SUPPLY CHAIN SECURITY

- National Strategy
- Security Planning
- Threat Survey
Let Dehnco Help You Evaluate and Integrate Workstations, Supply Storage and Equipment Needs with Your Automation, Technology and Material Handling Systems . . . AT A PRICE YOU CAN AFFORD

Dehnco offers a simple 4 step evaluation process that:
- Promotes Ergonomics
- Creates Efficiency
- Increases Productivity

**STEP : 1**
Evaluating Flow
Defined as the movement of materials/products into and out of the work area.

**STEP : 2**
Identifying the Process
Detailing the Step-by-Step Sequence of tasks required to complete the specific work being done in the area.

**STEP : 3**
Integrating the Supplies and Equipment Required to Complete a Task into the work area.

**STEP : 4**
Integrate the Work Area Design with the Process to Maximize the Efficiency of the Operation.

Contact Us:
Call: 847-382-1579
www.dehnco.com

Let Us HELP You Define and Resolve These Issues
- SPACE
- STORAGE
- HANDLING/DESIGN
- ERGONOMICS
- WORKFLOW
- SPACE

Easier to Assemble
New Color Pallet

Dehnco™
Your Workstation Solution Partner

300 Lageschulte St
P.O. Box 866
Barrington, IL 60010
Ph: 847-382-1579  Fax: 847-382-1615
Regionally Based; Globally Capable.

Sonwil, your strategic partner providing solutions to protect your economic future.

Take Advantage of the Power of Four.
Sonwil offers four highly focused, independently managed operations collaborating with you to tap your economic strengths locally, regionally and globally.

Logistics to power your distribution
- Warehousing and Distribution; Cold and Ambient, Food Grade, Rail Served, FTZ Certified supported by a dynamic Technology Driven WMS
- Value Added Services; Cross Dock, Pick and Pack, Re-Casing / Re-Packing and Display Builds
- Returns Processing and Refurbishment: Sorting, Inspecting, Re-Manufacturing, Parts Distribution all driven by Scalable Technology Solutions

Technology to increase your competitive edge
- RF Inventory Management Technology
- Real Time Tracking, Traceability and Transparency for optimal inventory management and quality control
- Resident IT Resources to address your current and changing Supply Chain needs

Transportation services to move your goods
- Asset Based Shuttle Services; heavy permitted equipment to reduce your transportation costs and your carbon footprint
- Refrigerated and Ambient Load capabilities
- Local, Regional and International Brokerage Services

Commercial Space to grow your business
- Clean Modern “flex” space – build to suit
- Superior amenities – from free / well lit on - site parking to close proximity main thoroughfares
- Immediate access to; local, regional, national and international transportation routes – NYS Thruway, Buffalo-Niagara International Airport and US /Canada crossings

Move your fixed expenses to variable by selecting just the services you need when you need them, reducing your costs and significantly improving your bottom line.

We’re in the center of it all.

A Responsive Strategic Partner, Working with You.
Contact Dave Harper: 716.206.1842 • dharper@sonwil.com
www.sonwil.com

A Total Solution for getting it from here to there

TRACKING
The most sophisticated technology at your fingertips to get precise tracking information of your goods.

TRACEABILITY
We use the latest software providing a global, multi-carrier shipping solution. Scalable from a single location to a global enterprise solution, it’s accessible online for tracing and confirming delivery.

TRANSPARENCY
Get the peace of mind of being able to virtually see the shipping process from start to finish. No surprises.
3PL Americas™
THE MAGAZINE OF IWLA IN NORTH AMERICA • SUMMER 2013

6 3PL Security: No News Is Good News
   By Joel D. Anderson

7 Failing to Prepare is Preparing to Fail
   By Paul Verst

9 Kenco: Guiding Principles and Company Traditions Create a Robust and Engaging Culture
   By Kim Biggar

12 Deloitte Survey: Executives Face Growing Threats to Their Supply Chains

15 An Emerging Security Threat — Fraudulent Carriers
   By Bill Anderson

19 National Strategy for Global Supply Chain Security: Implementation Update

21 Secure Supply Chain Management in a Changing World of Threats
   By Kevin Nevrous

24 Security Planning for High-Value-Product Distribution
   By Kim Biggar

26 Simplifying Tools for Trade
   By Kathleen Franklin

29 CBP’s New Air Cargo Advance Screening Program Brings Together Government and Industry to Enhance Security
   By Jay Mayfield

32 IWLA Events Calendar

33 Securing Your Data in the Cloud — How Amazon Web Services Can Benefit You
   By Jared Mendenhall

36 Harmonization is the Aim, Secure Trade is the Game
   By Terry Nusyna

38 Following the Supply Chain to Warehouse Security
   By Sue Poremba

40 Measures to Reduce Employee Theft from the Warehouse
   From Cisco-Eagle

42 Advertiser Index

43 The Magic of Mentoring
   By Chip Scholz

44 Future Issues of 3PL Americas

45 Entry Management: Maintaining Safety at Your Sites
   By Jay Hauhn
SECURITY IN THE SUPPLY CHAIN is like safety inside the walls of the warehouse: Success is measured by the events that do not occur. While it may be a logical challenge to prove a negative, in the practice of preventing losses and securing the content and delivery of product, the logic is a rigorously applied behavior. This issue of 3PL Americas explores the best practices and procedures available today and makes the case that a secure and safe supply chain is work done well.

You will read about what the best companies and best practitioners have achieved to secure the movement of freight and people in their care. Practices start with behavior and processes, and advance into auditing, evaluation and continuous improvement. It is a devotion to task every day that secures our supply chain. And a secure supply chain enables the benefits of trade and commerce to flow through borders and checkpoints, to shoppers seeking to increase their standard of living.

This issue focuses on many of the issues that affect our operations. It offers some solutions and highlights the expertise of the people, companies and agencies that impact our daily operations.

U.S. Customs and Border Protection has given us two viewpoints on the balance between the need for security and the demand for efficient import and export of goods.

Included are articles on the importance of securing your goods and vehicles against theft – two very common and expensive areas of cost to third-party logistics providers.

And, of course, what could be more important than protecting our data? It’s the lifeblood of what we do. We believe it’s secure but what if…? We are presenting an article that will dispel some misconceptions and offer some solutions and concepts to consider.

As always, 3PL Americas is your magazine. It’s our hope to engage you in emerging issues and practices that you can apply to your company today. We encourage you to enter into the discussion by sending us your recommendations and thoughts. Our goal is the same as yours: to advance the excellence of 3PLs in the Americas.

Joel D. Anderson
President & CEO
International Warehouse Logistics Association

It is a devotion to task every day that secures our supply chain.
Failing to Prepare is Preparing to Fail

WE ALL FACE RISKS in our daily lives; yet, the risks we face in the warehouse-based third-party logistics industry come with consequence and loss for us, our customers and the broader supply chain.

It is important to mitigate this risk as much as we can. At Verst Logistics, we implement safety programs and training sessions, and utilize standardized operation manuals to teach employees the proper methods to accomplish job tasks safely and efficiently. I’ve realized that, despite all of these efforts, there is a constant need to update procedures to address unforeseen hazards that arise. It is important to refresh these concepts to keep them top of mind.

One way to do this is to send those responsible for safety in your warehouses to the IWLA Safety & Risk Conference. For 2013, this course will be on September 12 and 13 in Fort Worth, Texas.

The program agenda spans the entire safety and risk-prevention spectrum:
- compliance and regulatory updates from OSHA;
- transportation updates, including top driving and vehicle violations;
- crisis-management strategies to mitigate risk;
- legalities of physical-abilities testing;
- global harmonization classifications of chemicals and appropriate labeling; and
- human resource best practices.

IWLA events like this are great places to share ideas with industry peers. Returning from an IWLA educational event, I always feel changed – I am wiser, more capable to handle challenges and, most of all, more conscious of implementing positive changes at my company.

When Verst Logistics created Zenith Logistics to pick, assemble and deliver grocery products for a large grocery retailer, our company encountered an entirely new set of risks. Our involvement in IWLA allows us to better understand and mitigate any security and safety concerns arising from new lines of business.

Another protective measure that continues to serve Verst Logistics well is the IWLA Insurance Captive (IWLA-IC). While not every IWLA member company is right for the captive (there are thresholds of premium and safety records that are barometers), our involvement brings us great safety- and security-related education. And the IWLA-IC also rewards members when safety programs are working and risks have been reduced. This reward is a form of a rebate from unused premiums.

Even if the captive is not right for your organization, your IWLA membership grants you access to other offerings, including the Warehouse Light insurance program. Call IWLA, at (847) 813-4699, for more information.

The captive is one of many benefits IWLA provides members – connecting companies with common goals of business growth and development in third-party warehouse-based logistics in a safe and secure supply chain.
In 2010, when Kenco was 60 years old, co-founder Jim Kennedy, Jr. issued what he called the “Principles of Success,” 10 standards that had been the essence of the company’s culture since it was formed. Since then, the company has maintained a keen focus on its “guiding principles,” a short and simple, easy-to-remember adaptation of the original list.

The guiding principles for Kenco employees at all levels are:

• Be remarkable and create uncommon value;
• Demonstrate courage, commitment and compassion; and
• Integrity above profitability.

These principles are now highly visible in Kenco facilities, on posters and flyers, and provided to employees on wallet-sized cards. David Caines, president of Kenco Logistic Services – one of five companies in the Kenco family, which also comprises Kenco Transportation, Kenco Toyota-Lift, Kenco Management Services and JDK Real Estate – talks about the guiding principles whenever he meets with employees. He spends about 50 percent of his time at team meetings sharing company stories that illustrate the principles. Caines says the principles, “state and describe how people should act, what
Kenco’s first warehouse.

GUIDING PRINCIPLES

Kenco’s mission is to be the preferred supply chain partner in North America.

The following principles reflect our values, define our culture and guide our actions:

**Integrity Above Profitability**
- Lead with humility and respect.
- Earn trust through authenticity and accountability.
- Cultivate mutually beneficial partnerships with customers, associates and suppliers.
- Practice servant leadership and demand the highest standards.

**Demonstrate Courage, Commitment & Compassion**
- Openly communicate and empower every individual.
- Think concretely and act with urgency.
- Encourage camaraderie to strengthen our community.
- Embrace our social, environmental and economic responsibilities.

**Be Remarkable & Create Uncommon Value**
- Deliver results through discipline and stewardship.
- Facilitate change and foster innovation.
- Develop passionate customer advocates through operational excellence.
- Focus on our core and win every day.

they should be modeling in their behavior.” They’re the core of the company’s service-quality culture.

**Company History and Overview**

In 1950, Jim Kennedy, Jr. and Sam Smartt, Sr. founded Kenco as a warehousing enterprise in an old foundry building in south Chattanooga, Tennessee. At the outset, the two brothers-in-law were the only employees of the company.

One favorite story shared with employees to illustrate the principle of commitment dates from the early years, when just Kennedy and Smartt worked for the company. It was their practice to take turns making sales and working in the warehouse, and to wear clothes appropriate to their roles for the day. One day, one would wear a suit, the other jeans; the next day, they’d switch roles and dress accordingly. On a day when Kennedy, Jr. was wearing jeans to work in the warehouse, one of his customers, a railroad, called to set up a lunch for that day with a VP who was in town. When he got off the phone, Kennedy asked Smartt to switch clothes with him. Smartt removed his suit and put on the jeans; Kennedy was able to get to his meeting, properly attired.

Another story from the company’s past is used to demonstrate the need for courage. In the late 1960s, when Kenco was still a single-city provider, an existing client mentioned to Kennedy over dinner that it would be expanding to St. Louis and Dallas. Kennedy immediately asked for the business in those locations, without a plan to deliver it, confident that his team would make it work. The client, Electrolux, has been doing business with Kenco for 43 years now.

Kenco has grown considerably; it now has about 4,700 employees, more than 100 facilities and 30 million square feet of warehouse space in 25 states and Canada that it operates, leases or manages. It is, says Caines, the largest privately held 3PL provider in North America, and...
is focused on the North American market, rather than globally. Kenco is also now the largest woman-owned logistics company in North America, following Jane Kennedy Green’s acquisition of the controlling interest from her father, Jim Kennedy, Jr., in 2011. Since 2002, it has grown at a compound annual rate of 10.8 percent.

“Our guiding principles are rooted in what most people already know is important,” says Caines. “It’s these common-sense values that empower our company to deliver uncommon value.”

Building and Communicating Company Culture

“From day one,” wrote Kennedy in a letter to employees in 2010, “at the suggestion of my father, we strove to establish a culture for this new company that would ensure success in the ensuing years.” Decades later, culture remains at the forefront of management concerns.

