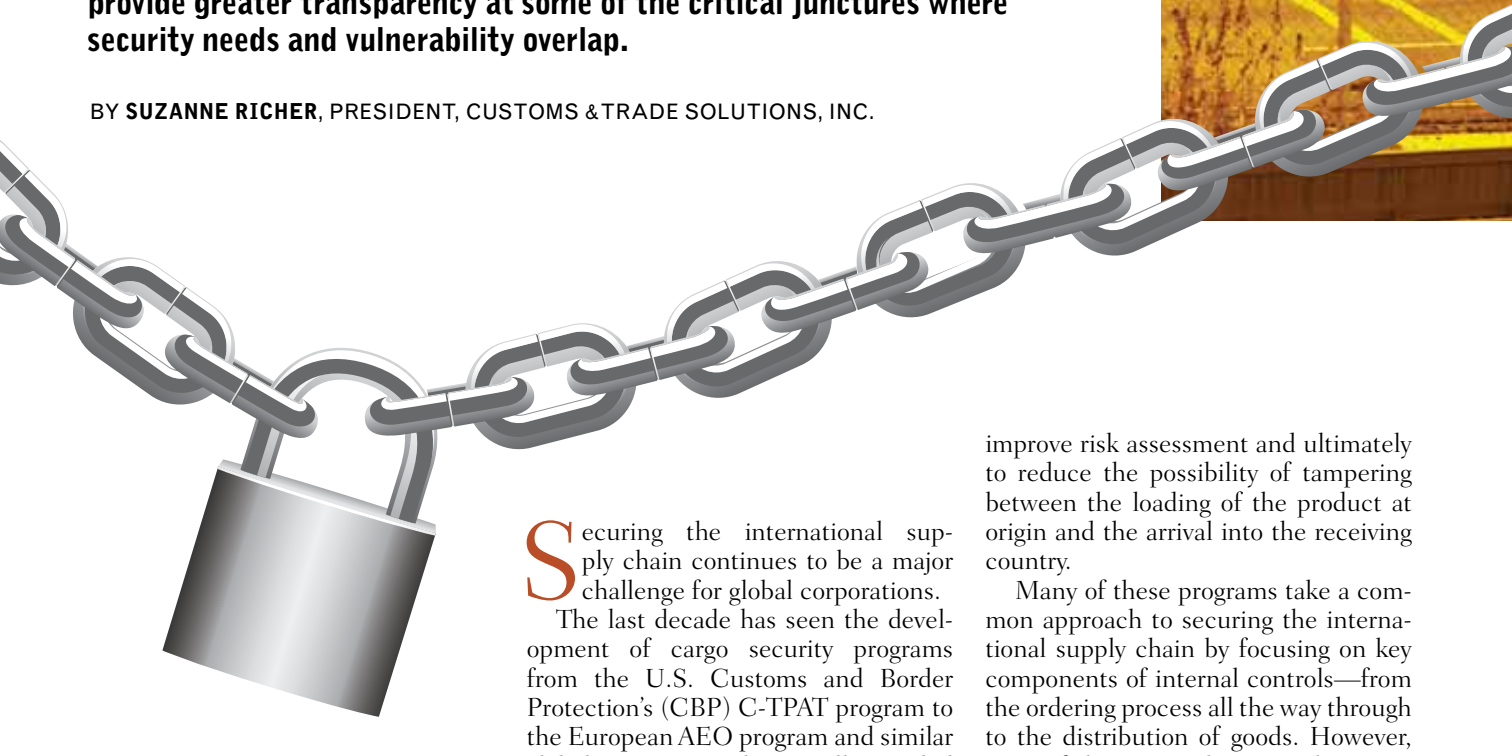
# SECURITY TECHNOLOGY: Closing the vulnerability gap

**Successful integration of technology into a supply chain security strategy will expedite border crossing wait times and reduce insurance costs. Fortunately, new technologies continue to be introduced that provide greater transparency at some of the critical junctures where security needs and vulnerability overlap.**

BY **SUZANNE RICHER**, PRESIDENT, CUSTOMS & TRADE SOLUTIONS, INC.



