SecurityManagement ONLINE
The Security Professional's Central Web Connection

Special Focus On Transportation and Cargo

Friday, June 15, 2007

Assessing Cargo Supply Risk

By Dan Purtell and James B. Rice, Jr.

A study of supply line risk in 45 countries finds that many companies are not properly assessing or countering vulnerabilities.

The largest and fastest growing global economies around the world include Brazil, Russia, India, and China (BRIC). These countries, along with other high-tech manufacturing centers such as Malaysia and Indonesia, are attractive to companies both as a source of supply and as new markets to sell into. Before companies enter these inviting markets, however, they must understand the risks of operating supply lines in these environments and how to counter them.

These issues have been the subject of a multiyear study that was completed earlier this year by our company, First Advantage. The study examined countries to see what risks they represent, and it looked at the measures being implemented by companies to see whether indeed they are mitigating those risks.

The study, which covered 45 countries, specifically focused on transportation route risk. Supply chain risk assessments typically included a review of companies' manufacturing locations, trucking operations, freight forwarders, third-party logistics warehouses, container-stuffing operations, and the supporting seaports and airports. We found that certain security gaps were common across the study group.

Top Vulnerabilities

Among the vulnerabilities were that most companies failed to conduct container security inspections; containers often arrived at the seaport with no seals; there were no background investigations on employees; and there was no security or threat awareness training for workers. Most companies had no idea what, if any, security procedures had been adopted by their business partners.

Within single businesses, the security equipment and procedures were limited to the main manufacturing facility. Security at other potential weak spots, such as container-stuffing operations or third-party warehousing, was ignored.

When judged against objective standards, such as the U.S. Customs and Border Protection's program, Customs-Trade Partnership Against Terrorism (C-TPAT), many of the facilities rate a poor grade. We estimate that most of the companies studied would be only 50 percent compliant with C-TPAT security criteria and some would be as low as 10 percent compliant.

Lack of consistency. A key contributing factor is the lack of a consistent security methodology across all operations of each company. For C-TPAT certification, the security methodologies must be consistently applied throughout a corporation's in-house and outsourced manufacturing locations and transportation base. For example, the study found that when companies conducted assessments of their own security operations, they generally looked only at one or two internal and outsourced facilities and suppliers, sampling them as an auditor would, rather than thoroughly examining security at every single site. This method is unlikely to reveal an accurate state of security for a particular corporation.

Corruption. The study also looked at the extent to which corruption was an issue in these environments. The study used an existing indicator, the Transparency International Corruption Index, developed by a German nonprofit group. The index indicates the degree of corruption as seen by business people and country analysts and uses a scale that ranges between 10 (highly clean) and 0 (highly corrupt). The calculation includes police corruption, business corruption, and political corruption.

As a point of reference, the United States has a corruption index rating of 7.6 and Switzerland is rated at 9.1. The study found that the three top-rated countries for corruption—Nigeria, Malaysia, and Indonesia—are also rated as

a “severe risk” in terms of anti-American or anti-Western sentiment. When we merge these two variables together, a potential risk emerges. For example, there may be a greater opportunity for something harmful to be introduced to a U.S.-bound container coming from one of these countries.

Cargo theft. The study also used First Advantage’s Global Loss Repository—a database of cargo theft data from around the globe—to create loss rates for cargo transiting through respective countries. The countries are rated as low, guarded, elevated, high, or severe, depending on the number of losses. For simplicity, the survey chose to use the same coding system the Department of Homeland Security applies to terrorism risk levels.

Companies operating in countries rated as “severe” can expect armed and violent truck hijackings, armed warehouse robberies, and frequent heists at airports. Companies operating in countries ranked as low risk should expect only minor losses due to pilferage.

Exposure Matrix

We also devised a weighted C-TPAT exposure matrix for the survey; it quantifies risks associated with anti-American sentiment or other hostility to Western governments. In this scale, countries rated as “severe” would present the possibility of terrorist attacks against U.S. or Western citizens, possibly have travel restrictions in place, and support high levels of supply chain theft.