Sometimes when he’s talking with employees about the guiding principles, Caines reads part of the poem ‘Tis the Set of the Sail, by Ella Wheeler Wilcox:

One ship sails East,
And another West,
By the self-same winds that blow,
‘Tis the set of the sails
And not the gales,
That tells the way we go.

The company, he says, faces all kinds of winds – the economy, client issues and so on – but they are not what determine where the company heads. Rather, it is Kenco’s principles that guide its decisions and path.

This year, Caines is doing a road show, visiting all of the company’s facilities to present to employees. In addition to company updates, he’s sharing stories, emphasizing the importance of the guiding principles. Last year, at a managers’ meeting that brought together 220 employees for several days, team-building and training exercises were infused with values messaging. In 2011, Caines communicated the same messaging through a series of VP roundtables. Everyone is hearing the stories and, through them, developing a common understanding of the company’s culture, along, believes Caines, with a sense of pride in and connection with the organization.

Because the guiding principles and the program of communicating about them are quite new, the company doesn’t yet have data to show their impact. Caines, however, feels that employee retention is being favorably affected by the focus on values. It’s been said that people leave bosses and co-workers, not jobs. A workplace, then, in which fairness, integrity, respect, empowerment, camaraderie and empathy – some of the 10 principles of success identified by Kennedy – are actively and regularly promoted is likely to remain attractive to employees.

Recently, a client of 22 years sent an email to Kenco, thanking the company and specific employees for their good work. Living up to the guiding principle that calls upon them to “be remarkable,” employees had provided service noteworthy even to a long-standing customer. To celebrate this success, management shared the email throughout the company, creating an opportunity to further cultivate its culture.

Perhaps in the future, this achievement will be shared with employees as a company story. As Caines notes, the stories have become Kenco parables, shared to illustrate key value messages. They certainly make for a unique culture, and contribute to engaging employees and inspiring them in their work.

Left to right: Monique Osban, EIP Coordinator, Tom Martin, Returns CSR and Josh Nicotra, Operations Manager, reviewing their site’s weekly key performance indicators at a Kenco Logistic Services’ facility in Mt. Vernon, Indiana.
According to a new survey from Deloitte, global executives are increasingly concerned about the growing risks to their supply chains and costly negative impacts such as margin erosion and inability to keep up with demand. As they operate in this environment of escalating risk, an alarming 45 percent of surveyed executives say their supply chain risk-management programs are only somewhat effective or not effective at all.

“Supply chains are increasingly complex and their interlinked, global nature makes them vulnerable to a range of risks,” said Kelly Marchese, principal, Deloitte Consulting LLP, who specializes in manufacturing operations and supply chain strategy. “This increased complexity, coupled with a greater frequency of disruptive events, such as geopolitical events and natural disasters, presents a precarious situation for companies without solid risk-management programs in place.”

According to the global survey of 600 executives, supply chain disruptions are not only more frequent, they are also having a larger negative impact. Among the findings:

- More than half (53 percent) of executives said that supply chain disruptions have become more costly over the last three years.
- Executives from the technology, industrial-products and diversified-manufacturing sectors were most likely to report that supply chain disruptions have become more costly.
- Nearly half (48 percent) of executives said the frequency of risk events that had negative outcomes – such as sudden demand change or margin erosion – has increased over the last three years.

Margin erosion is considered the most costly outcome of supply chain disruptions, with 53 percent citing it as one of their top two issues. Consumer products, diversified-manufacturing and energy companies were especially likely to report margin erosion as one of their most costly issues.

Forty percent of respondents cited “sudden demand change” as one of their two most costly problems – a reflection of ongoing challenges involved with growing customer expectations, short product cycles and emerging competitive challenges. Executives at retail and technology companies, which operate in a world where markets change rapidly, were most likely to identify demand change as being costly.

Executives surveyed recognize the strategic importance of supply chain risk, with 71 percent responding that supply chain risk is an important factor in their strategic decision-making. Nearly two-thirds (64 percent) claim to have in place a risk-management program specific to the supply chain.

However, only 55 percent of surveyed executives think their risk-management programs are extremely or very effective. The top two challenges according to executives surveyed were “lack of acceptable cross-functional collaboration” (32 percent), followed by “cost of implementing risk-man-

1. In this document, “Deloitte” means Deloitte Consulting LLP, a subsidiary of Deloitte LLP.
There are also organizational factors making effective supply chain risk more difficult: Three-quarters (75 percent) of executives said their supply chain risk-management model is organized around silos, which can lead to a lack of supply chain visibility and collaboration, and make it difficult to assess and manage risk on a holistic basis.

Although surveyed executives report using a wide range of tools to manage risk, only 36 percent use predictive modeling and less than one-third (29 percent) use risk sensing data, worst case scenario modeling, or business simulation — all tools that help drive more proactive management of supply chain risk.

“Many companies have some form of a supply chain risk-management program, but unfortunately they do not always get the results they need from these programs,” said Marchese. “To be effective, companies should take a holistic and integrated approach to managing supply chain risk and go beyond traditional approaches. Because of the complex nature of today’s supply chains, disruptions will inevitably occur. True resilience means building in the ability to recover efficiently and decrease the impact of those events.”

According to Deloitte — which was recently named a Vanguard Leader, based on capabilities, by Kennedy in Supply Chain Risk Management Consulting² — the four important attributes that are critical to supply chain resilience are:

- **Visibility:** The ability to monitor supply chain events and patterns as they happen, which enables companies to proactively — and even preemptively — address problems.
- **Flexibility:** Being able to adapt to problems efficiently, without significantly increasing operational costs, and make timely adjustments that limit the impact of disruptions.
- **Collaboration:** Having trust-based relationships that allow companies to work closely with supply chain partners to identify risk and avoid disruptions.
- **Control:** Having policies, monitoring capabilities and control mechanisms that help confirm that procedures and processes are actually followed.

### About the Survey

Deloitte conducted a survey of 600 executives from manufacturing and retail companies with a minimum of $100 million in annual revenues to assess their attitudes and challenges in managing supply chain risk. The survey was conducted via both telephone and online interviews from July to October 2012. Thirty-six percent of the companies are headquartered in North America, 28 percent in Europe, 11 percent in China, 11 percent in Japan and 7 percent in Brazil.

---


---

Continued on page 32
Solutions that lead to better lighting.

At SYLVANIA Lighting Services our goal is to help you maximize your company’s energy savings. We’ll start with a detailed assessment of your current energy usage and, if appropriate, follow up with a customized design for more efficient lighting. As the industry leader in turnkey lighting solutions, SYLVANIA Lighting Services can help you be sure your lights are on when you need them and off when you don’t. And with the installation of dimming lighting controls, you can even set your lighting somewhere in between. To order an accurate energy assessment or to discuss a lighting solution custom-designed for you, call 1-800-323-0572 or visit www.sylvania.com/sls.
The trucking industry has long been the target of both opportunistic and organized crime. Dealing with hijackings while the vehicle is on the road and robberies at delivery points, carriers and shippers have spent countless resources to prevent cargo theft. However, the latest trend of exploiting the Internet and common identity-theft techniques to pose as legitimate carriers can’t be prevented with seals, locks and tracking devices.

As with every other facet of business, companies with freight to be moved are looking for more cost-effective transportation solutions. This often involves the use of Internet load boards, communicating by e-mail and mobile phones, and brokering loads to companies and individuals in a somewhat-anonymous transaction. Organized criminal organizations are well-versed in the methods to exploit these systems to pose as legitimate carriers and obtain freight: a very low-risk, high-profit opportunity.

One technique used involves posing as a driver from a legitimate carrier that has been assigned a load. In this scenario, the imposter obtains load information, and arrives early at the pick-up location in a truck that looks like the assigned carrier’s or may actually be a truck stolen from the assigned carrier. The theft is usually discovered when the legitimate driver shows up for a load that has already been released. The downside for the criminals in this scenario is (1) the risk of discovery if they are using a stolen tractor, and (2) their lead time is limited to the length of time between the theft and when the legitimate driver arrives.

A more-recent technique being used by criminals steers clear of these problems. The technique involves creating a business-partner relationship with a shipper or broker using fraudulent information. For example:

A theft is usually discovered when the legitimate driver shows up for a load that has already been released.
A high-value load is identified from an Internet load board. Even though the load information may seem generic, the load may be identified as “high-value” based on a known pick-up location, insurance requirements or destination.

The bad guys will contact the shipper with interest in the load. Pulling information from Internet sources, they’ll establish themselves as a carrier by replicating, and slightly altering, a legitimate-carrier’s information. Doing this, they’ll probably target a small carrier from another part of the country that is unlikely to already be in the shipper’s system. They will submit registration documents with slightly altered phone numbers or addresses and what appear to be legitimate insurance documents.

If they are awarded the load, they will provide a driver’s name and mobile phone number.

The transaction seems normal until the load never reaches its destination, and the carrier and driver disappear. The mobile phone will work for a few days to provide updates until it eventually goes dark. This often allows anywhere from a few days to a week of lead time before the theft is detected.

How Can Shippers Prevent or Mitigate This Risk?

There is no single technology or procedure to combat this risk. A layered approach, depending on the operation and type of goods being shipped, is always best. This involves vetting carriers, establishing driver-verification processes, protecting proprietary shipping information, and training employees to recognize this type of fraud.

Vetting Carriers

It’s important to verify the legitimacy of every new carrier a shipper works with. This includes independently validating information submitted by new carriers. Keep in mind that the contact information submitted by a new carrier could be just as fake as the registration numbers, addresses and so on. There are a variety of services that can help shippers validate carriers, but there are also a number of steps shippers can take on their own to reduce the risk of working with fraudulent carriers.

The information submitted by a carrier should be compared with information obtained through the use of independent sources such as Yellow Pages, Internet searches and DOT profiles. If the information submitted by the carrier is slightly different from what you find through a separate source, this should raise a flag and warrant additional investigation. Once you’ve established the legitimate contact at the carrier, give him or her a call. Confirm that the company is asking to be set up as a carrier and validate its information. Contact the carrier’s insurance provider separately to verify its policy, dates, limits and contact information.

Finally, when it comes to vetting carriers, if you release loads to brokers, be sure they have similar processes for vetting their carriers. Also, be aware that it is not uncommon for carriers to broker or assign loads to other carriers without the shipper’s knowledge. It’s up to the shipper to decide whether this type of activity will be allowed and how best to insulate themselves from fraudulent activities through contract language.

Driver Verification

When high-value goods, food or hazardous materials are involved, it’s important to verify the identities of drivers when they pick up a load. When possible, request that the assigned carrier provide pre-arrival information such as the driver’s name, vehicle number and arrival time. Be suspicious of a driver that arrives hours ahead of his appointment, as this may be an imposter. Dispatchers that are releasing loads to drivers should contact the carrier if the information they were provided does not match the driver or carrier that arrives to pick up a load.

Shippers can also take steps to ensure that the driver’s license is legitimate. A reference book with verifying information for government-issued IDs can help spot false credentials. An ultra-violet flashlight can verify hidden watermarks that are embedded on most government-issued IDs.

Other steps that can help deter criminal activity include capturing digital images of drivers using Verification of driver information.
CCTV or taking digital still photos. Dispatchers can even use inkless fingerprint pads, commonly used in banks, to have the drivers leave their thumbprint on shipping documents retained by the shipper. While these steps may not directly prevent a fraudulent pick up, they can greatly aid in the investigation and may indirectly deter fraudulent activity.

**Protecting Shipping Information**

Most of us have heard about the dangers of releasing personal information such as social security numbers or account numbers. And while we have heeded these lessons in our personal lives, we don’t always apply the same discipline when it comes to protecting shipment information. In today’s data-intensive world, it’s more critical than ever to protect any information that could be used to identify or target shipments.

Sometimes it’s as innocent as an employee giving shipping information over the phone to what sounds like a legitimate carrier inquiry. Or it could be as simple as sending advance shipment information to destination sites that gets printed and posted on the receiving dock. Shippers need to balance the need for sharing this information with the threat that it could be used to target their loads.

It’s also important to train employees about how to handle calls from carriers or individuals looking for information over the phone. Transmitting shipment data via EDI, versus e-mail or telephone, is the most-secure way to ensure information is getting to a credible partner. Employees that have access to systems containing shipping records should have individual assigned usernames and passwords that must be reset on an appropriate schedule. Personnel who administer these systems should routinely audit access records for unused usernames, and deactivate them.

**Employee Training**

Preventing the release of shipments to fraudulent carriers is about having the right systems, processes and procedures. But this relies on having well-trained employees to execute these procedures. There have been several alerts generated recently from various sources identifying suspect carriers. However, it is not enough to simply distribute these alerts, as carrier names can be changed with a few keystrokes. Employees must be trained on the methods used by fraudulent carriers so that they can recognize future attempts.

