SUPPLY CHAIN BRAIN

Date: Tuesday, September 01, 2009
Location: GREAT NECK, NY
Circulation (DMA): 50,148 (N/A)
Type (Frequency): Magazine (8Y)
Page: 28,29,30,31,32....
Keyword: Center for Transportation & Logistics

Are Companies Slacking Off on Supply Chain Security?

BY ROBERT J. BOWMAN

Tough economic times are forcing many businesses to make substantial budget cuts. But security might be the one area where they can't afford to pare back spending.

The global recession has cut deeply into nearly every aspect of business operations. But supply chain security programs remain largely intact.

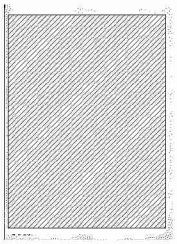
It's not as if companies had a choice. Regulators in the U.S. and abroad are ramping up their requirements for ensuring the integrity of import and export shipments, and the containers that carry them. At the same time, there are indications that cargo crime is on the rise, spurred by the worldwide economic crisis.

The Transported Asset Protection Association (TAPA) is warning of a surge in crime. The U.S. Federal Bureau of Investigation has previously estimated losses from cargo theft at some $30bn a year. Recent reports from law enforcement agencies suggest that illicit activity could be climbing in some locations by as much as 32 percent, according to Thorsten Neumann, TAPA's chairman for the Europe, Middle East and Africa (EMEA) region. Cargo most at risk includes consumer electronics, food and beverages, metal, clothing and footwear. In short, says Neumann, "We've seen an increased threat against the supply chain."

In particular, he notes a rise in theft from vehicle hijackings in the first half of this year. He ties the trend directly to the recession, which has swelled the ranks of the unemployed. TAPA points to a 19-percent increase in violent crime in the United Kingdom during the downturn of the early 1990s. Says Gilad Solnik of TAPA's Incident Information Service: "We expect 2009 to be one of the toughest years of the last decade in terms of cargo crime statistics."

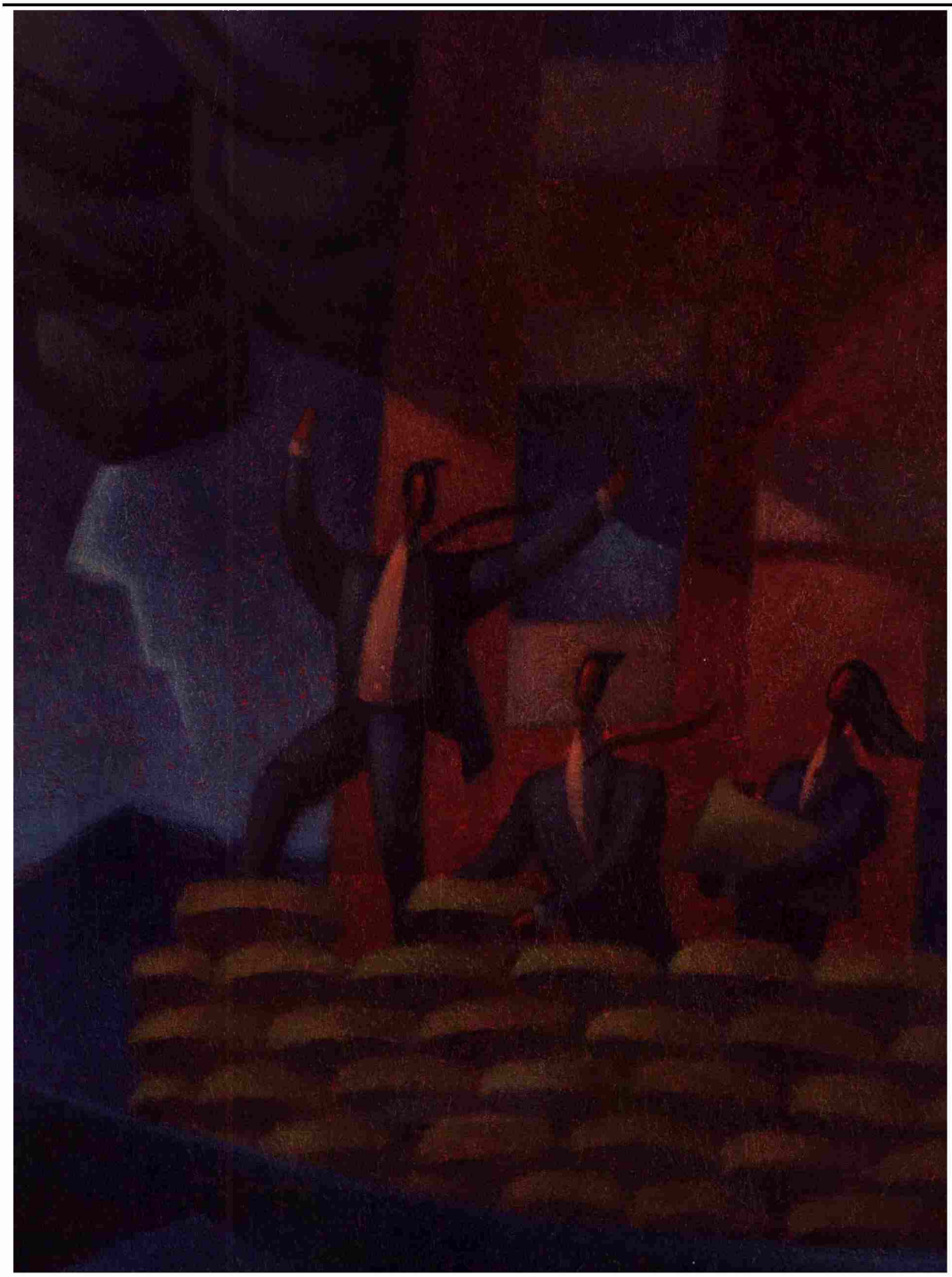
AMR Research hasn't seen businesses cutting back on spending related to security, even as they have shed entire plants and divisions, says chief strategist Kevin O'Marah. "You really can't afford to make a serious security blunder," he says. "On a relative basis, the cost just isn't that high to be secure. If anything, it seems to be a component of a [corporate] budget that is close to sacred."