Securing the international supply chain continues to be a major challenge for global corporations.

The last decade has seen the development of cargo security programs from the U.S. Customs and Border Protection's (CBP) C-TPAT program to the European AEO program and similar global initiatives. These well-intended global programs seek to add transparency to the international movement of goods, tying in the sharing of electronic data between governments to improve risk assessment and ultimately to reduce the possibility of tampering between the loading of the product at origin and the arrival into the receiving country.

Many of these programs take a common approach to securing the international supply chain by focusing on key components of internal controls—from the ordering process all the way through to the distribution of goods. However, most of the activity between these two points is outsourced to business partners who then become responsible for the safety and security of the freight while it's in their possession.

As any global supply chain manager is well aware, this extended process heightens supply chain vulnerability and opens the door for tampering and fraud along the entire supply chain, creating a situation that's well beyond the scope of a corporation's internal controls and audit checkpoints.

We have found that companies that incorporate new technologies in conjunction with participating in these initiatives have created an opportunity to benefit by reducing their own costs and risks to the corporation. And fortunately, new technologies continue to be introduced that provide greater transparency at some of the critical junctures where security needs and vulnerability overlap.

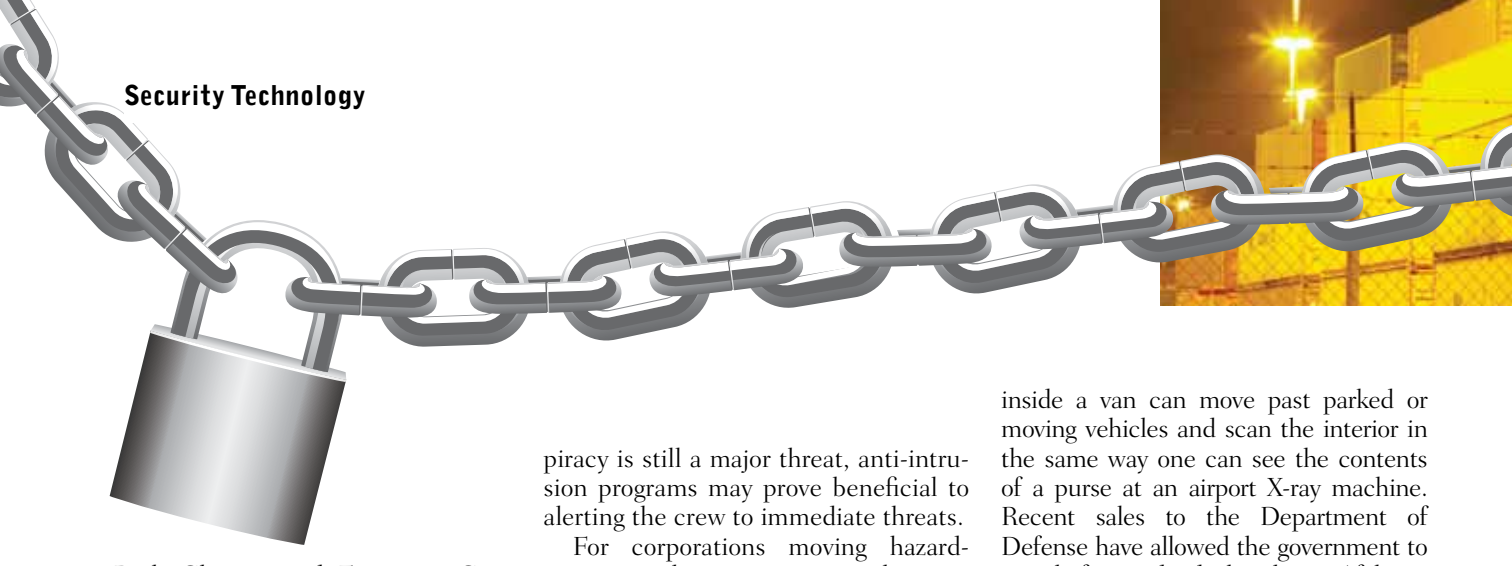
## IMPROVED CONTAINER DATA SECURITY

CBP has successfully updated the management of data for risk assessment on full containers bound for the U.S. by implementing the Importer-Security Filing (ISF) requirements prior to loading in the foreign port.