Employees who are responsible for setting up new carriers must be aware of the threat posed by fraudulent carriers and the proper steps that must be taken to verify carrier information. Employees who have access to shipment information must be trained on the need to protect this information, and recognize attempts to gather sensitive information. Dispatchers who are releasing loads must be trained on how to validate driver credentials and the importance of verifying driver and carrier identities. And any employee who has access to electronic systems must be trained on the importance of not sharing usernames and passwords.

While the threat posed by driver imposters and fraudulent carriers may not be new, today’s reliance on systems and the need to drive out cost creates an environment where these conditions can be exploited by the creative criminal. Combining the right processes and technologies with a highly trained and diligent workforce is the most effective way to mitigate this security risk.

Bill Anderson is Group Director, International Safety, Health & Security for Ryder, a provider of transportation and logistics solutions. He is based in Miami, Florida.
President & Chief Executive Officer

The Organization
Since 1891, the International Warehouse Logistics Association (IWLA) has been promoting the growth of the warehouse logistics outsourcing industry. IWLA provides its 400 member companies with resources, information, education and professional programs designed to advance their businesses and provide greater value to their customers. Located in Des Plaines, Illinois, with an advocacy office in Washington D.C., IWLA is led by a 22-member Board of Directors. With a full-time staff of 8, plus consultants and contractors, and an annual budget of $2.8M, IWLA is the unified voice of the value-added warehouse logistics industry. For more information, visit www.iwla.com.

Requirements and Qualifications
The President and Chief Executive Officer directs and administers all aspects of the Association’s operations. This individual is responsible for the Association subsidiaries, including IWLA Services, IWLA Education and Research Foundation, the IWLA PAC, as well as councils, chapters and affiliated organizations. This individual also serves as President of the IWLA Insurance Company and administrator of the IWLA employee retirement and deferred compensation programs.

Qualifications include: Bachelor’s degree in business, political science or economics; advanced degree preferred; a minimum of ten years’ senior management experience, including significant staff, budget, operations and marketing; strong oral and written communication skills, including outstanding public speaking capabilities; demonstrated experience and track record in advocacy and government affairs; experience with a multi-faceted organization involving volunteer leadership, professional staff, large meetings, enduring educational materials, and trade journal experience strongly preferred; experience within the industry or a related logistics or supply chain field preferred; understands and is comfortable with the use and integration of technology; ability to travel up to 40%.

The successful President and Chief Executive Officer must be a strategic and collaborative leader with high energy and a desire to innovate and establish operations on new projects in close partnership with our member driven association and volunteer leadership. The candidate must present a positive image of the organization and our industry, and be the “head cheerleader” for our industry.

The candidate must encourage a culture of respect and communicate openly with IWLA officers and staff. He or she must have outstanding written and oral communication skills, problem solving and interpersonal skills, as well as an ability to listen and delegate effectively. The candidate must have a demonstrated knowledge of the political and legislative process and be able to articulate the IWLA’s value proposition (education, advocacy, networking).

Search Process
This search is being conducted by Tuft & Associates. Please submit cover letter and résumé no later than August 15th in confidence to:
Tuft & Associates, Attention Jill Christie
Email: cmarg@tuftassoc.com
www.tuftassoc.com

President & Chief Executive Officer
National Strategy for Global Supply Chain Security: Implementation Update

Federal government’s recent assessment report on security implementation

The National Strategy for Global Supply Chain Security, released in January 2012, establishes the United States Government’s policy to strengthen the global supply chain to protect the welfare and interests of the American people and to enhance our Nation’s economic prosperity. The Strategy complements and supports existing policies, and emphasizes:

- All modes of transport (air, land, and sea) as well as critical intermodal hubs to provide “end-to-end” coverage of the supply chain system;
- An all-hazards approach, recognizing that man-made as well as natural threats could trigger disruptions to the system; and
- The need for the global supply chain system to be both more secure and able to recover quickly should an incident occur.

The primary focus during this first year of implementation has been to build additional models and assessments for how the global supply chain system operates as an interconnected network. Much of this work built upon existing analysis of the systems’ constituent parts and, as a result, the United States Government now has a greater ability to describe, predict, and mitigate the disruptions that could affect the different types of supply chains that feed our domestic critical infrastructures and contribute to our national welfare and economic prosperity. This is a necessary first step toward the ultimate goal of developing and institutionalizing global measures to enhance the security, efficiency, and resilience of this vital global system.

As required by the Strategy, this report summarizes progress made by Federal departments and agencies to strengthen the global supply chain system during the first year of implementation.1 It also highlights opportunities for continued work and makes recommendations for future implementation activities.

■ 2012 Accomplishments

Over the last year, the United States Government made good progress in advancing the priority actions identified in the Strategy’s Implementation Guidance. These priority actions include:

- Refining our understanding of supply chain threats and risks by completing insightful new assessments of the system as an interconnected network and updating analysis of the specific radiological or nuclear terrorist threat that reaffirmed current policies and programs.
- Advancing technology by establishing United States Government pri-

1. The Strategy for Global Supply Chain Security notes that “Departments and agencies will submit to the President, through the Assistant to the President for Homeland Security and Counterterrorism, a consolidated report on implementation status within 1 year of the release of the Strategy. The report will detail progress made on each of the priority action areas identified [in the Strategy]. It will also include additional recommendations for future action developed during the outreach process.”
orities in the supply chain space (such as tracking and intrusion detection capabilities for containers in transit) and developing a process to better coordinate research and development projects to advance those priorities; and supporting international capabilities to identify the illicit transport of radiological and nuclear materials in the supply chain by increasing the number of detection systems provided to foreign government partners.

- Building resilient critical infrastructures by creating new incentives, such as Resilience STAR, to encourage industry stakeholders to build resilience into their supply chains, which then strengthens the system overall; mapping the dependencies among the supply chains of various critical infrastructure sectors (such as energy, cyber, and transportation); and creating common resilience metrics and standards for worldwide use and implementation.

- Promoting the development and utilization of supply chain standards through active engagement with relevant stakeholders to advance technical standards for radiation and nuclear detection technologies as well as global standards or best practices guiding the submission and analysis of postal and air cargo information.

- Improving commercial information analysis and sharing capabilities through innovative pilots with foreign governments to assess data and inspect high-risk cargo prior to arrival at the U.S. border.

- Streamlining and harmonizing government processes and policies to facilitate trade by completing milestone mutual recognition arrangements with the European Union for air, land, and sea cargo security programs; establishing four virtual Centers of Excellence and Expertise to improve the uniformity of trade enforcement processes among all our Nation’s ports of entry; and creating a new Interagency Trade Enforcement Center to identify and address unfair trade practices.

- Establishing a Cross Sector Supply Chain Working Group, composed of private-sector representatives from domestic critical infrastructure sectors, and supporting their development of a “Global Supply Chain Findings and Recommendations Report” that will inform future implementation efforts.

### 2013 Implementation Activities

Throughout 2012, Federal departments and agencies engaged with industry, international organizations, and other government stakeholders to identify areas for focus in 2013. These 2013 implementation activities include:

- Continuing to refine the United States Government’s understanding of threats and risks to the global supply chain system as an interconnected network by exchanging views on threats and risk with key domestic and international stakeholders, and advancing long-term efforts to characterize system-wide risk and develop common risk indicators, metrics, and mitigation measures.

- Further aligning technology needs and investments among Federal departments and agencies by developing a set of United States Government-wide cargo and supply chain research and development (R&D) priorities; and identifying opportunities to test, in operational environments, specific technologies that have the potential to improve the security and integrity of cargo.

- Supporting international capabilities to detect and address the illicit global transport of radiological and nuclear materials and devices and other prohibited items and contraband.

- Promoting supply chain and critical infrastructure resilience by designating new Resilience STAR projects in the transportation sector; conducting exercises to identify and address critical infrastructure dependencies; and utilizing lessons learned from Hurricane Sandy to inform new policies and programs that will enhance our Nation’s preparedness.

- Engaging Congress to identify opportunities to enhance alignment between legislative requirements and the goals and approach established by the Strategy.

- Advancing selected global supply chain standards by strengthening intragovernmental coordination to better convey a unified, “whole-of-government” position during engagements with standards development or other intergovernmental organizations and bilaterally with foreign governments.

- Improving information sharing among Federal departments and agencies and with the private sector by establishing a task force to accelerate implementation of key components of the International Trade Data System; and by formalizing information-sharing agreements where necessary to improve the United States Government’s situational awareness of cargo and goods moving throughout the supply chain system.

- Streamlining and integrating public-private partnership programs requirements across relevant Federal departments and agencies and with key foreign trading partners.

- Emphasizing the completion of additional mutual recognition arrangements with key trading partners.

- Engaging industry stakeholders and private sector owners and operators by continuing the Cross Sector Supply Chain Working Group, and increasing the coordination and awareness between it and other industry or government advisory groups.


---

2. The 2012 arrangement with the European Union brings the total number of mutual recognition arrangements to seven Customs Trade Partnership Against Terrorism and Authorized Economic Operator mutual recognition arrangements; a maritime security mutual recognition arrangement with the European Union, air cargo security mutual recognition arrangements with 33 foreign nations, and mail security requirements with 32 nations.
Secure Supply Chain Management in a Changing World of Threats

An Australian Cautionary Tale

By Kevin Nevrous

THE GOAL for every organization is to drive shareholder value through improved profitability, enhanced revenue generation, cost reduction and better asset utilization. On paper, global, or even regional, moves look great and, in reality, might be the right thing for an organization to do. However, moving operations or sourcing supplies offshore – in a changing world of threats – has the potential to substantially increase a company’s risk level if correct risk-scenario planning is not employed and, typically, companies don’t have sufficiently strong processes in place for a review of risk scenarios.

As witnessed by the recent demise of Melbourne-based motor-component company Ajax Fasteners, when you have increased supply chain complexity, there is inherent added risk. And it is only going to get tougher to maintain a secure supply chain in a world increasingly affected by terrorism, natural disasters and pandemic threats.

If transport services are cut so that employees can’t get to work or they stay home due to fear of contagion, or if a product gets into the wrong hands, or distribution is disrupted because component parts are not available, the supply side will feel the pain immediately. The demand side follows soon after because it can’t fill orders. The resulting loss and market-share erosion will hit the entire company and its shareholders hard. In fact, from a cost and disruption perspective, product and supply chain disruptions can have every bit as far-reaching an organizational impact as an Australian Securities and Investments Commission non-compliance letter, fine or shutdown decision, if not more.

Often when disaster strikes, cross-functional groups look to each other for ownership of the problem and, at times, blame each other. It is easiest to fault the supply organization when something goes wrong; after all, it owns the “physical” inventory. However, in reality, every department bears responsibility for risk and security planning, because every link in the supply chain can be impacted through an adverse event.

The threat related to, and the key to managing, supply chain complexity is similar for corporate and government organizations alike. The challenge – and the responsibility – is to vigilantly maintain sustainable business-continuity management (BCM) planning. Implementing a boardroom-driven, cross-functional secure supply chain process can potentially stop most security breaches, or threats, before they happen. Organizations need to continuously ask questions like: What is our level of risk exposure? What happens if, for instance, there is disruption at the ports in Singapore? What happens if there is a natural disaster in China? How do we protect against counterfeiting? Is our risk and scenario planning developed enough to protect against these types of threats?
Unfortunately, most organizations fail to engage in this type of holistic, enterprise-wide thinking. For BCM plans to be sustainable, they must be regularly pulled out of the drawer for scenario testing and evaluation. Most importantly, BCM planning must be integrated across the whole enterprise and driven from the boardroom.

While many Australian companies and government organizations might like to believe this country’s physical isolation means relatively low risk of exposure to pandemic flu or viruses, we are potentially at risk. You have only to look to the SARS outbreak in Toronto, Canada, in 2004 – which shut the entire city down for two days – to realize the knock-on effect for essential services and supply chains for both government and business for months.

While the avian flu pandemic may yet turn out to be “Y2K with wings,” the threat regionally of natural disasters, terrorism attacks or a pandemic flu is very real. The World Health Organization has defined six phases of an influenza pandemic and, in terms of the avian flu, we reached Phase 3. Even if a pandemic were localized to Asia, which is unlikely, this scenario still has the potential to bring down a growing number of countries now dependent on the region’s low-cost labor and manufacturing. Australian government and business would most certainly be disrupted.

As an aside, it might be noted that the U.S. Centre for Disease Control and the World Health Organization believe the threat of a global pandemic flu is 100 percent likely, and that it’s overdue!

In this scenario, there will be challenges and responsibilities for all levels of government, businesses and individuals who will be impacted. All are responsible for preparedness and response to the next terrorist event, pandemic or natural disaster.

