

November 2002

Global eyefortransport research

Cargo Security Overview



*Technologies, Government and
Customs Initiatives*

Author: eyefortransport
Publication date: November 2002

Table of Contents

1.) Introduction:	3
2.) The threats:	4
2.1) Cargo Theft.....	4
2.1.1) <i>The effects of cargo theft?</i>	4
2.1.2) <i>Where does the threat of theft come from?</i>	5
2.1.2) <i>Why an increase in the threat of cargo theft?</i>	5
2.1.3) <i>Conclusions for Cargo Theft</i>	6
2.2.) Cargo Terrorism.....	6
3.) The key drivers for a secure global logistics chain	7
4.) The barriers to cargo security	8
5.) What are the solutions?	8
5.1.) Government, Trade and Customs initiatives.....	8
5.1.1.) <i>C-TPAT (Customs Trade Partnerships against Terrorism)</i>	8
5.1.1.1.) What is C-TPAT?.....	9
5.1.1.2.) What does participation in C-TPAT require?.....	10
5.1.1.3.) What are the benefits of participation in C-TPAT?.....	11
5.1.1.4.) Who is eligible for C-TPAT?.....	11
5.1.2.) <i>The Smart and Secure Tradelanes initiative (SST)</i>	11
5.1.2.1.) The founding members and technology being used.....	11
5.1.2.2.) The SST model and what will it solve?.....	12
5.1.3.) <i>The Container Security Initiative (CSI)</i>	13
5.1.3.1.) What is CSI?.....	13
5.1.3.2.) Why is CSI necessary?.....	14
5.1.3.3.) What are the benefits of participating in the CSI?.....	14
5.1.4.) <i>Other Government initiatives</i>	14
5.1.4.1.) Establish a database of vessels, cargo and passengers.....	14
5.1.4.2.) Force inbound freighters to transmit electronic crew and cargo manifests.....	15
5.1.4.3.) Coordinate business and security agencies efforts.....	15
5.1.4.4.) Secure Trade in the APEC Region - (STAR).....	15
5.2.) Technological solutions.....	15
5.2.1.) <i>Electronic Seals:</i>	16
5.2.1.1.) Design.....	16
5.2.1.2.) Feature & Functionality:.....	17
5.2.1.3.) Integration & Information Management:.....	17
5.2.1.4.) Procurement and Costs.....	17
5.2.1.5.) Standards.....	18
5.2.1.6.) Access Control.....	18
5.2.1.7.) Hardware and software.....	18
5.2.2.) <i>Biometrics:</i>	20
5.2.3.) <i>CCTV</i>	21
5.2.4.) <i>Container Sled: Cargo Transfer Apparatus and Method</i>	22
5.2.5.) <i>RFID</i>	22
5.2.5.1.) How does it work?.....	23
5.2.6.) <i>Real Time Location Systems (RTLS) and cargo security?</i>	23
5.2.7.) <i>Other Systems and Technologies</i>	24
5.2.8.) <i>Tracking Technologies</i>	25
5.2.8.1.) GPS/ Commercial Telematics - Global Positioning Systems.....	25
5.2.8.2.) Cellular based location services.....	26
5.2.8.3.) Assisted Global Positioning System (A-GPS).....	26

5.2.8.3.) Other emerging technologies	26
5.2.8.4.) Extending tracking information	27
5.2.9.) <i>Summary of technological solutions</i>	27
6.) Concluding summary – and general recommendations.....	28
6.1.) Adaptive Supply Chain Networks – is that the solution?	29
6.1.1.) <i>Sense and interpret</i>	30
6.1.2.) <i>Decide and act upon notification</i>	30
6.1.3.) <i>Learn and transform</i>	30
6.1.3.) <i>Supply chains must evolve into adaptive supply networks</i>	30
Future Cargo Security Reports and Events.....	31
List of References	31

1.) Introduction:

In today's economy, every organization is working on reducing its bottom line to get its profits up, as top line growth is almost non-existent. One area that can add to your organizations profitability, but which is often overlooked, is prevention of cargo theft. Putting this concept in perspective - "Depending on the respective organizations operating ratio, for every dollar lost through theft, it takes around \$3 to \$5 in increased revenue to make up for the loss, says John Albrecht, Vice President, Transport Security, Inc."