The study incorporated all of this information to develop a profile of emerging-market country risk. The results were surprising, especially when compared to the Department of Homeland Security’s Threat Advisory panel.

For example, Russia and Brazil are among two of the highest-risk countries in terms of supply chain theft. Incidents commonly involve government representatives including police, military, and customs officials. However, in terms of C-TPAT, these countries are given a “low” threat rating because the governments and residents are on amicable terms with the United States and are not hostile to Western culture.

China presented a similar situation. The three-year cargo theft trend in China reveals that losses are increasing and higher levels of violence are being used in cargo theft, leading the authors to give the country a “guarded” rating. However, China was rated “low” in their level of C-TPAT exposure because of a low cargo tamper rating and alignment with Western culture.

The study also went beyond BRIC countries to places such as Indonesia, Malaysia, and Nigeria. In contrast to countries like China, these countries are rated as risky (severe risk) from a C-TPAT perspective because of the cultural differences and high cargo-tampering rates throughout the country. Some of these countries, which export huge volumes of goods to the United States, present an opportunity for terrorists to use those shipments to smuggle weapons of mass destruction into the U.S. or to use the shipments as cover for an attack.

A significant problem contributing to this risk in Southeast Asia is labor shortages that affect the quality of the work force. To use Malaysia as a specific example, shortages of manufacturing labor within the country have led to high rates of foreign workers within Malaysian factories.

Some factories may sustain a 75 percent foreign work force, and many workers come from countries with a high rate of anti-American or anti-Western sentiment. These workers are typically not vetted and are working on products bound for U.S. importation.

Organized crime. But terrorism, while high consequence, is low probability. The more common risk in these countries is theft from organized crime. For example, in Malaysia, the Mamak gang is a highly organized group of cargo thieves that has plagued Malaysian transportation for over two decades. Members are primarily Southern Indian Muslims who target high-value loads from the central and northern regions of Malaysia. This gang, although smaller today than in previous years, is still active in the region and carries out thefts on a monthly basis.

Land routes are not the only problem. The Strait of Malacca, between Indonesia and Malaysia, suffers the highest rate of sea piracy in the world.

Adding to troubles in the region, experts speculate that Southeast Asia’s most wanted terrorist—Noordin Mohammed Top—resides and is active in Malaysia or neighboring Indonesia. Top is the self proclaimed leader of Tandzim Qoedatul Jihad, commonly referred to as the al Qaeda of the Malay Archipelago.

He is believed to be involved in the Bali nightclub bombing, the Marriott Hotel bombing in Jakarta, and the Australian Embassy bombing in Indonesia. Top, a bombmaker by trade, is also believed to be actively recruiting in several Southeast Asia countries with primary targets being the United States or other supporting Western countries.

Company Analysis

Firms that are assessing their supply chain operations should take each of these risk variables into consideration. However, the study indicated that, within the global supply chain, a cookie-cutter approach to security has led companies to overspend in low-risk countries such as China and underspend in high-risk countries such as Malaysia and Indonesia.

This was the case with one high-tech organization that had small facilities in both Malaysia and Indonesia, but imported 80 percent of its goods through China. The company focused security on its supply lines in China because that country supplied the most goods. That approach might seem logical, but it is ill advised. Volume-based risk assessment will only identify a company's largest importer, not necessarily its biggest risk.

After reviewing the company for the survey and applying the results to its entire supply chain, we recommended a different approach. By reviewing all of the supply chain risk variables, no matter what size, we determined the level of inherent risk. For this company, the risk variables included mode of transportation, the country of origin, type of load—consolidated or LTL (less than full load)—and transshipment locations. We found that several relatively small suppliers in Malaysia represented more risk than all of the suppliers in China.