While obtaining this data in advance of shipping has improved security targeting, tying it to the actual movement of the container will improve the visibility of the entire shipment. For example, the European funded INTEGRITY project is an IT data exchange platform titled the Shared Intermodal Container Information System, or SICIS. A recently introduced extended version of SICIS will track a container from origin to destination, linking the container monitoring data with vessel tracking information via satellite.

The result is a unique view of both the vessel and the container, marrying logistics and security data. SICIS is intended to integrate with the European cargo security program Authorized Economic Operator (AEO), similar to the U.S. version of Customs-Trade Partnership Against Terrorism (C-TPAT).

Currently in use for containers moving from China to Europe, the next proposed step will be able to link data from the container to the receiving CBP officials, allowing clearance capabilities to take place earlier in the supply chain, possibility while it is still on the water.



Both Chinese and European Customs have expressed interest in participating in these discussions, and the results may be an incentive for other trade lanes to be approved for this technology that is set to improve lead time for a product by reducing the time it remains at the border.

## NEW TECHNOLOGY FOR PORTS

New and improved technology is now available for the marine industry to promote greater visibility of ports, offshore installations, and security zones. Designed for both military and civilian markets, updated diver detection sonars can pick up underwater swimmers or divers that are approaching a vessel.

New and improved range performance capabilities allow the sonar to detect an underwater diver through a "signal-to-noise ratio" using pulse compression or chirps. This same system can be adapted to fixed or mobile systems, whether for underwater detection near a vessel or placed near port entrances and exits where maneuverability is important.

For corporations moving product through international waters where piracy is still a major threat, anti-intrusion programs may prove beneficial to alerting the crew to immediate threats.

For corporations moving hazardous materials via ocean, a newly introduced chemical warfare detector with closed circuit TV cameras will soon be in place in the Port of Providence, R.I. Developed by Smiths-Detection, the video management system will alert authorities to chemical hazards in the port area, linking the data feedback to real-time video feedback.

This system will allow the port to remotely identify vessels with chemical spills, accidental or otherwise, and integrate data management and immediate warning systems, sending the data to emergency response teams for evaluation and crisis response capabilities.

## SCANNING VANS

Since the discovery of shoe bombs and liquid explosives, the world of X-ray capabilities has continued to improve. X-ray scanners are in place in over 150 countries today, allowing customs officials the ability to scan for explosives, weapons, narcotics, and contraband in a non-intrusive way.

Body scanners are next in line, with the continued debate playing out on just how intrusive these machines are. But the most interesting scanner now available on the market has similar capabilities and is being driven through the streets of the U.S.—scanning vans.

American Science & Engineering (ASEI) is the developer of the Z Backscatter Van, or ZBV as its known in the business. ZBV capabilities mounted inside a van can move past parked or moving vehicles and scan the interior in the same way one can see the contents of a purse at an airport X-ray machine. Recent sales to the Department of Defense have allowed the government to search for road-side bombs in Afghanistan and check for vehicle-based explosives here in the U.S.

The ZBV is a powerful tool for scanning vehicles for drugs, human bodies, or other illegal items, making it a desired technique of security programs for law enforcement and border control activities. The company has reported the sale of 89 of the vehicles through June of this year, delighting law enforcement and shareholders while raising alarms with privacy advocates.

For supply chain professionals, knowledge of which ports are utilizing this tool for stronger targeting of enforcement will be helpful when outlining their risk assessment strategies by trade lane.