The government is making sure of that. Since the terrorist attacks of 9/11, business has been presented with up to 20 new security initiatives, says Joe Dunlap, senior manager in the supply chain management practice of Accenture. Among the most recent is the "10+2" rule of U.S. Customs and Border Protection, requiring importers and carriers to submit additional data elements related to incoming shipments. The law officially went into effect at the beginning of this year, although CBP won't begin assessing fines for non-compliance until January 2010. Other initiatives to have surfaced in recent years include the Customs-Trade Partnership Against Terrorism (C-TPAT), Free and Secure Trade (FAST)



SUPPLY CHAIN BRAIN

Date: Tuesday, September 01, 2009
Location: GREAT NECK, NY
Circulation (DMA): 50,148 (N/A)
Type (Frequency): Magazine (8Y)
Page: 28,29,30,31,32....
Keyword: Center for Transportation & Logistics



SUPPLY CHAIN BRAIN

Date: Tuesday, September 01, 2009
Location: GREAT NECK, NY
Circulation (DMA): 50,148 (N/A)
Type (Frequency): Magazine (8Y)
Page: 28,29,30,31,32....
Keyword: Center for Transportation & Logistics

program, Operation Safe Commerce (OSC) and Container Security Initiative (CSI). Some are voluntary, others not, but all require an extensive commitment on the part of the commercial sector to protect against cargo tampering and terrorist acts.

The very meaning of the word "security" has evolved in the minds of supply chain executives over the last few years. As 9/11 becomes more distant in time, companies focus on more immediate issues. Security today means protecting against day-to-day incidents of cargo theft and threats to product integrity, O'Marah says. Terrorism, by contrast, has become "the monster under the bed. It's not going to mess with your orders."

Theft is a constant concern for global security managers, especially where high-valued goods are involved. Walt Fountain, director of enterprise security with truckload carrier Schneider National, cites the case of a stolen trailer (not being hauled by Schneider) with $11m worth of product inside. That might be an extreme example, but the average value of a load of merchandise is rising "fairly quickly," notes Don Osterberg, Schneider's senior vice president of safety, security and driver training. Products such as flat-paneled plasma TVs and iPods are making trailers and containers ever more attractive targets for thieves.

Other Priorities

With that trend in mind, it's not surprising that other security concerns are taking a back seat to outright theft of merchandise. "I've got to believe that terrorism is not even on the radar screen [for many businesses]," says Jim Rice, deputy director of the Center for Transportation and Logistics at MIT. They are concerned, however, with overall supply chain resilience—the ability to bounce back from any kind of disruption. For those organizations, security becomes one aspect of a larger concern, in which companies engage in continuity planning. Whether that exercise has much value in preventing acts of crime or terrorism in the first place is another question.

When times are bad, people and companies alike tend to look inward. For a consumer-products manager in the U.S., security is "mostly about protecting my brand," says Dunlap. What most frightens companies today is the threat of tainted product, which can cause death or illness and have a lasting impact on one's public image. Meanwhile, carriers, ports and third-parties must continually guard against garden-variety theft, even as they comply with rules that are primarily aimed at preventing acts of terrorism.

