

# Don't Unchain that Supply Chain 'Melody'

By Bill Zalud, Editor Emeritus

**S**o what do the Righteous Brothers, grapefruit, Cymbalta, packaged software, toy jewelry, Callaway golf clubs, Prada purses, Cowboys and Aliens and car parts have in common?

Everything, when it comes to theft, counterfeiting, terrorism, diversions, health threats and other illegal and unethical practices up and down the supply chain.

The key word in supply chain security is "chain." Products move from hand to hand, from factory to warehouse to distributor, from country to country, across the sea in containers, inside of trucks and railcars, on pallets, often then into the hands of others at production or assembly, and once again on

to a warehouse or distribution center. More recently, supply chain security has expanded to include data and documents. The supply chain can sometimes be simple; at other times, it is complex and a detailed process or series of processes. The challenge, however, would surely make those Righteous Brothers lament losing their lovin' feeling.

The threats can be simple or complex, too. A kid in Jersey City ripping the latest music hit from Adele gives off a different vibe than an equally illegal CD production mill in the Ukraine. Organized gangs, who obtain product or labels through the chain or through counterfeiting, can pump out millions of pills or purses. The pharmaceutical industry estimates that more than 10 percent of product has been diverted or is counterfeit. And buy-

ing a fake handbag on Canal Street in New York City has become a tourist pleasure.

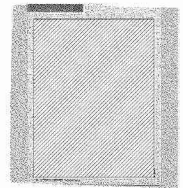
## SAFETY AND TERROR CONCERNS

But things can get decidedly dangerous. Fake drugs can kill. Lead-covered toys can harm. Containers on ships, supposedly with car parts, can blow up in thousands of faces in the case of a dirty bomb. And those grapefruits? There is evidence that terrorists adulterated them when they were imported into Israel in a premeditated terrorist attack.

Protecting the food chain is growingly important, especially at warehouses and distribution centers. And the technology can also help the operation.

In Aurora, Colo., Whole Foods is using a Brivo cloud-based access control system at

HillFresh, a major Dutch fruit and vegetable distributor, has deployed megapixel camera technology to improve security and operations and protect the supply chain.



its warehouse to improve security and operations in the 110,000 square foot facility and adjoining bakery.

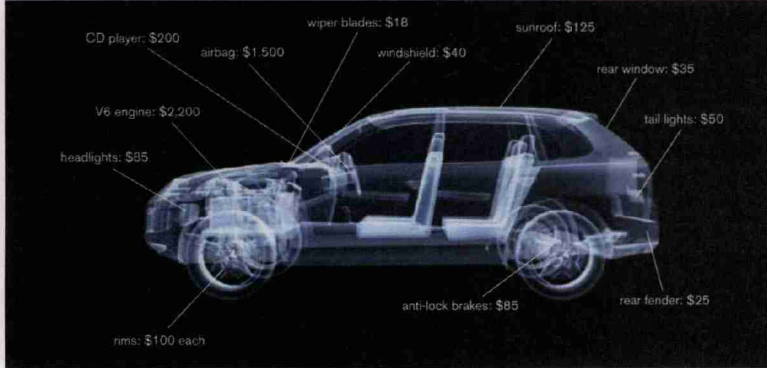
Previously, the warehouse relied on lock and key and keypads to manage access con-

trol for the 170 employees of the combined operations. "The old systems weren't very effective," comments Mario Ruiz, associate facility team leader. "We couldn't update our records." Ruiz and his team researched

alternatives, settled on a new system and were set to go until one of their suppliers introduced them to Rueben Orr from Security Install Solutions. Orr gave the Whole Foods team a demonstration of the WebService solution and very soon the system they had just purchased was on its way back to where it came from.

The Aurora Whole Foods warehouse handles produce, meat, cheeses, seafood, bulk items and more through its 23 bay doors for shipping and receiving. Along with the bakery, the two facilities supply 28 Whole Foods stores in a four-state region. Every main entrance is covered by the Brivo system and Ruiz serves as the main system administrator.

Ruiz uses the system to divide the employees from the warehouse and bakery, as well as outside contractors, into separate groups depending on each person's specific access needs. He uses an alert feature to



Counterfeit car parts too easily get into the supply chain. Sold parts can often total more than a new vehicle.

### Protecting the Coastline: Supply Chain Assignment

**A** coastal remote monitoring program for the Alabama Department of Conservation and Natural Resources, Marine Resources Division, is using thermal cameras with the ability to withstand wet conditions, high temperatures and corrosive salt water to capture high quality images in extremely tough environments along Alabama's 200 miles of coastline.