- **Imagining the Unimaginable**

There is today a need more than ever to proactively address low-frequency, but high-impact risks. Some of the greatest losses in value or capital occur because of exceptional events: systems failures, financial crises or terrorist attacks. It is important to realize that just because a risk may seem unlikely, its ultimate cost – the failure of a company or even a government – makes an investment in preparation for the unimaginable eminently worthwhile.

Yet, despite the potentially devastating impact of unlikely events, managers often emphasize the most-likely risks faced by a company when assessing its risk position. Probability models are based on likelihood and impact for given events – but tend to be biased, as they focus on the more-frequent risks or events, while overlooking low-probability events that could be devastating.

Rare events – from pandemics to tsunamis – are not preventable, but organizations can adjust their operational and capital structures to meet them. Stress tests and scenario planning provide an avenue for understanding the potential impact of rare events that are typically omitted in risk models. A stress test, for example, examines an organization’s ability to withstand specific scenarios and events. They are crucial in answering the question, “What can go terribly wrong?”

In addition to stress testing responses to low-frequency events, companies need to enhance their capability to respond to chosen scenarios. A company can build its ability to respond to different scenarios by selectively investing in requisite capabilities needed should the event occur.

For instance, a company might take a partial equity stake in a company in another market, or region, with the option to migrate to full ownership. A media company, for example, could support many different technologies and strategies for online media distribution until standards become well-defined. By initially supporting multiple technologies, the vendor/supplier in effect takes a “real option,” which allows it to adapt quickly to changing market conditions.

- **Business Continuity Management (BCM) and Planning (BCP)**

BCM and BCP are high on the organizational agenda following a spate of so-called rare events, e.g., 9/11 attacks, computer-network virus attacks and natural disasters. They have risen even higher today in the context of the current climate change and sustainability debates. Yet recent research in the U.S. by Deloitte shows that business-continuity programs have often not addressed the enterprise level, and that companies frequently do not take into account supply or vendor dependencies on third parties.

The lack of readiness of companies in addressing the eventuality of a pandemic flu is very much a case in point. A study by the Deloitte Centre for Health Solutions revealed a marked lack of preparedness. It is very much the same in Australia and the Asia-Pacific region, where by their own assessment:

- 66 percent of companies had not adequately planned to protect themselves from the impact of a pandemic flu;
- 73 percent of companies said they could use help understanding what they should do to plan for a pandemic outbreak;
- 39 percent of companies believed there was not much a company could do to prepare (while 41 percent disagreed).

Despite the challenges of addressing a possible pandemic, businesses must play a key role, along with governments, in planning for such an event (especially since it is regarded as 100 percent probable!).

While the cost of imagining and managing low-frequency risk can be high, the return on the investment is definitely worth it, especially when viewed from the stakeholder perspective.

A good case in point is Citigroup,
which began investing heavily in security and continuity planning some years before 9/11. It was one of the first major financial institutions to establish a backup trading area. When 9/11 took place, it was one of the first to get operations back up and running.

**Best-Practice Supply Chain and Business-Continuity Management**

In the course of interviews and research conducted by Deloitte, it has become very clear that some global corporations have already developed a number of best practices for managing a variety of security, performance and operational risks. A common thread for each is the ongoing sustainability of the programs they institute. These organizations:

- have an ongoing commitment to security and risk-management planning;
- keep risk assessments and contingency plans up-to-date;
- are clear about staffing issues and infrastructure or supply backup;
- keep vendors and customers informed;
- develop guidelines for managing a crisis locally if communications with headquarters fail;
- create a crisis-management team and guidelines;
- review major sites globally to assess exposure for people, facilities, data and other business-performance risk;
- protect high-visibility offshore and local operations by changing schedules and routines, so patterns cannot be detected;
- make sure local managers in foreign locations are informed of developments elsewhere in the organization; and,
- conduct drills and risk-scenario testing regularly.

**Conclusion**

Australian corporations that have gone global, or even regional, must recognize that they are on the front-lines of western global influence. As such, their facilities, their suppliers and vendors, and their brand and reputation are vulnerable.

Risk-management and best-practice business-continuity programs are essential to fostering the long-term sustainability of a company and its supply chain. A focus on costs and measurable financial success can obscure the real and vital contributions of non-financial factors in sustainable profitability. Outstanding quality, smooth supply chain operations and strong commitment to employees and customers are all key factors in profitability and establishing supply chain value.

Imagining and managing risk is not tangential to ensuring sustainability. To effectively imagine and manage the many indicators of success and risk requires leadership on the part of management and stakeholders. Therefore, organizations need to continually and effectively adjust and align their strategy, operations, governance and decision-making so that they can be proactive in identifying and quickly adjusting to changing risks and market conditions. Specific recommendations to improve supply chain security should include a mix of people, process and technological enhancements. Securing the supply chain process needs to be elevated to senior company leaders, who look beyond functional or departmental silos to implement a holistic, enterprise-wide secure supply chain strategy.

In short, developing a secure supply chain and business-continuity program is a way for companies to optimize enterprise activities to make sure all suppliers, and the company itself, have the right products, at the right time, under the right risk scenarios. It’s protection against “what if” and “it will happen” during a time when “the unthinkable” can become the reality.

Kevin Nevrous is lead partner for the Business Continuity Management team at Deloitte Risk Services in Australia. He can be reached at knervous@deloitte.com.au.
A formal audit plan must be in place to ensure compliance with security protocols.

Diligence...is required nowadays to stay ahead of the bad guys.

**PHARMACEUTICAL SUPPLY CHAINS** feature regularly in the news; product contamination, counterfeiting, theft and recalls, because of their potential impact, are certainly newsworthy. For pharmaceutical distributors – particularly those that also operate as pharmaceutical wholesalers – these are make-or-break issues, high-risk challenges that could have an impact not only on their profitability, but also, more widely, on consumer safety.

All 3PL providers, no matter what they handle, must consider the prospect of internal threats. Given their daily access to product and in the absence of adequate controls, employees could fairly easily tamper with or steal items. Extensive employee screening, training, supervising and monitoring help to minimize these risks. Measures such as tightly restricting access to alarm codes, periodically changing access codes, and implementing rigorous, automated inventory-control and order-processing systems further reduce internal risks.

Companies that distribute high-value products, including many pharmaceuticals, must also contend with serious external hazards. In this article, we focus on the threat of theft by outsiders.

Protecting a pharmaceutical distribution center and its employees from the risk of break-ins is an obvious necessity. Security measures and equipment include perimeter protection and surveillance, video surveillance, adequate internal product cages or vaults, mantraps (with options including bullet-resistant construction and metal detectors), keypad or electronic-reader access throughout the facility, employee training, scrupulous compliance with visitor security procedures, and regularly tested alarm systems.

For a company like McKesson Corporation, the largest pharmaceutical distributor in North America, protecting itself against the risk of theft is critical. Terry Carrico, vice president, corporate security & safety for McKesson in Alpharetta, Georgia, stresses the importance of a security plan for any 3PL provider dealing with pharmaceutical products. No corporation, he says, has enough resources to mitigate all of the risks it faces. He recommends instead that a company identify and understand its risks, then take steps to counter those risks, tackling the most-serious first and foremost.

### Developing a Security Plan through a Five-Step Process

Carrico’s corporate security team, working with internal business units, follows a five-step process in assessing risk in order to develop required security plans. Following is a sample of the thinking involved in those five steps. These steps would serve any warehouse-based logistics operation interested in reducing security risks.

**Step 1: Identify critical product.** Controlled substances, for example, are
highly sought-after by the black market.

Step 2: Identify threats. Organized gangs target full truckloads (FTL) of pharmaceutical product after surveillance of DCs.

Step 3: Identify where the company is vulnerable to the threat. At the first stop made by the driver after leaving the DC, particularly if within 200 miles of the point of origin, the truck and product(s) are most vulnerable.

Step 4: Determine the company’s risk related to the threat. How likely is it that such a theft will occur?

Step 5: Mitigate the risk. Implement counter measures to reduce the likelihood of an occurrence.

Assessing risk is an ongoing process for Carrico’s team, and the security plans that result through the process are subject to regular updates.

A complete security plan, says Carrico, addresses four fundamental areas. The example outlined below continues on the theme of FTL theft; it highlights the fundamental security areas a 3PL provider focused on risk will want to implement in selecting a transportation contractor. It is when a product is in transit, says Carrico, that it is most at risk for theft.

1. Security management. In selecting a transportation contractor, a 3PL provider should determine if the company has a security professional responsible for security, and examine the contractor’s security plans and policies. Some considerations, for example: Does the contractor use a risk-assessment process to identify threats to its operation? Does it conduct employee background checks and drug testing, and audit its security program?

2. Physical security. Are all entry points to the contractor’s trailers capable of being secured? Are FTL shipments locked and properly sealed? Does the contractor have a policy whereby drivers must stop only at protected locations, preferably at company terminals where available?

3. Electronic security. Are the contractor’s trucks and trailers tracked electronically? Does it use geo-fencing to monitor that drivers are complying with their planned routes and not making unplanned stops?

4. Procedural security. Does the company observe a two-driver rule for high-value shipments? Does one of the drivers remain with the truck at all stops? Do its trucks arrive with a full tank of fuel to preclude stops within the “red zone,” an area of 200 miles around the DC in which gangs are most likely to attempt a theft? Does it have emergency-response procedures for inclement weather, accidents and maintenance failures?

The 3PL provider can further protect its high-value shipments by placing covert tracking devices with the product being transported in the trailer. If the truck is stolen and the product removed, the covert device, if undetected, will allow the product to be tracked and possibly recovered by police.

A formal audit plan, says Carrico, must be in place to ensure compliance with security protocols. Contractor audits are part of such a plan, and should be stipulated in any service agreement with a transportation contractor. An agreement should specify the right of the 3PL provider to perform a certain number of announced audits and unannounced spot checks, and to receive the results of the contractor’s internal audits and street audits.

Security: A Continuous Process

Risks for 3PL providers change, as do the technologies they can use to mitigate risk. Staying abreast of security risks and technologies, particularly for companies dealing with high-value products, is key to success in avoiding – and responding to – potential threats.

The Pharmaceutical Cargo Security Coalition (PCSC) provides cargo-theft alerts to members on a regular basis. McKesson’s regional director receives these notifications and passes them on to each of the company’s DCs as they arrive; knowing when and where thefts are taking place keeps security staff apprised of risks. With that information, they can put drivers on alert to potential threats along their delivery routes.

McKesson’s security team continuously reviews its security processes and fine-tunes its security programs. Diligence to this degree is required nowadays to stay ahead of the bad guys.

A multi-step process is required to assess risk in order to develop the required security plans.

Success cannot be found in a box.

Work with an executive coach and look in the right places.

My clients are:
• Clear on what’s important to them
• Focused on results
• Paying Attention to new opportunities
• Intentionally creating the future, not just letting it happen

Is your business where you want it to be? Are you where you want to be? If not, call Head Coach Chip Scholz or check us out on the web to learn more about taking your success to the next level.

Call 704-827-4474
www.scholzandassociates.com
ARGO RELEASE/SIMPLIFIED ENTRY – now being rolled out in the air cargo environment – is the first phase of U.S. Customs and Border Protection’s efforts to modernize the cargo release process within CBP’s Automated Commercial Environment, known as ACE.

ACE automates and consolidates border processing and centralizes CBP access, linking CBP to the trade community and other government agencies. ACE provides CBP personnel with enhanced tools and information to decide – before a shipment reaches U.S. borders – which cargo may pose a risk and which cargo should be expedited.

The stakes are high. In fiscal year 2011, CBP processed approximately 23.5 million cargo containers arriving by land, air and sea. In 2012, CBP expects to have facilitated approximately $2 trillion in legitimate trade, while enforcing U.S. trade laws that protect the economy as well as the health and safety of the American people.

The success of this program depends on close collaboration with the trade community that draws on the best practices of both government and industry.

Valarie Neuhart, director of trade operations for CBP’s Office of Field Operations’ Cargo and Conveyance Security Division, explained that “the overwhelming response from our trading partners is that this new process will greatly improve how they are able to handle releases and arrange for cleared cargo to quickly depart the airport/terminal and be delivered to the importer.”

Cargo Release/Simplified Entry has been hailed by industry participants. Simplified Entry is an innovative approach to the import entry process and Boeing was eager to partner with CBP in the pilot program,” said Kathryn

(Photo courtesy Eduardo Perez, U.S. Customs and Border Protection.)
Greaney, vice president of global trade controls for the Boeing Company. “Boeing has been impressed with tangible results of the Simplified Entry process and looks forward to the program’s expansion.”

