the world. While the surrounding environment may be low threat, lax security standards can increase vulnerability, and if this facility is the only plant in the world that produces a particular component, the overall risk profile is actually very high.

Physical security standards and procedures

One of the most important things any organization can do to lower its risk profile and protect its supply chain is to implement minimal physical security standards at proprietary sites and any locations where loading and unloading take place. That includes some third-party sites, and facilities like trans-shipping warehouses, cross-dock operations, and rail-to-trucking facilities.

Best practices for basic physical security include things like access control: perimeter security such as fencing and gates, control of facility openings and access points, and controlling access to sensitive/high value areas. Does a site have a CCTV system, appropriate lighting, and effective alarms and alerts?

Having the right policies and procedures in place is also critically important. Perhaps the most valuable is to ensure that background checks and professional screening is conducted for all employees—including third-party contract employees. Make sure that cages or vaults are used for highly sensitive or valuable materials, and ensure that visitors to the facility (and especially to sensitive areas of the facility) are escorted and monitored at all times.

In North America, where 80-85 percent of all cargo transportinvolves trucks, having proper procedures in place for loading and unloading trucks is essential. Make certain that truck trailers are properly sealed, including the use of fastening cables or hardened steel bolts to improve security where appropriate. Even things like scheduling and route planning can play a role in improving security. The saying "freight at rest means freight at risk" is a good one to remember: it is always easier to rip something off from a freight yard or a truck stop, and those areas are consequently more at risk.

Nuts and Bolts

In addition to the basics, it also helps to be aware of common blind spots and specific strategies

please turn to next page

and tactics that can be used to minimize or neutralize threats. Details matter: supply chain security vulnerabilities usually manifest themselves as a result of lots of little things as opposed to one glaring hole. For example, security cameras may be in place, but they may not have been maintained particularly well and the lenses may not have been cleaned in years. Or perhaps a lack of clearly defined processes in shipping and receiving areas makes security lapses or breakdowns more likely due to human error.

In some cases, companies may mandate background screening on employees, but those companies might not be as thorough in performing those checks on their contractors and third-party vendors—or perhaps the checks may not include drug screening. Today, with new outsourcing business models on the rise, many outside companies are being brought in to handle supply chain and logistics issues. This significantly increases your vulnerability, and highlights the corresponding need to perform diligent and rigorous background and security reviews. Companies inherently have less control over and less insight into those third-party employees and circumstances—including employment details, who has access to what information, and other relevant data.

Simply keeping yourself educated and informed can make a big difference. Be aware of hot spots and danger zones. The vast majority of cargo theft and hijackings, for example, occur in just a handful of states in the U.S. Even the types of products and materials that are attractive to criminals change over time. Be aware of what is desirable and adapt strategies and policies accordingly.

Unsecured parking and storage areas are a problem. A high-security seal or a bolt locking system is an incredibly small investment to make for a significant level of added security.

Boosting security during the transport piece of the supply chain may also be a wise move. From the strategic planning and timing of routes, to deciding whether GPS tracking on shipments makes sense, to utilizing geo-fencing for ensuring that shipments are on route and on time, there are a number of ways to improve the security of goods in transport. Convoys and follow-cars can be deployed situationally for high-value shipments.

Pros and cons

No matter where you sit on the supply chain, one of the best things you can do to optimize your supply chain and logistics security is to seek counsel or assistance from trained security professionals.

The best reputable and experienced professionals will avoid “checklist assessments” and instead perform a custom holistic risk assessment: a comprehensive security audit that integrates standards and principles utilized by a wide range of different government customs and security agencies. When it comes to supply chain security, you do not want to simply check boxes on a checklist, you want to work with someone who can literally check your boxes in the warehouse and in transit. When possible, work with trusted professionals with a demonstrated ability to perform an analysis from a global top-down level, engage in detailed on-site local evaluations, and also train your own team to engage in regular and rigorous self-assessments going forward.

One emerging area of concern is in the phytosanitary arena, with environmental security flora and faunaimport restrictions. For example, if you have a manufacturing facility in Thailand that temporarily stores pallets outside, insects or seeds that are blown into those pallets could be a serious problem when passing through customs in the destination country. Phytosanitary compromise can be a significant liability from a financial and regulatory standpoint. If customs puts a hold on one of your trailers, it can essentially shut down your supply chain down for days or even weeks. In some countries, the shipper actually has to pay the storage fee, increasing the financial impact.

Finally, be wary of making the common mistake of assuming security based on past history. The “We've never had a problem, so why invest more resources in better security policies?” fallacy is a refrain that far too many organizations have repeated just before a damaging and disruptive security breach. Ensuring supply chain and logistics security before a problem arises is a much wiser and far more secure approach to a very common problem.

FEATURES

ANTHONY LEE

Sr Director Security & Facilities - AP & ME
Ingram Micro Asia Pacific Pte Ltd

Ingram Micro Inc. is the global leader in technology and supply chain services. In June 2014, the company's Mumbai-Thane Distribution Centre (DC)became the latest Ingram Microfacility in Asia Pacific region topass the TAPA certification audit. As a result, it isnow certified to TAPA Freight Security Requirements (FSR) Class A standards by TUV Rheinland.

Globally, Ingram Micro now has a total of 30 facilities that are TAPA FSR Class A certified. This includes advanced logistics centres in Sydney, Singapore and Shanghai.At each of the company'smajor facilities, including the Mumbai DC, Ingram Micro has made significant investments in modern digital surveillance and security technology and processes to ensure that its business operations and service delivery are world-class.

Ingram Micro is committed to protecting the people, products and property of both Ingram and its business partners, and the successful certification of its Mumbai DC is a direct result of the strong security partnerships across all segments of its businesses.The TAPA certification representsthe importance of security compliance and best-practice standards in the supply chain industry.

About Ingram Micro

Ingram Micro helps businesses fully realize the promise of technology. Ingram's global infrastructure and deep expertise in technology solutions, logistics services, cloud and mobility solutions enable its business partners to operate efficiently and successfully in the markets they serve. Combined with distinct market insights, and the trust and dependability generated from decades of strong partner relationships, Ingram Micro stands apart as the global technology services provider for the future.