The need for cargo security is critical to assist the transportation industry in combating the serious increases in cargo crime and the increasing threat of cargo terrorism.

Cargo security is not an isolated event; security has to be applied across the value chain, across borders, (countries, departments, competitors, customers and transportation modes) and integrate an ongoing awareness in every single point of interaction with the goods. Hence security will only be as secure as the security of all the steps that have been before; that's why it's important to apply it across the value chain.

Every person who is involved in logistics, distribution or supply chain management are impacted by on-going efforts to create a more secure global trading system. In order to create this system, partnerships are designed to bring together the best technology, best industry practices and regulatory authority that would create a trust between businesses and governments and create a more secure supply chain.

2.) The threats

To understand the need and design for cargo security a deep understanding of the threats is very important. The threats that are relevant here can be classified into two categories:

- Cargo Theft
- Cargo Terrorism

Let us take a more in depth look at these threats and the damage they cause to the global transportation chain, the organization and the business.

2.1) Cargo Theft

Worldwide, the direct cost of cargo theft is estimated at about \$40 billion per year, with indirect costs many times higher.

"The theft of cargo has become so widespread that it constitutes a serious threat to the flow of commerce in the United States" – FBI Internal Report

A single truckload of cargo can be worth as much as \$3 million. The risk of theft, especially if the goods have a black market value, is very real.

2.1.1) The effects of cargo theft?

- For a business operating on a just-in-time basis, the loss of goods may threaten viability—particularly if insurance cover is inadequate or compensation payments are contested.
- Companies can be exposed to litigation, liability suits or other attacks on their brand name through theft related circumstances - stolen goods can be out of date or ineffective due to bad storage which exposes the company to dissatisfied customers who bought these goods in good faith.
- Stolen goods reduce profits exponentially by losses in sales opportunities caused by the distributors – where the competition is selling the goods without these “extra theft cost”, the distributors goods will never be able to compete.
- Further, the illegal sale of stolen cargo undercuts prices in legitimate businesses

2.1.2) Where does the threat of theft come from?

Cargo theft creates substantial economic losses, however it is an area of business crime that receives little attention, many incidents are not formally reported and media attention is rare.

Cargo theft is an internal (employee) or external activity or a combination of them both and can happen at many different interaction points. Eighty percent of cargo thefts are insider theft according to Claire Mayhew from the Australian Institute of Criminology, in "The Detection and Prevention of Cargo Theft" paper.

The most common interaction points of theft are:

- ❑ During hold-ups
- ❑ Freight yards and warehouses
- ❑ Containers
- ❑ Theft off/from trucks
- ❑ Documentary fraud
- ❑ During transportation
- ❑ Airfreight and ships

As mentioned earlier Cargo theft occurs across a range of freight forwarding and storage operations, but the greatest risk is during truck transportation or when vehicles are in the process of being loaded or unloaded.

2.1.2) Why an increase in the threat of cargo theft?

Most cargo crimes remain undiscovered until non-arrival at destination. During the meantime offenders usually have time to dispose the goods before the loss is discovered. (Most stolen goods are disposed of within 24 hours.) These delays also make recovery less likely.

Pressure from narcotics law enforcement agencies in the United States and stiff mandatory sentences for drug trafficking have caused many criminals to shift their activities to cargo theft and other transportation-related targets. A drug gang's organization, transportation, and underground marketing systems provide a readymade conduit for cargo theft and fraud. The new cargo criminals often are nationally networked and internationally backed and they are able to bribe insiders and maintain contacts that provide valuable information on the most profitable cargoes.

Reasons for an increased rate of cargo crimes are:

- ❑ The spread of global crime syndicates - Shift in organized crime activity from narcotics to cargo theft. Organized crime is responsible for nearly half of the losses caused by theft.
- ❑ Lack of reporting
- ❑ A new breed of smarter criminals, able to adapt to the new technologies of the cargo transportation industry
- ❑ The availability of low-risk, high-payoff targets
- ❑ The financing of criminal activities with billions of dollars from drug trafficking
- ❑ Even if these criminals are apprehended, they face lenient prosecution and sentencing.