Participants in the Cargo Release/Simplified Entry pilot must be certified as brokers under CBP’s Customs-Trade Partnership Against Terrorism, known as C-TPAT, or as C-TPAT Tier 2 (or above) certified importer/self-filers and have the relevant system requirements.

By the end of September 2012, more than 18,000 simplified entries had been filed for more than 490 different importers.

**Win–Win**

Cargo Release/Simplified Entry offers numerous benefits to trade stakeholders:
- Drives down transaction costs;
- Streamlines and expedites the release of cargo;
- Enables importers/filers to update transportation and entry information in real-time, earlier in the transportation chain;
- Enhances cargo security.

The new program also helps CBP employees work more efficiently:
- Enables CBP personnel to apply more time and resources to the identification of potentially high-risk shipments;
- Provides CBP and other government agencies with more accurate and timely data.

Cargo Release/Simplified Entry helps Boeing achieve its core goals of moving cargo efficiently and predictably. “We anticipate this program will not only enhance cargo security, but help to streamline our entry process and supply chain,” said Greaney. “Boeing has been a participant in the Importer Self-Assessment program for several years. We appreciate the compliance-based partnership with CBP through the ISA, and this new simplified entry process is one more benefit of that enhanced cooperation.”

“FedEx Express is pleased to be working with CBP on this progressive pilot program,” said Andy Shiles, U.S. regulatory compliance manager for FedEx Express U.S. Global Trade Services. “Simplified Entry is a positive example of CBP’s ability to work closely with the trade industry to co-create new procedures that will allow all of us to work more efficiently and effectively. FedEx is looking forward to full implementation of Simplified Entry at all U.S. clearance locations.”

Simplified Entry moved from concept to actual functionality in less than a year, which reflects the program’s ease of use and its appeal to the importing community. The Simplified Process Joint Industry-CBP Workgroup met for the first time in June 2011; in May 2012, the first simplified entries were filed under the pilot program.

The response to CBP’s Nov. 9, 2011, Federal Register notice announcing the Cargo Release/Simplified Entry pilot was encouraging and enthusiastic: CBP received 40 applications almost immediately. In December 2011, CBP selected nine companies to participate in the Simplified Entry pilot for air cargo: A.N. Deringer; Expeditors; FedEx TradeNetworks; FH Kaysing; Janel Group of New York; Kuehne & Nagel, Inc.; Livingston International; Page & Jones, Inc.; and UPS.

CBP’s Office of International Trade worked closely with the pilot participants to develop a pilot schedule that allowed for robust systems’ testing for both CBP and the trade prior to going live.

The first Cargo Release/Simplified Entry pilot began on May 29,
2012, at three ports (Indianapolis, Chicago and Atlanta) to test the program’s capabilities. On July 25, CBP opened the pilot for volume testing of simplified entries by the initial pilot participants in the three pilot ports.

Based on the initial pilot’s success, on Aug. 14, 2012, CBP published a second Federal Register notice announcing the further expansion of the Cargo Release/Simplified Entry pilot for additional participants in the air mode of transportation.

The broker submits the shipment data, called the “entry,” and the carrier submits the transportation data in the form of the “manifest.” Before creating Cargo Release/Simplified Entry, brokers submitted certain transportation data along with the entry. CBP already receives these transportation data from the carrier, resulting in a duplication of effort. With Cargo Release/Simplified Entry, CBP has streamlined the entry process for trade stakeholders. In addition, because brokers often have shipment data well before transportation arrangements are finalized, brokers can provide this information to CBP earlier in the process.

The result? Instead of having to wait for the carrier to submit transportation information to include on the entry, brokers or importers/self-filers can submit the entry at any time prior to the cargo’s arrival in the U.S.

Furthermore, instead of supplying 27 data fields on CBP Form 3461, Cargo Release/Simplified Entry filers need only to submit 12 data elements (plus three optional ones), cutting the paperwork almost in half. Because the brokers or importers/self-filers can file their data in advance, CBP can perform critical targeting functions earlier in the process, ensuring that cargo gets to its destination faster and more securely.

“We’re finding that the early transmission of fewer data elements prior to export is resulting in faster clearance times and delivery,” according to Boeing Vice President Kathryn Greaney.

“Simplified Entry filings for Boeing’s Charleston location have been a huge success. Due to a limited inland freight movement schedule, if freight arrives after hours, expedited freight arrangements must be made and freight dispatch times are affected. Simplified Entry allows CBP to provide information on the likely disposition of the imported cargo prior to arrival, allowing for greater predictability and efficiency. It also reduces the need for costly delivery arrangements,” Greaney said.

**Next Steps**

CBP is exploring options for adding additional functionality to the pilot, such as the ability to electronically accept supporting documentation via the Document Image System and the inclusion of the Participating Government Agency Message Set, which will consolidate the data needs of all 46 government agencies involved in the import and cargo release process.

Finally, CBP is developing a plan to expand Cargo Release/Simplified Entry to the maritime cargo environment. “The major reason that Simplified Entry is not in the marine environment today is that we wanted ACE eManifest for rail and sea to be fully deployed before implementing a new system or process. Consequently, CBP elected to begin the Simplified Entry testing in the air environment. So far, that testing has gone extremely well, and we anticipate moving into the marine environment as soon as possible,” said CBP’s Neuhart.

That’s a move eagerly anticipated by importers. “We welcome the use of Simplified Entry for other modes...” Continued on page 32
In Late October 2010, air traffic at airports around the country was disrupted and the world’s attention centered on a series of planes – both passenger and cargo – believed to contain explosives. The suspected bombs weren’t carried on board by passengers, but were contained in cargo – computer printers, to be exact.

The printers, shipped from Yemen, had been loaded with cartridges that, instead of containing normal toner, actually contained the high explosive known as PETN, and they were rigged to be detonated via cell phone. For most Americans, the movement of cargo across the skies was an invisible process, and the images of planes surrounded by law-enforcement vehicles at airports around the country served as a wake-up call.

For the people of U.S. Customs and Border Protection, the events of those days exposed a critical gap in the way that air cargo was screened and processed as it entered the U.S. The packages from Yemen were specifically designed to be nearly impossible to distinguish through non-intrusive inspection processes such as X-ray.

That level of complexity meant that knowing a package is suspicious required more complete information: who shipped it, from where, what is supposed to be inside, and where the package is headed, among other pieces of data. Under the Trade Act of 2002, CBP has the authority to request information on incoming shipments, but at the time of the attacks, that data was received just four hours prior to its arrival in the U.S.

“To put it simply, if you wait until four hours before arrival, it has a greater potential to put bad things in U.S. airspace,” said Chris Kennally, CBP deputy executive director for cargo and conveyance security.

It was clear that CBP needed to get information about air cargo shipments sooner, but often people decide to ship a package via air because they have very little time to spare before its intended arrival. Unilaterally placing an arbitrary requirement on shippers could prove crippling to their ability to move cargo around the world.

The solution to these issues is known as the Air Cargo Advance Screening program, or ACAS, and it is blazing new trails in how the nation secures air cargo.

Industry Partnerships

Within days after the incidents, CBP officials reached out to leaders in the air cargo industry to determine the most effective course of action. In examining the breadth of the global movement of air cargo, it was clear that the express consignment industry – companies like FedEx, DHL, UPS and TNT
Comprising more than 75 percent of all air cargo shipping globally, these companies were in the unique position to spearhead this project, needed to leverage its existing targeting systems – powerful programs that compare information on people and goods entering the U.S. using risk-based targeting. When it came to finding the best possible ways to make sure that data could be used effectively by CBP, the agency sought industry’s guidance, with a goal to find ways to bring the companies’ powerful information sys-

said Kennally, by having full control of the packages they shipped from the moment they were accepted for shipment to the moment they were delivered to a loading dock or a doorstep.

“They own the planes, they have the data, and they have control over the merchandise,” he said of the express consignment companies. “We said, ‘Why don’t you guys step up and pilot this?’ and every one of them raised their hand, because every one of them has a vested interest in security.”

In fact, the data provided by their customers when sending a package was exactly the data that CBP

was the most fertile ground for a new screening program.

“What the Yemen incident taught us was that CBP needed to get this information faster,” said Robby Beau, managing director of U.S.-Global Trade Services for FedEx.

A True DHS Collaboration

While the sharing of data between industry and CBP was a huge milestone in the effort to secure air cargo, it did not represent the end of the process. The Transportation Security Administration is charged with securing air travel in the U.S. and has played a key role in the air cargo security strategy.

In the months before the Yemen shipments, TSA had mandated all air cargo bound for the U.S. to undergo X-ray screening, which provided a key layer of security. As the printer cartridge attacks showed, however, non-intrusive screening was not a solution unto itself.

CBP and TSA leveraged each other’s legal authorities to create a unique arrangement that would enable the agencies to receive advance data and mitigate risk before shipments are loaded on aircraft departing for the U.S. As part of this arrangement, TSA personnel are now permanently stationed at CBP’s National Targeting Center – Cargo, working alongside CBP targeters to identify packages that pose a possible security threat to the nation.

A Rapid Deployment

With all of the necessary pieces in place, ACAS was officially launched as a pilot program in January 2011. The program began by screening packages bound for the U.S. from 28 countries in the Middle East and North Africa that were shipped by the four major express shipping companies.

What began as an experiment quickly became a massive success both for government and industry.

“ACAS improves supply chain security, and it also benefits the par-

TSA inspectors work alongside CBP officers in the National Targeting Center – Cargo as part of the ACAS program. (Photo courtesy of U.S. Customs and Border Protection.)
“participants,” said Norman Schenk, vice president for customs and trade compliance at UPS. “By providing better data earlier in the process, ACAS reduces the number of inspections and improves customs clearing times.”

According to Kennally, many of the fines faced by shippers importing goods into the U.S. come from erroneous or incomplete manifest information. The ACAS program has refined the process of creating and updating those manifests with the best information possible, which means reduced penalties and a more efficient shipping process.

In its first nine months, the program screened more than three million packages bound for the U.S., and of those, only a few were flagged for further inspection and none were prevented from entering the country. The adjudication process for a suspicious package typically involves either a clarification of data or a further inspection of the package to relieve any doubts about its security.

“The advance screening of pre-departure air shipment data adds an important layer of security for our private sector partners, enhancing our ability to secure air cargo destined for the U.S. and helping to protect America 24/7,” said Dan Baldwin, CBP executive director for cargo and conveyance security.

To date, ACAS has processed more than 80 million shipments and is receiving data from 189 countries worldwide.

**Looking Forward**

ACAS is still a growing pilot. Air cargo enters the U.S. not only through express shipments from the four companies that helped launch the pilot, but also on passenger planes operated by traditional airlines and specialized heavy-shipping companies that send massive containers, automobiles and other large items into the country via air.

Currently, ACAS has participants representing the entire air-cargo transportation stream. These include express shipping companies, passengers, freight forwarders and heavy all-cargo carriers. Thanks to CBP’s willingness to work with private industry early in the process, the air-cargo industry has been enthusiastic about participating in the expanding pilot program.

“CBP and TSA both have collaborated closely with air cargo stakeholders to phase in ACAS using a pilot-program approach,” said Barbara Vatier, who co-chaired the Global Cargo Programs sub-group of the Department of Homeland Security’s Air Cargo Security Working Group. “The airline industry appreciates this partnership with government and the opportunity to work together in a way that improves security while speeding the transport of goods.”

Other nations have also reached out to CBP to learn more about ACAS and how it works in order to create similar screening systems for air cargo entering their own countries. These nations are working closely with CBP and TSA to harmonize their processes with ACAS in order to replicate worldwide the same efficiencies created by ACAS.

Ultimately, ACAS is expected to include screening of all air cargo bound for the U.S. before the flights...


Kathleen Franklin is a writer for U.S. Customs and Border Protection. This article originally appeared in *Frontline*, the agency’s magazine.

Jay Mayfield wrote this article while he was a public affairs specialist at U.S. Customs and Border Protection. He now serves as a senior public affairs specialist at the U.S. Federal Trade Commission.

This article originally appeared in *Frontline*, the magazine of U.S. Customs and Border Protection. It is republished with permission.

**SURVEY** from page 13


**TOOLS** from page 28


**SURVEY** from page 13


**SURVEY** from page 13


**SURVEY** from page 13


**SURVEY** from page 13


**SURVEY** from page 13


**SURVEY** from page 13


**SURVEY** from page 13


**SURVEY** from page 13


ANY 3PLS don’t have an abundance of resources to throw at IT. Building and maintaining an effective, secured IT infrastructure requires a significant investment in time, money, space, expertise and resources. However, using up-to-date, secured infrastructure today could never be more important, especially for small businesses. According to the latest Symantec Internet Security Threat Report, in 2012, 31 percent of all cyber-attacks were directed against businesses with fewer than 250 employees, an increase of 13 percent over the previous year.