While leaving the security plan for Chinese suppliers in place, the company increased security in Malaysia. It also began security escorts to and from the port, enhanced seal and lock processes at the warehouse, and set out to protect the integrity of the product from factory to port.

The company also ensured that the Malaysia facility implemented basic physical security procedures, such as fencing and surveillance, as well as a background screening program for employees. The new company plan ensured that facilities and practices in China were C-TPAT compliant.

In Malaysia, security procedures exceeded those required under C-TPAT. Security was tiered based on the associated threat in the company's global supply chain. In the end, this new strategy saved the company millions of dollars.

Threat Mitigation Options

An effective threat mitigation policy for supply chains has some key components: The first is to have a basic security program in place at all locations to protect all of the company's operations; second is participation in security programs, whether voluntary or initiated by the government; third is return-on-investment (ROI) analysis; and fourth is benchmarking with companies that have good programs in place.

Basic protection. A starting point for supply chain security is to ensure that the company has in place the basic traditional security measures, including personnel screening, physical perimeter and access controls, information security for all facilities and operations, route security for all transportation conveyances, education for awareness, and training for response to incidents. The optimal security program is one that is suited to the specific challenges of the firm and is flexible enough to renew itself as new risks emerge and uncertainties change.

Programs. Active participation in voluntary programs serves several purposes: It helps create a network of secure operations, it establishes a base level of security standards, and it helps raise the overall level of security for global operations. Also, participation in voluntary programs helps build the partnerships between the public sector and private industry necessary to create a secure environment.

The United States has been proactive with initiatives to upgrade trade and transportation security, and many other countries have also passed new legislation or have undertaken new prevention-based initiatives. Most of the initiatives involve approaches similar to those undertaken in the United States. They are based primarily on voluntary efforts by companies to improve supply chain security and include a benefit for companies in the form of a facilitated customs process.

While participation in C-TPAT is voluntary, the disadvantages for those firms that do not volunteer are significant. For example, the higher rates of inspection for those not in the C-TPAT program can add up to 10 to 12 days in a congested U.S. seaport and uncertainty in U.S. Customs processing.

More than 10,000 companies have applied to the program, and at last count, nearly 1,000 had been validated by U.S. Customs and Border Protection. C-TPAT validation typically includes a security review of one U.S- based and one foreign-based manufacturing operation. These reviews can also include the corporation's transportation carriers, third-party manufacturers and freight forwarders, or logistics providers.

Canada's Partners in Protection, Sweden's StairSec, and the European Union's Authorized Economic Operator program contain the central themes of voluntary actions to improve supply chain security and a benefit of facilitated customs process in exchange for security improvements.

International framework. The World Customs Organization is moving toward an international framework for supply chain security and customs processing. This year, it adopted the Resolution on Global Security and Facilitation Measures Concerning the International Trade Supply Chain, which aims to create an international system for identifying businesses that offer a high degree of security in their supply chain operations and to provide customs facilitation for those companies.

Return on investment. According to my experience, more than 80 percent of corporate losses due to theft occur within the supply chain, yet supply chain security spending typically accounts for less than 5 percent of a firm's security budget.

Some firms have implemented supply chain risk-modeling tools to identify financial exposures within their global supply chain. These firms are assessing each of their transportation routes to determine the level of financial exposure due to cargo theft contained within the origin, transshipment, and destination countries; transportation modes; product lines; and other pertinent shipping variables.

Once the data are gathered, transportation routes are ranked by relative risk and the value of revenue flowing through that route. The final step involves conducting a cost-benefit analysis to determine where security measures can be implemented to yield the greatest return on investment.

In doing these calculations, managers should remember to include the fact that insurance premium reductions will follow the lowering of loss rates. In many cases, insurance savings alone provide the necessary capital to fund these countermeasure programs.

Companies must understand, however, that they can negotiate with their insurance company to reduce premiums only if the program can be proven to reduce loss. For example, we recently met with the Brazilian government regulation body IRB and met with underwriters and actuaries on behalf of a Brazilian company. We demonstrated that the company exceeded all security requirements and provided evidence that their insurance premiums were overpriced. The IRB agreed and reduced the rates by 40 percent annually.