The assignment includes ships bringing in goods from off shore.

Alabama's Marine Resources Division is responsible for the management of marine fisheries resources through research and enforcement programs. It enlisted the assistance of the U.S. Space and Rocket Center/Geospatial Training and Application Center (GTAC) to design a ruggedized video surveillance solution that would be easily accessible by all of its law enforcement personnel in the field. The system also needed to be able to produce usable images in light, dark and foggy conditions.

GTAC and its partner, Crystal Data, created the system that enables Marine Resources Division officers to remotely view video and still images and control pan, tilt, zoom functions, using a smartphone or laptop computer, to investigate potential security risks.

This supply chain security effort has a geographic challenge. With more than 750 square miles in Mobile Bay and 11,000 square miles in the Gulf of Mexico patrolled by less than 20 officers, the video system helps secure strategic locations throughout the area.

"The coastal remote monitoring system is a force multiplier. It increases efficiency of officers on patrol and affords better situational awareness," says Major Chris Blankenship, acting director for the Alabama Department of Conservation and Natural Resources, Marine Resources Division. "We treat the cameras as just another sensor. The camera is a data collection device."

Using fiber and wireless connections, the cameras send video to Zaiobot appliances created by Crystal Data. The appliances convert video to the format preferred by the individual user, accommodating both low and high bandwidth connections. Users access video through customized consoles that allows them to securely view

live images or video, control cameras and select video for centralized archiving or saving to a remote desktop.

"The Zaiobot appliances allow the law enforcement officers to have access to video or still images from the cameras whether they are on a boat, in a car, or at the Marine Resources Division's central office," says Tim Erwin of Crystal Data.



Heavy duty cameras at terminals can communicate via wireless. The key to the Alabama installation is an appliance that allows myriad agencies assigned to protect the supply chain to see what they specifically need in their format.

All video is recorded and retained for extended periods. The system allows officers to quickly locate stored video using date and time parameters when forensic investigations are required. Archived video is watermarked with the department's logo and stamped with the location, date and time and can be used as evidence for legal proceedings when required.

"Many of the currently installed locations push the capability and functionality of the MIC cameras to the maximum, and we have been thrilled at the way they perform," said Chris Johnson, then with the U.S. Space & Rocket Center/Geospatial Training and Application Center, but now with A Visual Edge.

## Security Blanket: How to Wrap a Seaside Facility

Here is a stepped approach to facing this evolution, as provided by Jim Shepherd of Protection1, the nationwide integrator.

1. Establish purpose and end goal
  - a. Closed architecture system that serves one departmental function
  - b. Open architecture system that may serve other departments/purpose, functions outside of just security.
    - i. Business analytics
    - ii. Marketing
  - c. Integration with other systems
2. Communication and partnering with your IT department
3. Investment strategy
  - a. Full replacement
  - b. Hybrid
    - i. Keeping legacy or analog portions when it makes sense
    - ii. Adding IP systems when it makes sense
4. System design on:
  - a. Proprietary system versus non-proprietary
    - i. What are your options to change products, suppliers, integrators if there is failure?
  - b. Hardware
    - i. Future proof your investment for growth / expansion
    - ii. Server versus blackbox
    - iii. Types of IP cameras
      1. Compression
      2. Megapixel
      3. Brand, price, quality
      4. Form factor
      5. Ability to work with various head-end equipment, software
    - iv. Storage
      1. Local versus central
    - v. Network
      1. Bandwidth
      2. Access to system
      3. Usage
    - vi. Analytics
      1. Do you need them; will they really provide the ROI you seek?
      2. Which box to choose from with built in
      3. Which apps to choose from to add to an open architecture platform
    - vii. Video management systems
      1. Proprietary versus non-proprietary
      2. Enterprise system
5. Price structures
  - a. Capital expenditures
  - b. Software as a service
  - c. License fees
  - d. Maintenance fees
6. Suppliers
  - a. Venture cap type products
  - b. OEM products
  - c. Integrators – capabilities to install and service
  - d. Software support
  - e. Warranty, failure rates



Whole Foods uses a cloud-based access control system at a Colorado warehouse to improve security and operations.

warn him when doors are left ajar and regularly runs reports for time and attendance information to monitor employee lateness.

### LINKED WITH FORKLIFTS

In addition to improved access control, the warehouse ties its forklifts into the solution through an InfoLink system to monitor data for OSHA compliance. Drivers log into their forklifts with the same card they use for building access.

