Every Link in the Chain:

A rose is a rose is a rose.

Unless it's a Porsche or Prozac, a porterhouse or pansies, motor parts or plasma screens, petroleum or Harry Potter movies, the nation's budget or frozen peas.

Or anything that's in the vulnerable and valuable worldwide supply chain.

And as diverse and complex as the supply chain, security of it is as complex with local, national and international regulations, myriad threats as well as an everchanging mixture of policies, procedures and technologies.

At Ryder System, the mission is to help customers focus on optimizing performance in their core businesses by implementing broad-range, innovative supply chain solutions, which includes security, says Ryder System's Bill Anderson, group director of international safety, health and security.

Ryder's warehousing, transportation and integrated logistics solutions are the force behind many of the brands and favorite products used every day. Its supply chain solutions are quietly and effectively at work around the world, helping companies compete more aggressively and ultimately resulting in more value and lower costs for the end consumer.

Along the chain, it is essential to "know who owns the various companies, who are the shippers. If something changes or comes up in Shanghai, the information must be communicated immediately," says Anderson. "It's very much a matter of protecting cargo and mitigating losses as well as understanding what could happen to a brand name and a firm's reputation" if there are problems along the chain. "We must always monitor the various standards which tend to be mainly in the U.S. and Canada."

DIVERSITY OF MEASURES

There are numerous security measures that firms such as Ryder employ, from work instructions for pallets to the integrity of cargo seals to use of security video at warehouses and distribution centers.

But Anderson is no go-it-alone security executive. Programs such as Customs-Trade Partnership Against Terrorism or C-TPAT and Partners in Protection or PIP set a higher bar for everyone, thanks in part to terrorism concerns. C-TPAT is a voluntary government-business initiative that builds cooperative relationships to strengthen and improve overall international supply chain and U.S. border security. C-TPAT recognizes that U.S. Customs and Border Protection (CBP) can provide the highest level of cargo security only through close cooperation with the ultimate owners of the international supply chain such as importers, carriers, consolidators, licensed customs brokers, and manufacturers. C-TPAT traderelated businesses have reduced the number of CBP inspections with reduced (that is less expensive) border delay times and priority processing for CBP inspections, among other higher security advantages.

Also a voluntary program, Partners in Protection (PIP) is a Canada Border Services Agency program, that now is similar to C-TPAT, and that enlists the cooperation of private industry to enhance border and trade chain security, combat organized crime and terrorism and help detect and prevent contraband smuggling. There are electronic cargo release aspects of the programs that have bottom line benefits to product manufacturers, carriers, third parties and final sellers.

Things can still happen, points out Anderson. "True incidents are just the tip of the iceberg. What is underwater? You must continue to test the systems, put in place additional measures and evolve the policies and procedures. Odd situations are redflagged and addressed."

There are numerous efforts to protect and track cargo along the supply chain. For instance, Mexico-based Grupo Hemas has teamed with Savi Networks to provide realtime intelligence and responsiveness to cargo shipments. In the U.S., Hemi-Group will leverage SaviTrak intelligence service, GPS, environmental sensors and existing cellular infrastructure to automatically monitor the location, security status and condition of shipments.

Freshness of food in the supply chain is the aim of a similar application of the technology with Royal Food Import Corp., an export firm specializing in the food market, using the technology for its automated wireless monitoring service to improve the endto- end visibility, security and freshness of fruits and vegetables in cargo containers by truck, rail and ocean vessel from production sources in Thailand and China to distribution centers in the United States.

FOLLOWING THE FOOD CHAIN

Supply chain security for cold and frozen products, including medicine, is yet another story. Unique technology here can include multi-tasking self-contained, probeless temperature monitors with automatic Adobe PDF file generation capabilities and a USB communications interface. It comes from Sensitech, a wholly owned subsidiary of Carrier Corp., itself a business unit of United Technologies Corp.

In another application that centers of food and the supply chain, Airberg Ltd., which serves supermarkets and airline caterers in the Middle East, is the United Kingdom's leading specialist exporter of temperature sensitive, short shelf life foodstuffs by air and sea. With an in-depth knowledge of the Middle East including local customs and importing procedures, Airberg conducts close to 75 percent of its business in this region, but also delivers British specialty foods to embassies, High Commissions, and top hotels around the world. Exporting up to 150 tons worth of goods each week, Airberg relabels, repackages and ships merchandise from its 16,000 square foot facility in East Sussex. To conform to governmentregulated security requirements, ensure asset protection and provide a safe working environment for employees, Airberg has deployed a high-definition surveillance system from Avigilon at its headquarters and neighboring 15,000 square foot storage facility.

Similar to the U.S. and Canadian regulations, the UK's Aviation and Maritime Security Act states that all airfreight consignments must either be screened or originate from a Department for Transport accredited "known shipper" before being loaded onto an aircraft. To become a known shipper, exporters must undergo an annual inspection. Cargo from known shippers is considered secure and can be placed on an aircraft without further checks, dramatically expediting the shipping process. "By deploying an advanced, high definition surveillance system that captures even the smallest detail, we can confidently achieve known shipper status, saving us the inconvenience and expense of having our cargo checked every time we ship goods by air," says Tony Coates, co-owner at Airberg.

Still, the supply chain is traditionally vulnerable when it comes to products such as pharmaceuticals, where millions of dollars of product, brand reputation and life-anddeath situations all can come together.

There is theft, of course. But there also is counterfeiting and diversion tactics.

Recently, NanoGuardian entered into a license agreement with Capsugel, a division of Pfizer, in providing capsule-based drug delivery systems, which gives Capsugel global access to technology for the protection of capsule-based medications against counterfeiting and illegal diversion. The approach works directly on capsules, tablets, vial caps and single use syringes to provide a layered security strategy consisting of overt, covert and forensic security features at any point in a manufacturer's supply chain.