Of course, efforts to protect against those two threats aren't mutually exclusive. Companies are finding that the extra degree of diligence they achieve in meeting regulatory requirements can also give them tighter control over their supply chains. Knowing as much as possible about key suppliers isn't just a preventive measure; it's good business as well. And better cargo tracking capability can lead to lower inventories and improved customer service.

O'Marah suggests that companies can benefit in multiple ways from investments in systems and processes that achieve greater visibility of inventory throughout the supply chain. "It's not just a dollar spent on security," he says. "It's a dollar

SUPPLY CHAIN BRAIN

Date: Tuesday, September 01, 2009
Location: GREAT NECK, NY
Circulation (DMA): 50,148 (N/A)
Type (Frequency): Magazine (8Y)
Page: 28,29,30,31,32....
Keyword: Center for Transportation & Logistics

spent on efficiency. It will pay you back now and later."

Ty Bordner, vice president of solutions consulting with Management Dynamics, focuses on how companies can derive a return from necessary investments in security. The 10 new data elements that importers are required to file under the 10+2 Rule can end up saving a company money, he says. By supplying that information electronically, the importer relieves its broker of the need to re-key data manually, thereby reducing labor costs. A $100 entry fee might only be $60, and for high-volume importers, the savings add up quickly. By the same token, Bordner says, companies gained visibility over their suppliers by complying with an earlier Customs rule which mandated the filing of certain import information 24 hours prior to a vessel sailing from its origin port. (The same time frame applies to the additional data required under 10+2.)

Even so, the priority of many companies is simply to comply with the regulations, says Bordner. They're faced with a flurry of new rules and technology that can simultaneously make the country more secure and prevent cargo theft. Add to that the challenge of coping with recession, and it's not surprising that the security efforts of many executives are essentially reactive in nature.

"It's not just a dollar spent on security. It's a dollar spent on efficiency. It will pay you back now and later."

— *Kevin O'Marah of AMR Research*

What's not reactive is a desire for supply chain visibility, of which security is just one aspect. A recent survey of chief supply chain officers by IBM identified visibility as "one key capability that most global supply chains need," according to Mondher Ben-Hamida, an associate partner in the supply chain management practice of IBM Global Business Services. Companies can't respond properly to any type of event—whether it be theft, terrorism or natural disaster—without a real-time view of operations tied to a system of alerts. It was precisely this kind of capability that allowed Cisco Systems Inc. to secure alternative suppliers when a major earthquake hit China last year, Ben-Hamida says. The same setup works just as well for responding to incidents that compromise cargo security.

Modern-day information technology can link a business with all of its suppliers, especially in the age of the internet. But software alone won't get the job done. John Brockwell, global supply chain practice

SUPPLY CHAIN BRAIN

Date: Tuesday, September 01, 2009
Location: GREAT NECK, NY
Circulation (DMA): 50,148 (N/A)
Type (Frequency): Magazine (8Y)
Page: 28,29,30,31,32....
Keyword: Center for Transportation & Logistics

leader with J.P. Morgan Global Trade Services, says existing systems can theoretically track cargo throughout its journey, with minimal gaps. "What's scary is, you start to put a lot of technology on the solution and people think that is the solution. It goes back to the people you have and the process you have."

When it's approached from that perspective, supply chain security can be less expensive than companies might think. "When I look at any challenges, I look at the human [element] first," says Schneider's Osterberg. "I say, what can we do to keep people vigilant, aware of their surroundings and expectations? It doesn't cost a lot of money to do that." Schneider works closely with its drivers to assess the threat of a given situation, he says.

The carrier's efforts extend to all partners in the chain. In one case, Schneider scrutinized the process of moving a typical consumer electronics shipment. Following a meeting with all of the players, it made 25 corrections to the process, resulting in a 60-percent drop in losses within six months. "It wasn't so much about the technology," says Fountain, "but how we were coordinating use of the technology."

The Extended Supply Chain

A desire for visibility is one thing; making it happen in a globalized operation is another. Even the best-run supply chains tend to grow weaker from a security standpoint with the addition of multiple partners. Companies have a hard time keeping tabs on suppliers that are two, three or four steps away from their own operations, O'Marah notes. Often their biggest concern is securing the cheapest sources of raw materials and parts for later assembly; at such times, security concerns can get lost in the shuffle. Cut-rate suppliers are frequently the source of tainted or low-quality product, which can have a disastrous effect on corporate reputations.