Hillfresh, a major Dutch fruit and vegetable distributor, has deployed IQinVision HD megapixel camera technology to improve security and operations at its Barendrecht facility in the Netherlands.

Hillfresh's 123,785 square foot facility handles 21,000 pallets on an annual basis in its global business of importing and exporting fruits and vegetables. The company decided to implement video surveillance to address a number of business challenges: to stop truck drivers sleeping on the job, more effectively manage trucks entering and exiting the docking stations, ensure staff are staying on the job and to prevent abuse of parking spaces.

Hillfresh has five employee administrators monitoring the grounds from the five available workstations. In addition to monitoring day-to-day logistical operations and suspicious activities, administrators are also responsible for responding to intercom prompts. When a user pushes a button on one of the five intercoms on the grounds, an image pops up on each administrator video screen and the security system requires a timely response to the intercom query.

When it comes to security video and the supply chain, there is an additional challenge when migrating from analog to IP digital. According to Jim Shepherd, national account manager at **Protection1**, the nationwide integrator, "Stay with or go to whom you trust" for sources of advice. "And don't paint yourself into a proprietary corner. No doubt, analog still has life but all systems evolve."

He adds that, when it comes to applications, supply chain security executives "must focus on the business purpose of putting up each camera." He advises to stop running coax; "some analog run on Cat 5." Infrastructure is a most important element.

### DIGITAL VIDEO MIGRATION

Migration to IP video is increasing, agrees Jeffrey Stout of Tri-Ed/Northern Video Distribution. For security executives protecting the supply chain and others, "It's a race to zero. We all live in a mobile world" and that includes security through the chain, he says.

Then there are the "almost mission impossible" incidents. For



The pharmaceutical industry has a unique and challenging assignment when it comes to protecting the supply chain. Attention is necessary from research to manufacture and then to distribution and warehousing and finally at the point of sale. Pictured is Jaime Yanez, a Ph.D. candidate in the College of Pharmacy at Washington State University, performing laboratory tests. Photo courtesy of Vetri-Science

example, in March 2010, thieves broke into a Connecticut warehouse of Eli Lilly & Co. and left with drugs valued at \$75 million. They cut a hole in the roof of the warehouse, rappelled in and disabled the security system.

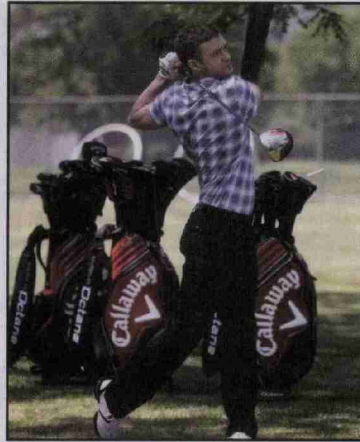
Everyone – enterprises, security, law enforcement and homeland security agencies – are involved in protecting the supply chain.

The assignment is not an easy one, however.

For example, U.S. Customs and Border Protection (CBP), working with the U.S. Consumer Product Safety Commission (CPSC), recently seized a shipment of Chinese imported children's toy jewelry for hazardous levels of lead. The shipment was approximately \$340,000. The importer or final retailer may not have known of the situation, and they may even established stringent specifications; not closely following the chain can cause trouble.

In this case, the shipment was examined by CBP officers at the port of Chicago, in coordination with the local CPSC compliance investigator. CBP seized the shipment when a sample tested by CPSC was found to contain an amount of lead that exceeded levels allowed by CPSC requirements for children's products.

The Consumer Product Safety Improvement Act of 2008 requires importers to test and certify that imports of children's products are in compliance with CPSC requirements. It is unlawful to import into the U.S. any children's product that con-



The Internet's impact on the chain. Customs officials report a growing business in fake golf products, with Callaway and Ping at the top. Pictured is Callaway Golf staff professional Justin Timberlake swinging his Diablo Octane driver. Photo for Callaway Golf Company by Jason DeCrow

rains lead with more than 90 parts per million of lead paint or more than 300 parts per million of total lead content.

**A GOLF CONNECTION**

Vigilance of the chain also impacts older people's toys such as golf products and, in some incidents, points to trading through the Internet as an encouragement of illegal activity.

For instance, *Security* magazine has been told that CBP is now seizing an increasing number of counterfeit golf products ordered by consumers over the Internet, many of them labeled Callaway. Seizures of counterfeit golf goods have increased by 33 percent from fiscal years 2009 to 2010 and 37 percent in 2009 compared to 2008.