The simple fact is, even as a small company, running your business with unsecured IT infrastructure paints a red “X” on your forehead.

Whether you are looking for better security, a means to differentiate your business or reduce costs, or a more-robust, highly available infrastructure, the cloud can help. There are several different types of cloud services out there, but for the scope of this article, I will focus on how you can use one of the fastest-growing cloud solutions, infrastructure as a service (IaaS), to secure your data, discuss some of the different IaaS vendors in the marketplace, and show you how to utilize one of the most popular IaaS providers, Amazon Web Services (AWS), to realize the potential of the cloud for your business.

■ But Wait, Isn’t the Cloud Less Secure?

One of the most common misconceptions about the cloud is that it’s less secure than a traditional approach. However, the data simply isn’t there to support that claim. In fact, several studies have found that the exact opposite is true. Alert Logic, a leading IT network security company, performed several studies over the last two years comparing the threat data of IaaS cloud customers and customers with traditional datacenters. In its spring 2013 State of Cloud Security Report, Alert Logic found that traditional datacenter environments were attacked both more frequently and with more sophisticated and targeted attacks than cloud environments, a trend that has stayed reasonably consistent over the last two years. See Figure 1.

■ What is IaaS?

Gartner*, a leading information technology research and advisory company, defines IaaS as:

*A standardized, highly automated offering, where compute resources,
complemented by storage and networking capabilities, are owned and hosted by a service provider and offered to customers on-demand. Customers are able to self-provision this infrastructure, using a Web-based graphical user interface that serves as an IT operations management console for the overall environment.”

In other words, the IaaS provider handles the datacenters, cooling, power, servers and so on, allowing you to focus on your environment.

■ Who Offers IaaS Cloud Services?

Some of the most recognizable IaaS players in the market are Amazon, Microsoft, IBM, BT, Rackspace, and CenturyLink. The beauty of the cloud is that it gives you the ability to run your services on top of the same multibillion-dollar IT investments of these massive companies.

For instance, Microsoft’s Azure cloud platform hosts over 299 million Skype users, 50 million Office Web App users, and nearly 50 million Xbox Live subscribers, in addition to businesses utilizing its IaaS services. Amazon Web Services (AWS) hosts many services, including Netflix, SAP, Sage, NASA, NASDAQ and, of course, Amazon.com. So, you can bet that these IaaS providers are committed to ensuring that their solutions work.

■ Why Many IaaS Customers Choose Amazon Web Services

AWS offers an incredible number of features and services for a cheap price. In 2013 alone, AWS released 71 new services and features. Since 2006, prices on various AWS services dropped over 30 times. Also, AWS boasts one of the most robust infrastructures on the planet, with eight geographic regions to choose from, each with multiple, highly available datacenters for failover and redundancy capabilities.

AWS also controls the lion’s share of the IaaS market. According to Synergy Research Group, an IT-analytics company, by Q1 of 2013, AWS owned 34 percent of the market. The next two largest competitors, IBM and Fujitsu, controlled 6 percent and 4 percent of the market, respectively.

Furthermore, in October of 2012, Gartner released its Magic Quadrant for Cloud Infrastructure as a Service report, placing Amazon’s cloud solution in the “leaders” quadrant based on its ability to execute and completeness of vision.

So how did AWS grow to become a market leader? Beyond its robust features, services and competitive pricing, a key factor in AWS’s success can be attributed to economies of scale. As more customers sign up, costs drop and AWS is able to pass on the savings to customers and invest in new features. And, with reduced prices and new features, more customers sign up and the cycle starts over. See Figure 2.

Since AWS is both one of the most widely recognized and successful IaaS providers out there today, let’s look at several benefits and features it offers to secure your environment.

■ Physical Security

Don’t underestimate the importance of physical security. With physical access to your equipment, a malicious intruder or internal employee can take down services, steal information, and destroy both data and hardware. Also, with critical equipment on site, other risks to your business infrastructure increase dramatically, such as power spikes, ineffective cooling, equipment failure, natural disasters and theft.

Any credible cloud provider, including AWS, secures its infrastructure in a set of certified datacenters, staffed 24/7 by trained personnel and locked down with multi-factor authentication mechanisms, cameras and security guards. Also, these datacenters have built-in redundancies in everything from power and cooling to servers, network devices and connectivity. And remember, because it’s the cloud provider’s equipment, it is responsible for ensuring that all infrastructure components stay operational.

■ Network Security and Monitoring

AWS offers several network-security tools that allow you to easily and effectively secure connectivity to your AWS environment, including technologies like Virtual Private Cloud (VPC) and security groups.
Also, AWS watches for suspicious traffic and blocks certain types of attacks automatically.

Some of the network-security functions that the VPC and security groups provide include:

- The ability to establish secured, encrypted VPN connections between AWS and your local sites;
- Restricting which services are allowed into or out of your cloud environment; and,
- Limiting which servers within your cloud environment can talk with each other.

AWS offers other connectivity options as well, such as Direct Connect, which lets you establish a dedicated network connection to AWS.

For monitoring your environment, AWS has a system called “CloudWatch,” a built-in reporting mechanism to monitor your resources in real time and send alerts. CloudWatch has a list of pre-populated metrics, but you can also build your own custom metrics, and define alarms and alert-notification thresholds. Another interesting feature is URL monitoring, which keeps tabs on your websites. See Figure 3.

■ High Availability and Storage

The cloud offers a level of failover capability and data resiliency unachievably by most organizations. In the unlikely event of a failure, services can be moved to a secondary or tertiary location, often completely transparently or with limited downtime.

AWS has eight different “Regions” all over the globe, including Ireland, Singapore, Australia, Japan, South America, and several in the US. Each region contains a cluster of “Availability Zones,” each of which comprises multiple, highly available datacenters interconnected with low-latency links. You can choose to deploy your services to any Region, and freely move your environments between each Availability Zone within the Region. See Figure 4.

To keep your data safe, AWS stores and replicates data between Availability Zones with its “S3” storage platform. S3 has a 99.999999999 percent data-durability design goal. AWS also offers other storage options, such as “Glacier,” which provides a cost-effective method to store backups, and “EBS IOPS” for faster speeds and guaranteed disk performance.

■ Other Considerations

Because the cloud is located off site, ensuring a constant, low-latency connection to the cloud is Continued on page 42
T HE Customs-Trade Partnership Against Terrorism (C-TPAT), Partners in Protection (PIP) and Authorized Economic Operator (AEO) programs are, respectively, the American, Canadian and European Union supply chain security programs designed to help facilitate border crossings for known, trusted traders in times of high alert. At such times, border crossings are reduced, and priority is given first to critical loads, followed by trusted traders, leaving others to wait. Joining these programs is not required, but note that unpredictable world events in far-off places do affect many borders all over the world, including in the U.S. and Canada, and could inhibit the movement of goods.

In North America, the Fortune 100s that depend on on-time delivery were the first to join C-TPAT and PIP. They realized that the cost of delivery delays could be higher than the cost of security measures. To help ensure that their front-of-the-line, fewer-searches status doesn’t attract illegal “hitchhikers,” low-risk members must be committed to keeping themselves and their supply chains secured. In fact, a weak link in a member’s supply chain could cost it its coveted position to move goods ahead of unknown traders. To encourage supply chain partners to participate, many members are including requests in their supplier contracts, requiring that the suppliers qualify for C-TPAT, PIP or AEO, as applicable. This means previous relationships could be at risk if the suppliers are not in compliance.

Most people are good. Unfortunately, though, there are people trying to take advantage of our freedom to cross borders. To lower chances of disruptions to business as usual, you must be aware of your vulnerabilities, leaving no doubt about your security practices and no opportunity for someone to use your weaknesses to support their undesirable deeds.

If you are doing business with a member of C-TPAT, PIP or AEO, or anyone in a secured supply chain, you and your staff need to know about these programs. To be in compliance, you must look at your location and your security practices, as well as your supply chain partners. Each program has minimum requirements that are generalized guidelines for both large and small companies. The information you provide assists customs border agents to judge your worthiness for membership as a trusted trader. These requirements should help guide you to look for your unique vulnerabilities. It is important to go beyond paper reporting systems. The bad guys will go deeper and so will the customs agents. Validators from the respective programs will visit you to see for themselves.

The aim is to eventually harmonize all programs. C-TPAT and PIP agents have been working together in harmonization for a few years now. The European Union’s AEO program is getting its footing. Requirements for all three are still a work in progress. In order to qualify for all supply chain security programs, including future programs, you should focus on finding and ad-
dressing your weaknesses. No two locations are alike, even when built with identical blueprints. And it is difficult to live up to the security expectations of a large company carrying high-value product if you are a mom-and-pop operation trying to stay in the game, yet both large and small are using the same application based on the same minimum requirements.

After conducting hundreds of vulnerability assessments, I can assure you that many weaknesses are unique and not found in the minimum requirements of C-TPAT, PIP or AEO. In fact, many issues are caused by your staff, often innocently, and are avoidable once the employees are trained and their apathy is transformed to co-operation.

### Impacts of Security Programs in the Warehouse

Warehouses are an important part of the supply chain. I have seen this confirmed by U.S. Customs and Border Protection (CBP) agents when choosing which location to validate first in determining a client’s membership status in C-TPAT. The client had manufacturing facilities across North America, yet the CBP agents chose to visit a third-party warehouse/distribution center first, rather than the company’s own facilities. Having multiple clients coming and going can pose a risk for many 3PLs, depending on how well the warehouse has prepared for the trade-security programs.

If left unsecured, third-party warehouses could compromise the hard work done – and the money spent – by their clients to qualify as low-risk members in C-TPAT, PIP or AEO. Informed clients will want to regularly visit the facilities of their 3PL providers to get a true picture of goings-on. Providers must always be prepared to “show well.”

Many warehouses I have visited were well-organized and personnel were in total control of all goods and activities. However, I have also visited sites where anyone could access product and no one would notice or care to stop them; even if they wanted to, they didn’t know how.

Here are 10 security issues I have seen in visits to warehouse facilities.

1. Goods were not where expected. Some had overflowed their racks, mixing with another company’s goods, and become accessible to strangers.
2. Handicapped-access buttons were not deactivated after regular hours, and could be used to automatically open perimeter doors when the warehouse was closed with no one on duty.
3. Loading docks were left open with no visible staff present and no perimeter access controls.
4. Fences were not only installed backwards providing easy access rather than perimeter control, but they also had holes cut in them by employees seeking shortcuts home.
5. Staff had no knowledge of C-TPAT, PIP or AEO, even though they had clients that were in the programs and visits by Customs agents could occur at any time.
6. People with records for crimes that should raise red flags for their job responsibilities had been left in charge of operations.
7. Drivers were left to freely access entire warehouses.
8. Shipping paperwork was left available for multiple third-party drivers to view in finding their orders among all orders.
9. Third-party drivers were provided extra seals that were left unaccounted for.
10. Unlocked rigs were left on site for extended periods of time with keys in the ignition for convenience. Some of these rigs had extensive damage to interior walls (great places to hide things).

Warehouse staff has to be prepared to answer to Customs agents about anything they see on site and, if your people are keeping secrets from managers, the surprises could cost you your client relationships really fast.

If you think you are okay when you have addressed the application minimum requirements, think again. I have received calls from those whose customers received their goods with unrelated weapons and ammunition included. I have also received calls from panicked companies after they lost a $10 million account within 15 minutes of losing their status in C-TPAT followed by their PIP membership. A third-party supplier was the cause.

The programs are voluntary for the moment; it is hoped that businesses will step up and take responsibility for the safety and security of their goods, their staff, their clients, their communities, their trading partners and their country. We are living in challenging times. Purchasing software or more security cameras, fencing and gates is not enough. You need your people aware and co-operative.

Your people will be the first to help or the first to breach your best security plans. Thus, people are the key to success in securing a supply chain. Bring them on board, train them so they know how to get involved and help you prevent issues. Management is often the last to know, and your staff could be innocently creating your biggest liabilities.

Most businesses are not security-equipment experts, yet they would rather spend money on security technology and expensive hardware than help their people understand how to practice threat awareness and prevention. Your people are your most important layer of security. They can prevent an issue, while your cameras are just reactive tools useful after an incident has taken place.

It costs much less to train people than to purchase expensive security gates that staff leave open. Once you realize you should be a member of a trusted trader program, make sure you transform the apathy of your staff and create security eyes and ears that are working with you and not against you.

Terry Nusyna is CEO of TN Security Intelligence. She can be reached through www.tnsecurity.ca.
IN A RETAIL ENVIRONMENT, much of the security focuses on protecting the merchandise. Yet, the risks begin long before the merchandise makes it to the store. Security has to begin with the supply chain and in warehouses and distribution centers.