C-TPAT limitations. When meeting with insurance professionals, proving that a company is C-TPAT compliant is usually not enough to win a reduction in premium payments. That's because companies have not seen a reduction in overall theft because of C-TPAT.

What has happened instead is that the program has caused threats to shift. For example, before C-TPAT, theft during warehouse storage and container stuffing accounted for a third of a company's losses. After C-TPAT, in most countries, losses at these specific locations and steps in the process have all but disappeared. However, now 90 percent of loss occurs while the product is being moved cross country by truck. This is because C-TPAT does not require increased security on trucking routes within the company's destination country.

Antiterrorism ROI. ROI methodology that could be used for antiterrorism countermeasure spending consists of modeling the financial impact corporations would face should an event occur within their supply chain. There is also data regarding how supply chain disruptions affect stocks. For example, a 2005 industry study of 861 firms over a nine-year period illustrated the significant impact of supply chain glitches. Each glitch had a lasting impact on the stock value of publicly traded firms. Stock value saw a permanent loss of approximately 9 percent after each event.

Benchmarking

A valuable but underused resource in addressing supply chain risk is the collective wisdom of companies that are security industry leaders. With that in mind, we'd like to offer a few suggestions from our research on companies that exhibited exceptional security performance. These leaders had three things in common. They all took a holistic view of security, they learned from prior security incidents, and they remained vigilant.

Holistic view. Companies with good security programs understand that security plays a critical role in the firm. Consequently, they integrate security into the business process in a number of ways. Organizationally, the integration is both formal and informal, manifesting as coordination between business operations and security with regard to issues such as supply chain design and the selection of transportation routes.

This approach is reinforced by regular training exercises that the security organization runs with the business operations end of the company. These exercises engender collaboration between operations and security while giving both parties a chance to practice response and coordination for successful risk mitigation. Ultimately, this integration builds a security culture that permeates the organization and socializes the concept of secure operations.

Prior incidents. Leaders also learn from past security breaches and near misses, building on past experiences to make the organization stronger. For example, in some European countries, hijackers fake a car accident on a trucking route. The plan is to lure the driver from the truck to help the "victims" of the crash.

Because these thieves use many dry runs to perfect their plan, near misses must be tracked just as closely as actual thefts. For example, in one company a well-informed driver failed to stop at a fake accident scene because he recognized it as a trap. However, the driver had been trained to report such incidents. Dispatchers were able to alert all drivers about the scam, and the company was able to conduct a refresher training course on the various schemes employed by such thieves.

Vigilance. Effective security leaders are ever-vigilant to avoid falling into a false sense of security. They know that their supply chain is only as secure as the weakest point in the network.

Security experts live in a world of expanding global operations amid increasing uncertainty and growing threats. The good news is that there are tools and processes that are available to address the challenge.

Operating in emerging markets such as BRIC and dealing with increasing risks can be managed by thoughtfully considering the quantified risks and risk exposure in those particular environments. Successful firms are integrating security into their operations and mitigating exposures before incidents occur.

As the study indicates, security must consider the extended supply chain and expand security to all company sites, internal operations, and perimeters. The entire network must be scrutinized. Finally, it is also important to recognize that the security requirements may vary by the type of market being served—local versus offshore, concentrated versus fragmented distribution base, and robust versus nascent transportation. These measures will make countering vulnerabilities an easier task.

Dan Purtell is president of the supply chain division for First Advantage, a consultant on global supply chain risk, in Phoenix, Arizona. James B. Rice, Jr., is director of the integrated supply chain management program at the Massachusetts Institute of Technology in Cambridge, Massachusetts.

Industry Initiatives

There are a number of industry initiatives that are helping companies find solutions for industry-specific issues. The following are among the initiatives underway today.