"CBP is sounding the alarm on a growing trend in the purchase of fake golf equipment," says Commissioner Alan Bersin. Today, the typical golf seizure consists of a set of clubs, a bag, head covers and maybe a cap. The items usually arrive from China via mail or courier addressed to an individual in the U.S. So far this year, CBP has made 265 counterfeit golf seizures with a total domestic value of \$192,000, and an estimated manufacturer's suggested retail price of \$589,000.

Traditionally, counterfeit golf products enter the U.S. inside seaborne containers with other goods. But, thanks to the rising popularity of Internet shopping, CBP has increasingly seen the ability of counterfeiters to sell directly. Consumers looking for less expensive products are going online, order-



Sometimes protecting the supply chain means getting down to street level. Fashion industry security professionals, working with law enforcement, for example, have microscoped on the Canal Street area of New York City to try to halt the sale of fake purses.

ing directly from Chinese suppliers and shipping the fake goods home.

In addition to skirting the normal supply chain of shipping via cargo containers, the more traditional method of seaborne cargo containers has its own security challenges.

About seven million cargo containers arrive at U.S. ports every year. These containers represent an important component of the economy. The port of Boston, which became an international cargo port in 1630 and is the oldest continually active major port in the Western Hemisphere, handles 1.3 million tons of general cargo and 12.8 million tons of bulk fuel cargos every year. Clearly, such global commerce is critical to a nation's economic.

**CONTAINER SECURITY**

Cargo containers represent tempting targets for terrorists.

One successful anti-terror program is Customs-Trade Partnership Against Terrorism (C-TPAT). Under it, shippers commit to improving the security of their cargo shipments, and in return, they receive a range of benefits from government officials such as ease of inspection.

The overall container security initiative (CSI) consists of four elements:

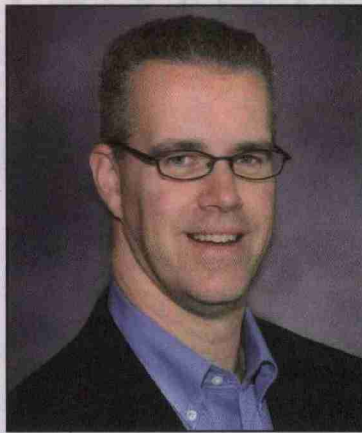
- Intelligence and automated information to identify and target containers that pose a risk for terrorism.
- Pre-screening those containers that pose a risk at the port of departure before they arrive at U.S. ports.
- Detection technology to quickly pre-screen containers that pose a risk.
- And smarter, tamper-evident containers. While shippers, enterprises and home-

land security continue to try to figure out the best way to protect the supply chain when it comes to cargo containers, a study by Reportlinker.com emphasizes the technology and process strategies of pharmaceutical companies when it comes to the supply chain. There are significant anti-counterfeiting activities from companies such as Pfizer, Johnson & Johnson, GlaxoSmithKline, Sanofi-Aventis, Novartis and AstraZeneca.

This includes radio frequency identification (RFID), pharmaceutical taggant, hologram/optical variable device or OVD foils, security ink and watermark technologies, to name a few.

RFID seems, according to some experts, to be gaining ground when it comes to supply chain security, after some skepticism of the solution.

For example, Jeremy Friedler of the Maxiom Group, contends that "amazing things can happen with revolutionary technologies when everyone takes a deep breath, relaxes and remains patient. RFID could be one of the most advanced technologies available to provide increased visibility into counterfeit products entering the supply



**Peter McLaughlin of Foley & Lardner urges enterprise security leaders to protect data and documents along the supply chain.**

chain while simultaneously protecting the integrity of therapeutics en route to the patient."

While, over the years, more product manufacturers have seen value in source tagging to combat shoplifting, information-rich RFID is catching on with pharmaceutical companies, in cargo containers, on

pallets, and with other applications, according to Geva Barash of Team AVS. "There are so many levels in the pharma supply chain," he points out. But RFID can provide a valuable link throughout the chain. "You can follow a bottle to pallet to distribution and then to a store shelf. You can scan the store rack to see if the real product delivered matches the unreal."

#### **INFORMATION SECURITY WORRIES**

While most of the supply chain security talk is about parts, produce, software and pills, the newest worry is about data and documents, which move along the chain or go with shipments.

According to Peter McLaughlin at Foley & Lardner, a world-recognized law firm, enterprises and their security executives must be aware of vulnerabilities and threat specific to cybersecurity and infrastructure. "You just cannot protect from everything," he says. There are significant challenges such as privacy laws that vary from nation to nation and that great leap of faith into the cloud. You need to track and authenticate data and documents as they move along the chain, he points out. **SECURITY**