Rice says companies haven't even managed to harmonize communications internally, let alone with outside partners. An effective risk management strategy must reach across disciplines, including operations, security and continuity planning. "Nobody's figured out how to do this in a matrix organization," he says.

The problem of dealing with multiple partners has compounded in recent years, with companies outsourcing bigger pieces of their supply chains. That strategy has helped to slash overhead while allowing businesses to focus on such core competencies as marketing and product design. But it has also made it tougher to secure the greater supply chain, says Ben-Hamida. "How can you pursue the two goals of being low-cost while [achieving] a great deal of visibility?" he asks. At the same time, he adds, companies need a high level of control over the extended supply chain in order to react quickly to changing business conditions.

Logistics service providers, meanwhile, have little incentive to invest in sophisticated tracking and tracing systems when their customers don't view them as strategic partners, Ben-Hamida says. That's one area where the recession has hampered security efforts, to the extent it has caused companies to focus on short-term issues of survival. They have cut back on investments that would have integrated them with their many supply chain partners, or led to better visibility of products and inventory.

For their part, carriers don't have the luxury of de-emphasizing traditional security programs. "We're highly regulated," says Earl Agron, vice president of security with APL. "We're also protecting multimillion-dollar assets. Even before 9/11, security was part of our framework."

Issues of piracy aside, a container is never safer than when it's deep in the hold of a ship. Far riskier is the process of offloading the box at a port, or transferring it to a surface carrier. "Most problems occur in the first and last mile, where you have transfer points and the cargo isn't moving," says Steve Sewell, senior vice president of Savi Networks.

He sees a number of "black holes" that can be plugged in part with visibility technology. Savi's answer is a Web-based platform, utilizing wireless data derived by tracking devices placed on containers. With the aid of satellite technology, Sewell says, "we know literally where cargo is in real time, at any time." Shippers don't have to rely on messages sent via electronic data

SUPPLY CHAIN BRAIN

Date: Tuesday, September 01, 2009
Location: GREAT NECK, NY
Circulation (DMA): 50,148 (N/A)
Type (Frequency): Magazine (8Y)
Page: 28,29,30,31,32....
Keyword: Center for Transportation & Logistics

interchange, informing them that the shipment has passed through predefined stages of its journey.

Too Much Technology?

Agron believes there's a limit to the value of sophisticated monitoring technology. Satellite systems allow shippers and carriers to track shipments virtually anywhere in the world, through a device that is affixed to the container. But he isn't sold on the reliability of the technology. For a carrier like APL, with half a million containers in its fleet, the effort might not be worth the substantial investment.

There's also the question of how to respond when the system indicates that a container has been stolen or breached. If a break-in occurs in an isolated area, asks Agron, how likely is it that a local sheriff will drop everything and respond to the alert? Moreover, the tracking units run on batteries, which must be stocked as spare parts and constantly replaced during the life of a container.

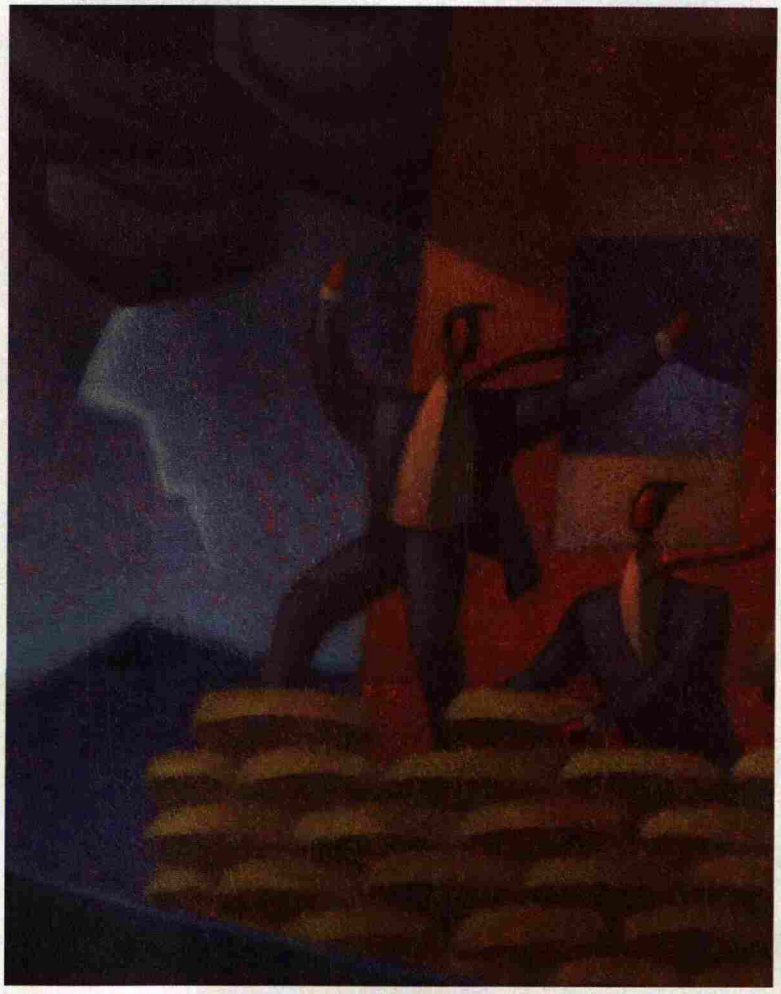
"It's an expensive solution," says Agron. "No one's been able to sit down with me and explain how it's really going to improve security."