TAPA. A nonprofit organization of more than 200 of the largest multinational corporations, the Technology Asset Protection Association (TAPA) has developed cargo security industry standards since 1997. Their Freight Security Requirements (FSR) are contractually mandated by member companies, and freight forwarders are required to have their facility and operations certified by an ISO-certified company trained to conduct the assessments by TAPA under FSR criteria.

Early on, this group realized the security exposures that could come with certifying only main facilities. TAPA, therefore, requires that transportation providers get the designated authority to certify the security of each of their individual facilities, rather than allowing them to get one certification for the corporation as a whole. This program has netted millions of dollars of loss reduction; the average TAPA member company has reduced losses by 40 percent by having its supply chain certified.

ACC. The American Chemistry Council (ACC) created the Responsible Care Security Code as a mandatory facility security program to protect chemical-specific facilities, transportation systems, and handling systems. The security code addresses three levels of security—cyber, facility, and transportation—by requiring vulnerability assessments, security system enhancements, and an independent compliance verification. The program has been recognized as a model for the chemical industry by various federal, state, and local government organizations, including the Department of Homeland Security. This industry group is lobbying Congress to pass legislation to create security standards for all chemical companies, and boasts that its members have already added more than $2 billion in investments to improve site security since late 2001.

Synopsis

Before companies enter new markets in foreign countries, they must understand the risks of operating supply lines in unstable environments and how to counter them. This has been the subject of a multiyear study by First Advantage, completed earlier this year and released here for the first time.

Focusing on transportation route risk, assessments were conducted in 45 countries. These supply chain risk assessments typically included a review of the company's manufacturing locations, trucking operations, freight forwarders, third-party logistics warehouses, container-stuffing operations, and the supporting seaports and airports. The study looked at the extent to which corruption was an issue in these environments.

The study also used First Advantage's Global Loss Repository—a database of cargo theft data from around the globe—to create loss rates for cargo transiting through respective countries. We also devised a weighted C-TPAT exposure matrix for the survey; it quantifies risks associated with anti-American sentiment or other hostility to Western governments.

The study incorporated all of this information to develop a profile of emerging-market country risk. The results were surprising. For example, Russia and Brazil are among two of the highest risk countries in terms of supply chain theft. Incidents commonly involve government representatives including police, military, and customs officials. However, in terms of C-TPAT, these countries are given a "low" threat rating because the governments and residents are on amicable terms with the United States and are not hostile to Western culture.

The study indicated that, within the global supply chain, a cookie-cutter approach to security has led companies to overspend in low-risk countries such as China and underspend in high-risk countries such as Malaysia and Indonesia.

Cargo Theft and C-TPAT Exposure Ratings

COUNTRY	CORRUPTION INDEX	SUPPLY CHAIN THEFT EXPOSURES	WEIGHTED C-TPAT RISK
Brazil, Russia, India, and China			
Brazil	3.7	Severe	Low
Russia	2.4	Severe	Low
India	2.9	Elevated	Elevated
China	3.2	Guarded	Low
Other Notable Growth Countries			
South Africa	4.5	Severe	Guarded
Poland	3.4	High	Low
Turkey	3.5	Elevated	High
Indonesia	2.2	Severe	Severe
Thailand	3.8	Guarded	Guarded
Nigeria	1.9	Severe	Severe
Malaysia	2.2	Severe	Severe

Source: First Advantage Corporation; CIA World Fact Book; Transparency International

Magazine Highlights| Marketplace | Library/Links | Events | Beyond Print| Today's News| Forums | Feedback|Subscribe | Advertise | Reader Service | Writer's Guidelines| Contact Us | Security Industry Buyers Guide| ASIS

back to Security Management Online

Worldwide Headquarters USA
1625 Prince Street, Alexandria, Virginia 22314-2818
email: Member Services
703-519-6200 | fax 703-519-6299 |www.asisonline.org
For permission email: Sherry Harowitz.
Report any broken links to the webmaster.