2.1.3) Conclusions for Cargo Theft

These cargo theft losses not only affect the victimized transportation companies and their insurers—the illegal sale of stolen cargo also undercuts prices in legitimate businesses. For small businesses with limited stock that operate on a just-in-time basis, non-arrival of ordered goods may result in the loss of a valued customer and may even threaten.

The issues are simple. All companies are vulnerable to theft and loss conditions. They must take the time to enlighten and educate everyone in the business of these threats and their ramifications and reward those who can reduce their exposure to them in the course of doing their jobs. They need to stipulate how each person in a business can help save money by asset retention techniques. Business managers must not reduce budgets for these solutions. They cannot wait until they have a significant loss to consider theft a threat to profits.

Everyone must have ownership of business assets in a way that causes them to be prudent in protecting these commodities.

2.2.) Cargo Terrorism

Terrorism is a virtual economic blockade. It has become evident after the events of 11 September that the terrorist's main goal is to disrupt the economy. They certainly want to terrorize and create fear, but they also want to affect the country's economy.

According to a Brookings Institutes study the economic consequences of an attack on the supply chain would have more devastating economic effect than a direct attack on a large city. In case of a bio-terrorist incident directed at a major U.S. city, like San

Francisco or New York City, the economic impact would have a devastating effect of approximately \$750 million.

Now, if an event were predicated upon the supply chain, whether it were a weapon of mass destruction or an explosive device in a container or trailer, the economic impact would be over \$1 trillion.

One of the greatest post-9/11 concerns is that terrorists will use the global supply chain to turn ocean cargo containers into weapons of mass destruction. Traditionally, the approach to supply chain security was focused on keeping the goods that were supposed to be in the box, in the box. But last October, a discovery at the southern Italian port of Gioia Tauro shook the foundations. A suspected al-Qaeda terrorist was found inside a container. The suspect, who later disappeared while on bail, was equipped in comfort for the duration of the container's intended sea voyage from Italy to Halifax in Canada. He carried plans of airports, an aviation mechanic's certificate and security passes. Intelligence sources say other containers similarly fitted out were found at the Italian port. Since then, experts have suggested that further terrorist attacks may target security gaps in the cargo supply chain.

Now, there is an added responsibility to ensure that things that are not supposed to be in the box are actually kept out of the box. As an importer, you must now be able to demonstrate that you have both aspects of this process under control, and you must be able to demonstrate that control as it extends throughout your entire supply chain.

Everyday, more than 17,000 containers, carrying some 80% of US imports, come into American seaports, which are often located near major cities and industrial centers. Each container – about the size of an articulated lorry – has the potential to conceal a dirty bomb or a bio-chemical weapon and yet fewer than 2% are opened and inspected. Extra efforts are being designed to keep the terrorist needle out of the global trading haystack.

3.) The key drivers for a secure global logistics chain

- ❑ Imminent threat of cargo terrorism - The multi-modal nature of international transportation results in a myriad of disconnects between parties and systems. The opportunity to exploit this physical and related information 'disconnects' or gaps, is why international supply chains can be used as delivery mechanisms for terrorist threats.
- ❑ Growing threat of cargo crimes.
- ❑ Technology is available now.
- ❑ Understanding of the dependence on JIT organizations on fast global supply chains.

- ❑ To better enable homeland security programs.
- ❑ Need for economic stability.

4.) The barriers to cargo security

- ❑ The lack of effective cargo theft reporting systems
- ❑ The weakness of current transportation crime laws and prosecution
- ❑ The lack of understanding and education of the nature of cargo crime
- ❑ Inadequate support for cargo theft task forces
- ❑ The need to improve local law enforcement expertise on cargo theft
- ❑ The need for more effective cargo security technology
- ❑ Standards lacking
- ❑ Government endorsement or approval needed
- ❑ Complex systems integration
- ❑ Shared (federated) databases
- ❑ Funding sources: who will bite the bullet - the Government, the Industry, or the Consumers?
- ❑ Political issues across the globe

5.) What are the solutions?

There are many different types of threats and they arise from many different areas and directions. Now that we have a better understanding of the problems that we are facing we are in a better position to appreciate and understand the solutions at hand.

The present solutions or prevention activities are categorized in two broad categories:

- ❑ Government, Trade and Customs initiatives
 - C-TPAT (Customs-Trade Partnership against Terrorism)
 - The Smart and Secure Trade lanes initiative
 - CSI (Container Security Initiative)
- ❑ A range of technological solutions.