Sewell counters that shippers can use the system to spot potential areas of risk, and redesign their routing accordingly. "One thing that's clearly of benefit is that people can identify where a problem occurred, and who was responsible at the time," he says.

The technology becomes more economically viable, Agron acknowledges, when it serves a dual purpose. Some carriers are using equipment monitoring to track the performance of their drivers—a variation on the old "black box" unit. They can tell when the vehicle is exceeding allowable speeds or not adhering to a chosen route. Still, Agron says, it doesn't make economic sense to deploy the pricey systems throughout a carrier's fleet, at every possible location.

Another weak link in the chain relates to the screening of key personnel. Brockwell says companies have been lax in the area of background checks. This despite the fact that "the biggest threat in terms of terrorism is an inside job." One employee in order management possesses enough information to tip off cohorts about the location or status of a shipment. While much attention has been paid to security at ports, relatively little effort is aimed at what happens to shipments traveling over unsecured distances, Brockwell says. DHS's Transportation Worker Identification Credential (TWIC) is a step in the right direction, but it must be backed up by diligence on the part of all companies involved in moving product through the supply chain.

Further clouding the security picture is the tangle of regulations being promulgated by various countries, who have made little effort to standardize their programs. Rules vary according to whether a container originates in Taiwan or mainland China, Ben-Hamida notes. The U.S. Food & Drug Administration, for one, is pushing to implement serialized item numbers on imports "down to the lowest level of granularity." It's doubtful whether that effort will



"No one's been able to sit down with me and explain how [the solution] is really going to improve security."

— *Earl Agron of APL*

conform to initiatives in other countries.

Neumann of TAPA suggests that global security programs won't become truly effective until they cross borders in both directions. C-TPAT only applies to goods entering the U.S., while the European Union has its own regime, in the form of the Authorised Economic Operator (AEO) program. The latter covers exports as well, although both programs remain voluntary. Eventually, says Neumann, they will probably become mandatory, as regulators ramp up the battle against both terrorism and organized crime. Shippers can further expect to encounter new rules for 100-percent screening of shipments entering the U.S. and other countries, despite the additional cost and time such a requirement would entail.

TAPA is adopting its own standards for implementing security measures within its members' supply chains. Developed in coordination with the European Union, the standards apply to such areas as incident reporting, truck routing, air cargo security, employee training and the certification of supply chain partners.

"Every country is implementing a program on its own through customs authorities," says Neumann. "The framework is the same, but the specific process can be different."

Ben-Hamida sees early signs of a move toward global security standards for all players. The International Standards Organization (ISO), with its 28000 series of specifications for security management, is leading the charge on one front. But the concerns of big American players such as the FDA and Department of Homeland Security, not to mention the European Union, must be satisfied before a truly global system can be put into place.

Recession or no recession, governments aren't holding back on new security efforts, and the private sector can't either. Rice urges companies to make more than a minimal effort, and devise programs that will realize additional benefits in the form of better visibility and control over their supply chains. In the process, they can achieve a degree of competitive advantage over those who prefer to sit out the slump. "If you're not getting ready for the upturn," he says, "when it comes, it will be too late."

To access this article online, visit The Digital Edition at www.SupplyChainBrain.com.

Resource Links

Accenture, www.accenture.com
AMR Research, www.amrresearch.com
APL, www.apl.com
IBM Global Business Services, www-935.ibm.com/services/us/gbs/bus/html/bcs_index.html
Management Dynamics, www.managementdynamics.com
MIT Center for Transportation & Logistics, http://ctl.mit.edu/
J.P. Morgan Global Trade Services, www.jpmorgan.com/tss/Product_Index/Trade_Services/1104848723140
Savi Networks, www.savinetworks.com.
Schneider National, www.schneider.com
Transported Asset Protection Association, www.tapaemea.com