

Stopping the Highway Bandits

How Security Convergence and Global Security Practices Are Helping to Cut Billions in Supply Chain Theft Each Year

*By Gerrit Wassink, Director
Strategic Accounts Logistics
Tyco Fire & Security / ADT*

In the good old days, back in the late 20th century, highway bandits never had it so easy. That's when global supply chains had security holes in them so large you could literally drive a stolen big rig through one. Not that goods manufacturers hadn't noticed. Yearly losses were running in the tens of billions of dollars. Even today the total annual cost of cargo theft worldwide is estimated to be as high as \$60 billion. Problem then was that corporate security and logistics teams had not yet joined forces to systematically fight the crooks. In addition, many legitimate stakeholders in the world's many supply chains considered theft just a cost of doing business.

Today that has changed dramatically, thanks to a call made in 1997 by a frustrated logistics manager at Compaq Computer (now part of Hewlett-Packard) in California's Silicon Valley. Gary Alton, then a Compaq divisional security manager who took the call, listened as the caller complained about thieves stealing truckloads of PCs and laptops. Not just a truckload: "Truckloads."

When Alton checked with his counterparts at other high-tech firms, they shared similar woes of tractor-trailers stolen from just about anywhere. Truck stops. Loading yards. Desolate highways. Theft of a single truck's payload could cost \$1 million or more. Alton's conversations with his colleagues led him to convene the security heads from 25 other local high-tech companies and, in a few months, the Technology Asset Protection Association (TAPA) was born.

Global problem, global solutions. Now, more than a decade later, TAPA has expanded its scope and name, calling itself the Transported Asset Protection Association. Its 600-plus member companies span affiliate organizations in Europe, the Middle East and Africa (EMEA), Asia and Brazil. Together its members have annual sales of nearly a trillion dollars, with much of that value in goods of all kinds transported from one part of the world to another.

With that kind of shipping volume comes clout. Early on, TAPA set up a security certification program based on standards it calls Freight Security Requirements (FSRs). It forced freight forwarders, logistics and transport companies to hire outside firms to audit their security practices. The TAPA proposition was simple: Those who gained TAPA certification could qualify to gain more of TAPA members' business than those who didn't. Today some commercial companies require TAPA certification of their logistics companies in order to do business with them.

But the FSRs, which focused on securing freight forwarding facilities, turned out to be just a start. TAPA members realized that 85 percent of cargo is lost on trucks. That's why it rolled out its



Photos courtesy: TAPA EMEA

Truck Security Requirements (TSRs) in 2006 and plans to introduce Cargo Terminal Security Standards next.

New era of cat and mouse. TAPA grew out of a crying need for theft protection by industries producing compact, high-value goods that are easy to steal and easy to fence. A single box of specialized computer chips, for example, can cost hundreds of thousands of dollars. Apparel, smart phones, watches, jewelry, gaming consoles, pharmaceuticals, plasma televisions are other goods prized by thieves. Small wonder that the world's leading manufacturers of these products are TAPA members.

TAPA reported in 2007 that an independent audit of 24 members showed savings of nearly \$500 million – about \$20 million each – over five years by applying TAPA standards. But the fact is that as the volume of world trade grows and as borders become more open, thieves have become more organized and sophisticated, able to steal goods seemingly at will. In fact, many gangs can “steal-to-order” digital cameras, athletic shoes or any other category of goods, depending on what their “customers” might want.

The European Union (EU) is a prime example. It now spans 27 countries with a forecasted \$18 trillion in economic activity this year and about one-sixth of that exported outside the region. The Transported Assets Protection Association (TAPA) estimates that about \$12 billion in goods will be stolen, much of it by criminal syndicates aided by insiders and loose security practices. That physical loss not only hurts the profits of the source companies but also is a loss of irreplaceable sales opportunities.

In today's interconnected global economy, companies want to know where their goods are. They have increased expectations of accessing that information 24x7 – even being able to see their goods in transit. But highly organized gangs – often working with insiders – want to know, too. Using increasingly sophisticated methods and technologies, both sides play a high-tech game of cat-and-mouse to prevent theft on the one side and to steal the goods on the other. The playing field is the entire supply chain. At any point along it, wherever goods sit, wherever they are transferred and wherever they change possession, they are at risk.

From reactive to proactive. Prompted by the TAPA standards, the logistics industry has made huge investments to thwart theft in recent years both in technologies and in processes. Some top logistic providers have gone much further than TAPA's standards. They're finding that providing tight security to the high-value goods of its customers today is a competitive edge. Tomorrow they assume it will be a market mandate.