The first area of risk falls within the supply chain itself. According to a report from Deloitte, The Ripple Effect: How manufacturing and retail executives view the growing challenge of supply chain risk, globalization and the push for greater efficiency and cost reductions has increased the security risks within the supply chain. The report states, “There are now more risks to the supply chain and risk events are becoming more costly. As a result, 71 percent of executives said that supply chain risk is important in strategic decision making at their companies.”

The Deloitte study points out four key elements that are essential for lessening supply chain risks. They are:

• Visibility: The ability to monitor supply chain events and patterns as they happen, which lets companies proactively – and even preemptively – address problems. Critical enablers include people capabilities and analytics capabilities.

• Flexibility: Being able to adapt to problems quickly, without significantly increasing operational costs, and make rapid adjustments that limit the impact of disruptions. Critical enablers include people capabilities and governance processes.

• Collaboration: Having trust-based relationships that allow companies to work closely with supply chain partners to identify risk and avoid disruptions. Critical enablers include people capabilities and analytics capabilities.

• Control: Having policies, monitoring capabilities and control mechanisms that help ensure that procedures and processes are actually followed. Critical enablers include governance processes and analytics capabilities.

These points can also serve as a guideline for how warehouses and distribution centers address their on-site security needs. As Andrew Elvish, VP of marketing and industry with Genetec, points out, there is always a lot of activity happening on the distribution side. Because of the layout of the centers, the high amount of traffic both inside and outside, and the constant flow of people, merchandise and machinery, it is vital for the facilities’ management to be equipped with the right security options to eliminate risk.

Security in a warehouse facility can be broken into two parts – inside and outside. As you set up your security system, you have to identify where the potential losses are coming from, both internal and external.

The trick to providing the best security in the distribution-center environment is to address the unique needs of the facility. One way, says Elvish, is to reconsider how to observe the inside of the center on the video screen. Lots of video management systems show their streams in 16”x9” format. However,
warehouses have long aisles that are only partially seen in the traditional screening method. Elvish believes that turning the video stream into a vertical rectangle rather than the horizontal solves this problem. It’s a small thing, he adds, but when you think about warehouse monitoring, it needs to be approached a little differently than for traditional retail space.

The security team must also consider access points into the facility, along with the natural flow of people throughout the day. Bill Smoyer, western regional sales manager with Access Hardware Supply, suggests that the number of people entering the warehouse daily should dictate how many points of entry there should be. How many entrances do you need for employees, for instance? Do you regularly have visitors coming to the office? If so, there should be an entrance specifically for them. The type of security at these access points should depend on the customers who utilize the facility and the products stored inside. A center that stores precious metals, for instance, may want to install metal detectors to deter theft. A custom warehouse would likely need more security at access points than one that held paper goods.

In addition to the everyday employees and visitors, supply chain facilities see a lot of truck traffic, and Smoyer believes that facility management should have some control over who is coming onto the property. He recommends that, in addition to the fencing that should protect any products stored outside, there should be a gate and a guardhouse to approve anyone going to the loading docks. A license-plate reader is another option for keeping track of truck traffic at the warehouse. According to Elvish, the reader can be used to monitor the trucks that come on to the property. You can use license-plate recognition to monitor truck traffic – what time did they arrive, when did they leave, how long were they at the truck dock, for instance.

Protecting the truck docks sets up a challenge because the doors are often left open all day. Whereas the front of the facility is well controlled, it is easy to enter the building through the docks. In this type of environment, Smoyer says the best security is to rely on employees to question anyone who doesn’t seem like they belong in the facility. Keeping doors shut and secured when the dock is not in use is another way to deter intruders. Cameras should also be focused on the dock area.

The warehouse yard also needs to be included in the security plan. This would include fencing around the yard and, depending on the situation, separate gating from the warehouse. Cameras should take a broad view of the yard, but also have the ability to zoom. Even though the yard may be well lit at night, the cameras should have capabilities to monitor the property in low light.

Security systems in a supply chain facility can do much more than provide security. The systems can act as enterprise-shaping technology and help the supply chain industry become more efficient. Most endpoints for warehouse goods work in a just-in-time environment – those goods sit in the warehouse until the moment they are needed, and then, of course, they are needed right away. The ability to build highly efficient systems is a big concern in warehousing. The security system allows managers to observe how goods are stocked and shelved, as well as how they are moved through the facility until they are loaded onto the trucks.

When BJ’s Wholesale Club decided to upgrade its security system, the company also wanted to run more efficiently and keep employees and customers safer. The company provides a retail experience in a warehouse environment. Although the company is selling directly to customers, the company has security needs more in line with the typical warehouse facility. Response time to potential incidents is paramount. Each location employed an older video system comprising a PC-based DVR and analog cameras to monitor its stores. The system featured an average of 32 cameras per store. But the legacy system was quickly reaching end of life, and more time was spent resolving issues with the DVRs, rather than using them to their best security advantage. Also, as in most warehouses, large equipment, such as forklifts, is frequently used to transport goods for restocking, and products are commonly stored on large pallets. The combination of a large space, frequent goods restocking and large machinery can lead to accidents. The company was looking for a solution that could help spot theft, fraud, intrusion and trespassing throughout the various stores, gas stations and distribution facilities. The system also needed to be scalable, in case camera deployments were expanded, and be able to store video for the length of time that the company needed, not according to the system’s standard capabilities.

BJ’s implemented an enterprise IP video-surveillance solution because the system can accommodate thousands of cameras and enables the company to set its own parameters for storage and recording schedule. Currently, the system is deployed in 75 stores, with another 60 to be brought on board within the year. BJ’s uses the solution to review video for investigations purposes and also on a non-incident basis to gather an understanding of where the stores could modify their processes before a loss or incident occurs.

BJ’s security system was built on the premise that it would add new cameras and facilities onto its network. One of the key considerations in putting together a security plan is scalability. As facilities add more acreage to the original property or expand to multiple facilities, the security system should be built to adjust to any changes. Another consideration is the ease of accessing and using the information that is coming from the security system, particularly if there are several warehouses.

Continued on page 42
For a typical warehouse, losses from theft are almost entirely down to employees; there are no customers to shoplift, and external thieves often work with an employee to gain access or information.

The threat from internal theft to your inventory and profitability is significant. It costs you in lost inventory, higher insurance premiums, and personnel turnover.

A recent study at the University of Florida reveals that security managers attribute more than 48 percent of theft to employees.

**Hire the Right People**

It starts with hiring the right people – which is easier said than done. You can reduce your risks with personnel steps like checking references and the backgrounds of your applicants. Look for felony records, especially for those you’re going to trust with access to areas with highly desirable inventory. Even mundane inventory will be pilfered at surprisingly high rates if you have the wrong people in place.

**Lay Out Your Warehouse for Security**

Figure 1 illustrates common security flaws in a typical warehouse and demonstrates ways you can utilize layout to reduce opportunities for theft.

1. **Trash dumpsters and other containers**: It’s a poor idea to place a dumpster or other bins, large containers, scrap vessels, or cans near an accessible door. They can become ideal places for thieves to stow stolen inventory for later pick-up.
up and removal to cars. If you cannot position your dumpster in a way that discourages thievery, consider making it lockable so that access is difficult to unauthorized personnel, searching it frequently, and letting people know it is monitored.

2. Total number of doors: This warehouse has far too many doors. There should only be one that is open, and there should be a guard or other employee in charge of watching this door. If fire regulations require more than one door, use bars that set off an alarm if the doors are opened. You can secure these doors with equipment such as folding security gates or man-trap cages if they are already in your facility (but be certain to follow all local fire codes).

3. Staging area: This staging area may be too close to the loading docks. If no one is around to keep an eye out, it would be easy to take something and put it in a truck.

4. Shipping and receiving doors: The receiving dock and the shipping dock are too close together, and there is no barrier between them. It would be easy to take things from one truck and put them into another. Erect a barrier between the doors if they are in place already, with easy cross-access between them.

5. Employee parking lot: This parking area is too accessible to employees who might steal inventory. The door is very close to the parking lot, making it easy to take things from the warehouse out to cars. It’s best to have parking separated by a comfortable distance from the warehouse doors, making it more difficult to transport pilfered items. Best-case scenario is to have a fence separating the warehouse from the parking lot, as well.

6. Trucker’s lounge, break room, etc.: To get to this lounge area, the truckers have to walk all through the warehouse. Look at the tracks (light blue arrows) to see where they might walk. Everything along these routes is at risk. It is important to restrict movement in your warehouse. Don’t let people just go wherever they want. If possible, lay out your warehouse to move visitors or guests to a lounge area without any access to inventory. If not, strictly instruct them on where they are expected to walk through your facility (and make sure they stick to it). Consider man-trap dock-area cages that let you admit truckers and other visitors at your convenience, within your restrictions.

7. Restroom location: This is a bad spot for the restroom. To reach it, the truckers have to walk through the warehouse. This puts your goods at risk of being stolen. Just because people are dropping off or picking up shipments doesn’t mean they are free to wander around. It’s best to keep unauthorized people out of the warehouse, or within a strictly limited path if they must be inside. There is usually no reason for someone other than your employees to be in your shelving or storage racks with access to stored items.

8. Bushes and foliage: Bushes, shrubbery and foliage are a good hiding spot for things stolen out of the warehouse, especially when they are near a door. Remove the bushes or lock the doors to curtail this avenue for thieves.

Utilize Warehouse Equipment that Secures Areas

Consider installing such items as security mirrors, which would give you visibility into closed areas, around corners and into hallways. Wire partitions and security cages will tightly control access. You can also limit access to an area with folding security gates, if you need flexibility and door coverage.

Lockable wire cabinets and lockers can provide pilferage deterrence and protection in the right situation. There are other products that can lock a pallet rack bay or a shelving unit down, allowing you to combine security and storage into the same process.

Security-focused storage equipment is not the sole answer, of course, but its role is often understated.

Monitor and Check Frequently

Look toward your inventory-monitoring processes to provide some relief. If you know what inventory you have and what you’re supposed to have at any given point, identifying a source of theft is much easier. If it goes on for weeks or months before you know about it, the damage has already been done and you probably won’t recoup the losses. It’s best to check early and often.

For extreme cases, there are companies that specialize in undercover operations and surveillance. You can find many of them by searching Google or Yahoo under the term “warehouse security system.” Often, they will discover problems that undermine productivity as well as pilferage. For instance, Florida-based Internal Intelligence International discovered a significant illegal drug-selling operation in the plant of one of its clients. This is an extreme measure, but if you need it, you need it.

Focus Security Systems and Processes Internally, as well as Externally

Sufficient monitoring systems should be considered for high-risk areas, too. Camera and surveillance systems are good, but something as simple and inexpensive as unscheduled walk-throughs are very effective theft deterrents. Unpredictability is the key. Your information should be timely, but your walk-throughs in the warehouse should be something that you do frequently and without a fixed schedule. Watch your loading docks and platforms – they’re very easy places for a thief to remove stolen property, often in partnership with an outsider. Your security system is typically designed to protect your facility from outside thieves. How much emphasis does it put on employee theft?

Read and Update your Knowledge

U.S. Customs and Border Protection has warehouse-security information for companies dealing
with customs issues available on its website, at www.cbp.gov. Many of its recommendations are common sense and apply to general warehousing, as well as customs-specific operations.

One common-sense recommendation is that you separate shipping docks from employee parking lots, making it much more difficult for employees to remove items from the warehouse.

No single thing will reduce theft, but a combination of processes, hiring standards, security systems and equipment will help you improve your operation and eliminate losses associated with internal inventory pilferage.

This article combines two articles previously published on the Cisco-Eagle website, “Employee Theft and the Warehouse” and “Lay Out Your Warehouse for Security: How Your Warehouse Layout Can Deter Inventory Theft, Pilferage, and Shrinkage.” The latter article was originally published on the Rutgers University Crime Prevention Service for Business website, at http://crimeprevention.rutgers.edu/index.htm.

DATA from page 35

paramount. Fortunately, internet service providers continue to push bandwidth rates higher and offer new services in more areas than ever before. You can also use several internet providers simultaneously to load-balance traffic across the internet links and prioritize production internet traffic.

Another point to keep in mind is that IaaS requires you to manage your environment within the cloud. Many providers, including AWS, have easy-to-understand tutorials freely available online. There are also many third-party companies that provide additional services to deploy, run and monitor everything in the cloud for you.

Finally, the cloud isn’t an end-all, be-all security solution. Ensuring that your organization follows best security practices is of the utmost importance, whether you are deployed in the cloud or not.

While the frequency of attacks on small businesses steadily increases, IaaS cloud providers such as AWS offer solutions that can not only help secure your mission-critical environment, but also provide you with an incredibly robust infrastructure unattainable on site.