PHARMA PARTNERSHIP

In addition, DHL, the logistics company, in partnership with American Airlines Cargo, agreed to support pharmaceutical industry customers as they prepare to implement a new U.S. regulation aimed at 100-percent piece level screening of cargo carried on passenger aircraft.

With half a year to go before the regulation takes effect, which could cause major delays of shipments, both companies have started offering joint trainings to educate pharmaceutical customers on how best to comply with the Transportation Security Administration's Certified Cargo Screening Program.

"DHL's partnership with American Airlines and the TSA is designed to provide important information to customers regarding the most efficient way to screen freight to meet the new mandates, while also meeting critical delivery deadlines," says Gary Schultheis, senior vice president Airfreight DHL Global Forwarding, Americas.

Most recently, the biggest loss in the drug industry occurred just two months ago when members of an organized gang cut through an Eli Lilly & Co. Connecticut warehouse roof, disabled security and stole $75 million in prescription drugs for probable resale on the black market. Most of the previous drug supply chain robberies involved cargo taken from trucks or containers, though warehouses, especially on the east coast, have also been hit. Ironically, such incidents are mostly in the U.S., with the rest of the world escaping such crimes thanks to other governments' healthcare policies which hold down the cost of drugs and encourage a more structured pharmaceutical industry.

There are unique supply chain security assignments ranging from floral shipments to dry ice needs.

For instance, horticulture and flower industry auctioneer FloraHolland now tags and tracks trolleys that transport flowers and plants throughout the supply chain. Omni-ID, and partner Mieloo & Alexander, specializing in RFID-enabled process improvement, developed an UHF RFID solution to meet FloraHolland's requirements. The company has six auction centers, a nationally operating intermediary organization and a transit department. There are 270,000 auction trolleys used for logistical processes throughout the entire supply chain. As part of the redesign, over the next two and a half years, every auction trolley will be tagged with a passive UHF RFID tag that would work well near waterfilled buckets, in a high humidity environment, and with obstructed line-of-sight visibility of the tags. "The technology was able to withstand FloraHolland's process and heavy industrial environment as well as those between and with supply chain partners," says Johan Star, advisor supply chain logistics for FloraHolland.

PASSIVE AND ACTIVE RFID

In a much bigger supply chain security operation using active RFID, Unisys Corporation is one of four companies selected by the U.S. Army Program Executive Office's Enterprise Information Systems for continuing technology that resulted in the creation of one of the largest active RFID networks in the world, the Army's RFID In-Transit Visibility system. It provides the military with instant access to information about equipment and supplies, enhancing readiness and safety.

Currently, RFID tags are attached to approximately 125,000 shipments of military supplies each week. As shipments pass through field locations, fixed and handheld readers send and receive data to and from the tags. This data is made available to the military for greater visibility into the location and status of shipments

By the way, ABI Research shows the outlook for RFID is good for steady growth through the next five years. "Not all segments of the RFID market are created equal," adds ABI's Michael Liard. "To 2014, the greatest growth will be found in RTLS (real-time location systems), baggage handling, animal ID, and item-level tagging in fashion apparel and retail." Also worth watching is slow but continued progress in retail supply chain management, and multiple flavors of asset management that leverage RFID technologies, including specialty passive UHF tags.

Another unique supply chain security assignment centers on post-earthquake Haiti.

There the Salvation Army is replacing handwritten paper index cards with hightech barcode technology to ensure that more than 4,000 families the agency serves efficiently receive food, shelter and medical supplies. UPS has donated the technology and adapted it for disaster relief supply distribution. The system is based on UPS's Trackpad technology, which UPS customers use to track packages within campus environments as the packages move from the loading dock to distributed offices for delivery.

Salvation Army staff members will now be able to confirm what goods each family receives by tracking the information embedded in a laminated card that bears unique barcodes tied to the number of family members, their location in the makeshift camp that has sprung up in an adjacent soccer field and their needs.

There is also a digital supply chain. Among improvements in this area, a joint project involving Brocade and Digiplug, a provider of end-to-end digital distribution solutions for rights holders and digital content retailers worldwide, is digitizing customer assets and building a new high-performance, highspeed data center. With clients including Universal, Sony and Warner, Digiplug is working on the boom in digital services that has drastically changed the way entertainment content is funded, manufactured, marketed, distributed, monetized and consumed. For the media and entertainment industry, recorded music was the first to go digital, but now the whole industry is focused on digitization of its content. To cope with the huge amount of data, Digiplug needed to securely interconnect between its two data centers and its headquarters in central Paris via a dedicated fiber link.

DIGITAL SUPPLY CHAIN NEEDS

Following a document through its chain is a crucial security need, according to John Landwehr, responsible for overseeing Adobe's information assurance solutions for securing the information lifecycle. "That includes not only new and enhanced capabilities within the desktop product, such as creating secure eEnvelopes, but also new server-based solutions, primarily the Adobe LiveCycle Policy Server," he says. Use of default and custom policies extends document protection beyond delivery, allowing the document creator to specify the authorized users and uses, and control all aspects of what happens to a document.

Landwehr stresses pillars for confidentiality along the supply chain of a document. "We see increasing concern for IT protection inside the firewall and outside of it."

Such technology can create an audit trail of who has opened or tried to open the document; revoke contents; virtually shred documents; enforce version control; turn off an old version; and authenticate that content has not been tampered with. There is also digital signature technology.

The certification is used at the U.S. Government Printing Office in critical documents like the FY 2011 Federal Budget.