## BIOMETRICS AND ACCESS SECURITY

Biometric identification via a hand or fingerprint has been a long established system, but not widely used in industries outside of pharmaceuticals or similar businesses.

Updates to the reading mechanisms now allow the full hand to be scanned, capturing data on the width, length, and size of the hand, palm, and fingers. The systems, which can be established at port gates or at the entrance ways to distribution facilities, no longer need to capture the actual fingerprint, as the unique size of the hand, tied to an individual code, will accurately verify identification.

These systems work whether the hands are clean or dirty, allowing for ease of use for many industries. The unique pin can be tied to payroll or

**The Z Backscatter Van moves past parked or moving vehicles and can scan the interior in the same way one can see the contents of a purse at an airport X-ray machine.**

used to track employees as they move from one building to another. Taken to the next level of security and technology progress, the biometric capabilities mixed with smart cards can move from opening doors to opening sensitive files, allowing for greater confidentiality of proprietary company information.

Supply chain managers may find these updated biometric capabilities supportive in both access and IT security elements—at the cost of a single system update.

## TIGHTENING BORDER CROSSINGS

Recent outbreaks of violence south of the border are pushing CBP officials to increase exams for U.S. bound shipments, especially by truck. To help defray the risk, CBP has completed the full implementation of the Border Detection Grid. Under development since 2008, the project uses a grid of advanced sensors and detection capabilities to monitor cross-border activities.

The program allows the classification of the incident to reflect the level of risk, rating the detected movement to be from friendly forces, small animals, or even the weather. This capability supports the border patrol unit to establish a reaction plan based on the risk identified and allows one person to monitor up to 10 miles of border.

**Supply chain and security professionals who focus only on doors or files miss the most important objective—securing the business.**

With enhanced security capabilities using fewer resources, supply chain professionals can focus on the risk to the shipment earlier in supply chain planning and apply resources to lowering the risk of intrusion farther from the border.

## START BY ASSESSING RISK

Risk within global supply chains continues to be influenced by external factors, most of which are out of the control of the supply chain professional. Those with best-in-class programs keep cargo security programs at the top of the CEOs focus by tying risk to other corporate objectives, such as branding and intellectual property rights.

Supply chain and security professionals who focus only on doors or files miss the most important objective—securing the business.

Working with cross-functional teams to ensure all threats are identified, from procurement to counterfeit products, will protect a company's reputation, as well as its people, customers, suppliers, and contractors. The challenge is to integrate the security programs with the physical and logistical risk management programs.

Successful integration of new technologies may expedite border crossing wait times, and reduce insurance and other associated costs to the company. Luckily, there is no shortage of new technology programs to help corporations reach that goal. □

*Suzanne Richer is president of Customs & Trade Solutions Inc., a consulting firm specializing in international trade and cargo security programs (smricher@ctsiadvisors.com).*

## Developing a strategy: Put a security integrator to work

DEVELOPING NEW STRATEGIES FOR COMBATING SECURITY threats within the supply chain continues to be at the top of the list for most logistics professionals, especially those moving freight across borders and around the globe.

From our experience working with global shippers, collaboration with business partners outside the organization is the key to success. Threats can only be reduced by the ability of the port, security force, police, or other enforcement officials to reduce the risk associated with an identified vulnerability in the supply chain.

Implementation of many of the new and upcoming technology capabilities will depend on the company's established security budget as well as the threat and vulnerability assessment of the global supply chain.

One essential best practice to consider while exploring new security technology opportunities includes working with a security integration partner for any new construction project. Many corporations forget to include security groups during the design and construction stages of new buildings such as warehouses and distribution centers.

The opportunity to reduce the cost of implementing security programs could be greatly reduced when integrated into the planning, yet could be cost prohibitive post construction.

The role of the security integrator should include analyzing, designing, and building a technology plan for current operations with an eye on where the company will be in five or 10 years. Assessing needs with a future view will lower costs of integrating various levels of technology. —*Suzanne Richer*