In the meantime, security professionals have and will continue to deploy the usual prevention, intervention and investigation tactics and accompanying tools. Access control, CCTV, electronic

Cargo Theft “Hot Spots” *Around the World*

- Sao Paolo & Rio de Janeiro, Brazil
- Kuala Lumpur & North Malaysia
- Mexico
- India

In the U.S.

- Atlanta, Georgia
- Miami, Florida
- Chicago, Illinois
- Los Angeles, California
- New York-New Jersey
- Tennessee
- Virginia

article surveillance and tracking, unmarked boxes and pallets, fire and intruder alarms, monitoring and GPS devices are all part of the mix. What's changing in this toolset are the technologies inside them and, more and more, the technologies networking them.

The components of these security devices, systems and solutions, for example, are becoming highly integrated, putting more and more "smarts" inside them. Internet Protocol (IP)-enabled video cameras can have chipsets in them with analytical capabilities that can provide pattern recognition of, say, boxes on a moving conveyer line and even facial recognition of logistics personnel. That's in contrast to analog cameras and DVRs without built-in intelligence and useful only for extremely tedious forensic investigations.

To further illustrate, if the camera is monitoring the line and suddenly a box is missing, it can send an alarm over the company's network (or even encrypted via the Internet) to a centralized monitoring system or station for investigation. Best yet, the facility's entire network of IP video cameras could be interconnected with barcode scanning or RFID tag data of the moving packages. The converged data makes it easy to automate an ultrafast frame-by-frame video search of the entire video data pool in seconds to find the "last seen" scene of the missing package.

That kind of insight can help make catching the thief much more likely – or, in the very least, help prevent such theft from happening again.

As for networking, IP means the central station can be anywhere on the planet. From there, it can signal an onsite guard's wireless smart phone that something's amiss and even provide the video clip to help investigate.

Among other examples of IP networking's applications are pan-regional access control systems. Until now, access control was typically localized, so drivers would need several badges to access different sites. Or, they'd borrow them from other drivers. Either way makes for huge security risks and big administrative overhead. A single IP-networked system can improve security and optimize operational efficiencies across the company.

This convergence of security and information technologies has many implications. One of the most profound is this: Convergence can enable security professionals to be less reactive to events such as alarms and more proactive in their fight against crime via data-driven, predictive security models. This way, security professionals – teamed with their logistics counterparts – can neutralize risks before they happen, say, by designing loading patterns and processes so goods are not left exposed. They can use predictive security models to reduce the probability of risks. Or, they can even better determine what levels of vulnerability are acceptable.

Convergence can enable security professionals to be less reactive to events such as alarms and more proactive in their fight against crime.

Keeping it all simple – and consistent. Logistics by its nature is a distributed enterprise. As such, it needs transportation, warehousing and material handling capabilities, of course. But to scale globally, it needs extraordinary information management and communications capabilities to match. Technology, of course, is the answer. Someone once joked that Fedex is a technology company that ships goods to pay for all its technology. While certainly not true, that aptly describes the extensive technology capital investments of all big logistics companies today.

Since logistics companies are in the business of moving goods, securing those goods from loss and theft is also inherently part of what they do. It only makes sense then that eventually – and inevitably – their operations people, information technologists and security professionals would all meet at the table has they now have done.

While that coming together has helped make great strides in better protecting the valuable goods of their customers, they still have a primary mission of getting the goods where they need to go, with delivery when promised. That in itself is a tall order on a daily basis. That's why it can help to have strategic partners supporting their efforts.

These partners should be logistics sector experts who fully understand the market and customer dynamics and solutions. They should know that service levels drive performance pressures and quality of service is a logistics company's key competitive differentiator. They should think beyond borders and time zones, but realize both can provide logistic challenges nonetheless. Most importantly, they should be able to imagine integrated solutions both across systems and business processes.

Along with technological advances, TAPA has helped the logistics industry take giant steps toward standardized security practices worldwide. Both technology and standards are important to keeping worldwide security as simple and consistent as possible. Both make the global application of converged security solutions not a cost of doing business, but an investment in the business – with payoffs in better operational performance and greater customer responsiveness and satisfaction.

Some day, we'll look back on the times we live in now and call them the "good old days" too. Thieves will be with us then just as they are now, ever adaptive as they can be. But with the continued evolution of technologies and standards, their percentage take of the world's material value stream will be ever smaller, we can be sure. ●

About the author: *Gerrit Wassink, an active TAPA EMEA member, is a 20-year veteran of the logistics industry, with major customer account management tenures at Fedex, TNT and Penske. Before assuming his current role as Director of Strategic Accounts, Logistics, for Tyco Fire & Security / ADT, he helped lead Tyco's pioneering supply chain RFID efforts. Garrit can be reached at gwassink@tycointl.com.*