The cloud will not solve all of your security concerns, but it can provide you with a great step in the right direction.

Jared Mendenhall has served the supply chain community for over five years, designing and recommending on-site and cloud solutions for Accellos Inc., a supply chain execution software provider for logistics service providers.

WAREHOUSE from page 39

houses hooked into one system. As Elvish points out, if the system is too complicated, it won’t be used.

Few companies have the luxury of having unlimited funds for security, so building a security plan for your budget requires understanding your needs. A smaller facility may want to consider products that are all-in-one, pre-packaged solutions with software pre-loaded, for example. Systems that are cloud-based are good options for areas that use fewer cameras, such as monitoring the facility’s yard. This cuts down on IT overhead and saves money. Most important, focus on today’s security needs, but plan to grow the security system as the distribution center grows.

Losses in the supply chain are costly, and as the Deloitte survey found, likely to grow if more isn’t done to recognize the risks and create a solid security plan.

Sue Poremba is a contributing writer to Security magazine. This article was originally published on www.securitymagazine.com; it is re-published with permission.
The Magic of Mentoring

By Chip Scholz

When people think of mentoring, they often associate it with an older executive who counsels a promising newbie. The senior leader advises the junior employee on his career, navigating office politics and what’s needed to get ahead. But mentoring has dramatically changed over the last few decades.

Maybe you find yourself stuck in a career rut or itching to broaden your skills and take on new challenges. Perhaps you’re eyeing a higher-level management role or other professional advancement. If you wait for senior managers to notice you and “bring you along,” you’ll be disappointed with the wait – assuming a promotion ever happens.

Effective mentoring is essential for leadership development. Done right, it’s one of the most powerful tools for gaining wisdom, reaping the rewards of job growth and achieving a strong competitive advantage in today’s job marketplace. Successful leaders mentor, coach and partner with their employees instead of practicing command-and-control management. Top organizations are more adaptive, innovative and smart about bringing out the best in their people. Employees are always learning, and managers are always teaching.

That said, it’s up to you to cultivate a beneficial mentoring relationship – and to pursue it with rigor and commitment.

Mentoring Vs. Coaching

“Mentoring magic cannot be a solo performance. It is not a one-way, master-to-novice transaction. To be effective and lasting, it must be accomplished through a two-way relationship – the synchronized efforts of two people.” – Chip R. Bell and Marshall Goldsmith, Managers as Mentors, Berrett-Koehler Publishers, Third Edition, 2013

At its most basic level, mentoring is the simple act of helping someone learn. But the relationship between the helper and “helpee” changes significantly when performed as a learning partnership. Today’s competitive organizations need “learning entrepreneurs,” whose curiosity is valued over conformity.

Words like “mentor” and “coach” are sometimes used interchangeably, but there’s an important distinction:

• Coaching is specifically aimed at nurturing and sustaining performance.
• Mentoring focuses on learning; its primary outcome should be competence, proficiency, skill, know-how and/or wisdom.

Coaching is practiced by managers who are responsible for meeting performance goals and by executive coaches who are hired to boost personnel development. Mentoring can be practiced without the supervisory constraints imposed by the organizational hierarchy.

While coaching and mentoring are similar, this article will assume that a mentoring partnership:

1. Exists between two people (usually one more experienced than the other);
2. Is dedicated to promoting self-directed learning and development.

What do we need to understand about mentoring, and how can this relationship be most helpful? How do you know when it’s the right time to find a
mentor? What’s the best way to start a mentoring relationship?

**Mentoring Myths**

In the last decade, the concept of mentoring has changed, but the need for career counseling has not. In fact, mentoring is more important than ever because most careers take numerous twists and turns in a rapidly evolving world.

In “Demystifying Mentoring,” a February 2011 Harvard Business Review blog post, Contributing Editor Amy Gallo identifies four common mentoring myths:

**Myth #1: Mentoring is a formal, long-term relationship.** Because the business world moves fast and people frequently change jobs, a long-term advisory relationship may be unrealistic. Mentoring can be a one-hour session; it needn’t be an official six-month assignment.

Instead of focusing on the long term, think of mentoring as a tool you can access when you need it. Of course, advice and guidance may be more relevant if they come from someone who knows you and understands your goals. But you still need to build relationships so you have connections in place when you require advice. In some instances, you may wish to consult people who don’t know you as well, but can offer a fresh perspective.

**Myth #2: You have to find one perfect mentor.** It’s actually quite rare these days for people to get through their careers with only one mentor. In fact, many people have several esteemed advisors. Seeking a variety of perspectives on a crucial issue may be warranted.

**Myth #3: Mentoring is just for junior-level employees.** Many people assume they need a mentor only when starting their careers. In reality, professionals at every developmental stage can benefit from a mentoring relationship. You may be surprised to find that reverse mentoring often occurs (a senior manager, for example, learns technology skills from a junior employee).

Don’t wait for problems to occur to find a mentor. Whether you are making a career change, taking on a new role or contemplating leaving a job, solicit advice from someone who has experienced a similar transition.

**Myth #4: Experienced professionals mentor out of the goodness of their hearts.** It can be an honor to be asked to mentor someone, but the relationship is about more than respect for a trailblazer. Mentoring should be useful to both parties. Think about what you can offer a potential mentor:

- Can you provide a unique perspective on his role in the organization?
- Do you bring valuable outside information that can help your mentor in her job?

While not a direct barter, you may be able to offer your prospective mentor a promise of future assistance.

**Dos and Don’ts**

Mentoring can take many forms, but your goal is to find the right kind of advice, from the right person, at the right time.

Gallo offers the following guidelines in her Harvard Business Review article:

**Do:**
- Build a cadre of people you can turn to for advice when you need it
- Nurture relationships with people whose perspectives you respect
- Think of mentoring as both a long- and short-term arrangement

**Don’t:**
- Assume that your success or experience precludes your need for a mentor
- Rely on one person to help guide your career
- Expect to receive mentoring without providing anything in return

“The most powerful yet difficult part of mentoring is being who you are,” write Bell and Goldsmith. “This is not to imply that a mentor must be some kind of super-hero without flaws, doubts or the capacity for making mistakes. Fundamentally, mentoring is about growing – mentors growing with protégés, protégés growing with mentors.”

**Encouraging Reciprocity**

An effective mentoring relationship can be best described as a mutual search for wisdom. It’s grounded in a true partnership that thrives on reciprocal facilitation of learning. Such reciprocity requires the mentor to surrender power differences to build rapport and trust. Learning cannot occur with fear in the room.

Bell and Goldsmith encourage the “SAGE” approach to forming the foundation for an effective mentorship:

- **S = Surrendering.** Power, authority and command (or the protégé’s perception of these traits in a mentor).
Entry Management: Maintaining Safety at Your Sites

Replacing keys, deleting expired codes and arming the intrusion system

By Jay Hauhn

MOVING EMPLOYEES and vendors smoothly in and out of a company facility outside of regular business hours (and during regular hours where constant security is required) can pose risky and potentially costly security challenges. Consider some of the following incidents...

• A major financial-services business had key locks on its local office doors. Each time an employee or vendor lost a key, a locksmith had to rekey the locks and provide new keys to all employees requiring access. This cost the business about $3 million per year.

• Members of a janitorial crew didn’t speak English well and didn’t understand instructions for disarming and rearming a local office’s intrusion alarm. The language barrier hindered the setting of alarms, which triggered numerous false alarms. The local police soon stopped responding to any alarms from the office, costing the business false-alarm fees.

• An office manager responsible for maintaining alarm access codes was constantly adding new employees and vendors, but did not always delete obsolete codes. This resulted in more than 300 inactive, yet still valid, codes built up within the office’s alarm panel. A former employee passed along his facility and vault access codes to a burglar, who used them to steal $400,000 from the local office.

Problems like these are common within the industry. Fortunately, today’s intrusion-detection systems can offer simple, cost-effective solutions for these types of situations.

■ Code-Management Solutions

Entry Management: When employees, couriers, ATM servicers and cleaning crews all carry keys, there are many opportunities for keys to be lost or stolen, requiring expensive replacement.

Wireless locks work with inexpensive access cards to open main entry doors. If a card is lost, it can be deleted from the alarm system with one touch on a keyboard. A new card can be created quickly on site.

Other cards in the system are not affected. Unlike keys, cards can be individually programmed to allow access only to certain areas and at defined times.

The battery-powered locks are easily installed with no wired connection to the central processor required. This type of system also compiles an audit trail of all entries and can create customized reports for the activities of any individual or of a specific entry point.

Alarm-Arming Management: Vendors failing to properly arm and disarm an intrusion alarm may create a major security issue. Many municipalities have police non-response policies and/or levy expensive fines after only a few
false alarms. Strengthening the arming and disarming process can help mitigate false-alarm issues.

That’s exactly what a modern intrusion-alarm panel can do. Each credentialed user’s profile can be customized to automatically rearm the system after a programmed amount of time. For example, the cleaning crew can be given an hour to complete its job; a courier may get only 10 minutes. Once a valid vendor has entered the office, the alarm is disarmed, yet the doors remain locked to anyone without a valid access card.

**Code Management:** Local site managers may typically be too busy – or simply forget – to delete codes when employees leave the company. In any given location, there may be 50 listed codes, but only 7 to 10 active users requiring access to the premises, vault and ATM room. This can create additional risk. One way to avoid the risk is to take advantage of a managed service from a security provider.

When a company requests a code change, the security provider’s central-monitoring-station personnel remotely upload and download from an office’s intrusion panel to delete unnecessary codes, or create new ones for new hires. Working with trained professionals can help mitigate a potentially serious problem of leaving your site at risk.

Access, alarm and code management are all important parts of managing security risk. Businesses need to reduce potential risks wherever and whenever possible. That requires awareness of best practices as they apply to both internal processes and available solutions. Centralized management of codes doesn’t automatically solve all of the challenges. A systematic approach to managing and improving your code-risk profile is needed.

**Code-Management Best Practices**

- Start with a code-risk assessment or audit
- Prioritize top deficiencies and evaluate where technology upgrades can help mitigate the risks
- Develop a code-management policy and communicate it
- Determine how to communicate any new processes to the affected employees and vendors
- Track your codes and report on changes frequently
- Expire codes that are not being utilized
- Change codes regularly
- Utilize technology to automate what can be automated
- Consider working with an integrator to perform not only the assessment but also the remediation plan.

**Quick Tips for Mentors and Protégés**

The quality of your mentoring relationship will determine its ultimate success. Each partner must accept responsibility for making it work. When something isn’t gelling, be sure to communicate your concerns. When expectations are met, let go and move on.

Bell and Goldsmith offer some fundamental tips in **Managers as Mentors:**

For being a great protégé:

- Select a mentor who can help you be the best you can be – not the one who can ease you into a promotion.
- You can sometimes learn more from people who are different from you.
- Clarify goals and expectations for the mentoring relationship, and communicate them in your first meeting.
- Be yourself. Be willing to take risks with new skills and ideas.
- When given feedback, listen well and say thank you.

For being a great mentor:

- Mentoring is a partnership to help your protégé learn. It’s not about being an expert or authority.
- Don’t instruct; foster discovery. Ask powerful questions instead of giving smart answers.
- Be authentic, open and sincere. Establish a comfortable and safe environment.
- Act more like a friend than a boss.
- Be curious and attentive.
- Give feedback with a strong focus on the future, not the past.

**Mentoring from page 44**

**A = Accepting.** Strive for a safe relationship. The protégé must trust the mentor to provide an environment that encourages risk and experimentation.

**G = Gifting.** A mentor should supply advice, feedback and/or focus. This stage is actually the most delicate. If the mentor has failed to pave the way for Surrendering and Accepting, the protégé may ignore, undervalue, resist or reject the gift of knowledge.

**E = Extending.** A mentor must help the protégé apply information to real-life experiences so self-directed learning may occur. Creative teaching tools include role-playing, feedback and storytelling.

**Chip Scholz is head coach of Scholz and Associates, Inc. and serves on the IWLA board of directors. This article originally appeared in the June 2013 issue of The Scholz Report. It is republished here with permission.**
Simplifying the User Experience

MercuryGate TMS, with ezClick architecture

Automate and manage complex workflows with ease!

www.mercurygate.com/ez
RACKS

SELECTIVE, ROLL FORMED, STRUCTURAL, PUSH-BACK, PALLET FLOW, CARTON FLOW, DRIVE-IN, CANTILEVER

- DESIGN  - MANUFACTURING
- ENGINEERING  - TURN-KEY INSTALLATION

Atlanta, GA TEL: 770-207-0002
Los Angeles, CA TEL: 949-757-1377

CONTACT INFO:
www.elitestoragesolutions.com