5.1.) Government, Trade and Customs initiatives

5.1.1.) C-TPAT (Customs Trade Partnerships against Terrorism)

C-TPAT, the Customs-Trade Partnership against Terrorism was developed to provide a template on how to handle cargo securely throughout global supply chains. C-TPAT is designed to secure the entire supply chain so that weapons of mass destruction or other terrorism efforts or terrorists themselves do not enter the U.S. through Ports, Terminals or Borders.

C-TPAT provides verifiable evidence that every organization participating in this initiative and their related suppliers are watching every event in the supply chain. Their enrollment and compliance demonstrates that the company is above reproach in the area of security and that all appropriate efforts have been taken to assure that each event in the supply chain is managed.

The events of September 11, 2001, caused the closing of the entire border and port systems. On that horrifying day, just-in-time production systems broke down, material flow was frozen and trade systems worldwide crumbled. Customs needed a methodology to begin processing goods at the borders and the ports, so a partnership was formed with key traders who agreed to demonstrate that they would attend to the security of products flowing into our trading system, regardless of mode or port.

5.1.1.1.) What is C-TPAT?

The partnership (C-TPAT) is designed to capture information and demonstrate control over all aspects of the supply chain including the events and providers that have a role in moving goods. It requires a complete self-assessment that encompasses procedural security, physical security, personnel security, education and awareness training, access control, manifest and conveyance security issues. The partnership requires that the organizations report back to Customs with an evaluation of their own supply chain systems and the actions you have taken or plan to take to assure that your entire process is secure. Customs will review the plan and make recommendations that they deem to be appropriate.

C-TPAT in bullet points:

- ❑ C-TPAT is a joint government-business initiative to build cooperative relationships that strengthen overall supply chain and border security.
- ❑ C-TPAT recognizes that Customs can provide the highest level of security only through close cooperation with the ultimate owners of the supply chain—importers, carriers, brokers, warehouse operators and manufacturers.
- ❑ Through this initiative, Customs is asking businesses to ensure the integrity of their security practices and communicate their security guidelines to their business partners within the supply chain.

C-TPAT will provide a guideline to determine how to open the borders if there is a future issue or concern at any border or port of entry. Participation in the program will determine the priority of trade flow as goods begin to move, when they begin to move through restricted border entry points. Preferential treatment will be provided to products that are determined to be the lowest risk and if there are ample evidence of control throughout the chain of commerce. On the other hand, non-C-TPAT materials will be subjected to intensive inspection during times when borders are closed or restricted. Carriers will be more inclined to move goods that have been demonstrated to be under appropriate care during times of crisis or tension. C-TPAT removes any client-based bias and provides an objective platform for processing merchandise and the assessment of risk.

This initiative will overlay the LRI (Low Risk Importer) Program and will expand the drug smuggling focus of programs such as the BASC (Business Anti-Smuggling Coalition) and the SCI (Super Carrier Initiative).

Private companies are being enlisted to push the borders and points of control all the way out to their offshore suppliers while maintaining the ability to validate security from the point of origin to the points of destination. This program will re-invent border security by moving the control of product away from the ports.

In addition, the goal is to engage the best of breed or emerging technologies that will provide electronic proof statements that monitor and report the movement of legitimate cargo in transit prior to reaching the border. Total asset visibility and authentication are the desired end state.

5.1.1.2.) What does participation in C-TPAT require?

Businesses must apply to participate in C-TPAT. Participants will sign an agreement that commits them to the following actions:

- Conduct a comprehensive self-assessment of supply chain security using the C-TPAT security guidelines jointly developed by Customs and the trade community. These guidelines, which are available for review on the Customs website, encompass the following areas:
 - Procedural Security
 - Physical Security
 - Personnel Security
 - Education and Training
 - Access Controls
 - Manifest Procedures
 - Conveyance Security.
- Submit a supply chain security profile questionnaire to Customs.
- Develop and implement a program to enhance security throughout the supply chain in accordance with C-TPAT guidelines.

- ❑ Communicate C-TPAT guidelines to other companies in the supply chain and work toward building the guidelines into relationships with these companies.

5.1.1.3.) What are the benefits of participation in C-TPAT?

C-TPAT offers businesses an opportunity to play an active role in the war against terrorism. By participating in this first worldwide supply chain security initiative, companies will ensure a more secure supply chain for their employees, suppliers and customers. Beyond these essential security benefits, Customs will offer potential benefits to C-TPAT members, including:

- ❑ A reduced number of inspections (reduced border times)
- ❑ An assigned account manager (if one is not already assigned)
- ❑ Access to the C-TPAT membership list
- ❑ Eligibility for account-based processes (bimonthly/monthly payments, e. g.)
- ❑ An emphasis on self-policing, not Customs verifications

5.1.1.4.) Who is eligible for C-TPAT?

C-TPAT is currently open to all importers and carriers (air, rail, sea). Customs plans to open enrollment to a broader spectrum of the trade community in the near future. C-TPAT membership will be made available to all sectors of the supply chain. Customs will be consulting with the trade community to develop the most effective approach for each sector to participate in C-TPAT.

5.1.2.) The Smart and Secure Tradelanes initiative (SST)

The world's three largest seaport operators have banded together to create this initiative called "Smart and Secure Tradelanes" (SST). Hutchison-Whampoa Ltd, PSA Corporation Ltd and P&O Ports handle over 70% of the world's container traffic, and they have agreed to collaborate to demonstrate and deploy automated tracking, detection and security technology for containers from the time they enter foreign freight terminals to when they are collected from US ports.

The Smart and Secure Tradelanes (SST) initiative, which uses wireless identification and detection technologies, was first installed in Washington by an initiative from Mrs Patty Murray, a US Senator from the state of Washington, in July 2002. The system is to be extended to the Port of New York-New Jersey.

5.1.2.1.) The founding members and technology being used

Founding members of Smart and Secure Tradelanes, initially driven by the industry, includes representatives with high-level military backgrounds, Hutchison Whampoa, P&O Ports, PSA Corporation, Savi Technology, QUALCOMM, SAIC, Parsons-Brinckerhoff and Sandler/Travis Trade Advisory Services.

SST is based on tried and tested RFID technology, which has been used by the US Department of Defense (DoD) for several years. Major port operators are adopting radio frequency id (RFID) technology in a bid to plug what has been described as the biggest hole in US security. The Total Asset Visibility (TAV) network has been deployed in 36 countries worldwide and helps the DoD to track and identify thousands of containers, providing real-time data on location. The system features anti-tamper tags, event-driven alerts, and virtual inspections and authenticated audit trails.

The technology was developed by Savi Technology with a grant from the DoD, and since receiving clearance to market the technology for civilian use, has been actively building support for the product within the container transport community.

Current solution providers involved in SST are:

- ❑ Savi Technology, which helped build and operates the TAV Network. TAV is the world's largest, active RFID tracking system and has been dubbed "the internet" of freight containers.
- ❑ Sandler, Travis Advisory Services, an international trade consulting firm.
- ❑ Qualcomm, a global leader for mobile fleet management using satellite communications and GPS systems.
- ❑ SAIC, a leading systems and technology company for ports and transportation companies including non-intrusive inspection.
- ❑ Parsons Brinckerhoff, the largest transportation and infrastructure engineering company in the world.

It is expected the system will be operational by the end of 2002.

(Note the technologies mentioned in the section above are explained later in this document)

5.1.2.2.) The SST model and what will it solve?

SST is seen as a potential solution for one of America's greatest worries, that somehow a terrorist group will smuggle a dirty nuclear bomb or biotechnology weapon into an American seaport in the heart of a major city. The US government wants to roll the system out quickly, and the initial implementation calls for an integrated security and container security system to register individuals, authorize roles and capture tracking and security events throughout the supply chain.

In time, working with shippers, carriers, service providers and foreign and US port terminal operators, containers will be tracked and automatically authenticated from the point of manufacturing, through ports of loading and transshipment, through to final discharge from a US port terminal. SST will work with government agencies to develop and test auditable security standards for maintaining secure ports, shipping facilities and container tracking and security.

“This is a model for how our nation can improve port security,” said Senator Patty Murray. “The new thinking, new technology and new partnerships at work here will result in a more secure and more efficient chain of commerce. This partnership protects our cargo and our ports and closes the gap that may leave us vulnerable.”

5.1.3.) The Container Security Initiative (CSI)

The U.S. Customs Container Security Initiative (CSI), proposed by Commissioner Bonner in January 17, would secure an indispensable but vulnerable link in the chain of global trade: the oceangoing sea container. Ensuring the security of the maritime trade system is essential, given that approximately 90% of the world's cargo moves by container.

Each year, more than 17 million containers arrive in the United States by ship, truck, and rail. In 2001, U.S. Customs processed more than 214,000 vessels and 5.7 million sea containers. A proactive stance by Customs in screening sea containers will significantly contribute to the agency's overall efforts to secure the borders against dangers that might be introduced through commercial traffic.

5.1.3.1.) What is CSI?

A proactive stance by Customs in screening sea containers before they reach the United States will significantly contribute to the agency's overall efforts to secure the borders against dangers that might be introduced through commercial traffic.

The Container Security Initiative consists of four core elements. These are:

- 1) Establishing security criteria to identify high-risk containers
- 2) Pre-screening those containers identified as high-risk before they arrive at U.S. ports
- 3) Using technology to quickly pre-screen high-risk containers
- 4) Developing and using smart and secure containers

The fundamental objective of the CSI is to first engage the ports that send highest volumes of container traffic into the United States, as well as the governments in these

locations, in a way that will facilitate detection of potential problems at their earliest possible opportunity.

5.1.3.2.) Why is CSI necessary?

CSI is an effort to enhance the security of the world's maritime trading system. By working together, the plan is to jointly achieve far greater security for maritime shipping than by working independently. Recognizing that trade is vital to the world economy, U.S. Customs has proposed the four-part program designed to achieve the objective of a more secure maritime trade environment while accommodating the need for efficiency in global commerce. A critical element in the success of this program will be the availability of advance information to perform sophisticated targeting.

5.1.3.3.) What are the benefits of participating in the CSI?

While the pre-screening that would be performed in the CSI presents clear benefits to U.S. security, early targeting of high-risk containers is potentially of great value to the ports that have implemented heightened security initiatives. A more secure maritime trade infrastructure would help ensure the continued smooth flow of merchandise through seaports. Ports that have implemented increased security and pre-screening will become more attractive locations to those companies that depend on timely movement of merchandise or processing inputs. In the event of a catastrophic event involving the use of seagoing containers and subsequent paralysis of maritime trade, those ports that have participated in the CSI are well positioned to resume operations quickly and with the confidence of the trade community.

In addition to these benefits, advance targeting of containers destined for the United States should, under normal circumstances, result in those shipments not presenting identifiable risks, clearing Customs rapidly, taking full advantage of the facilitative mechanisms that U.S. Customs has already been employing for some time.

5.1.4.) Other Government initiatives

Below is a quick overview of other Government initiatives that have been implemented or are being implemented.

5.1.4.1.) Establish a database of vessels, cargo and passengers

Senate bill 1214, the port and maritime security act of 2001, aims to gather and organize information about the movements of vessels, cargo and maritime passengers in a database. If the bill passes, a committee will have six months to report on the

feasibility of establishing a general database in order to identify criminal threats, national and economic security threats and threats of terrorism.

5.1.4.2.) Force inbound freighters to transmit electronic crew and cargo manifests

On May 22 2002, the house approved the customs Borders Security Act, which would require ships to transmit data about the people and packages onboard 48 hours before entering the port. The bills backers have no illusions about inspecting all shipments, but electronic manifests would enable logistics companies to create profiles that identify the high-risk shipments far in advance.

5.1.4.3.) Coordinate business and security agencies efforts

The presidents' Office of Homeland Security (OHS) has been charged with coordinating the activities of more than 100 government agencies, from the CIA to the EPA. Coordinating leads and tip-offs from law enforcement agencies has been hard enough – now the OHS must include data from the departments of Transportation, Commerce and the Treasury too.

5.1.4.4.) Secure Trade in the APEC Region - (STAR)

The Secure Trade in the APEC Region (STAR) is designed to enhance security while increasing trade. The STAR initiative commits APEC economies to accelerate action on screening people and cargo for security before transit; increasing security on ships and airplanes while en route and enhancing security in airports and seaports. The U.S. proposed earlier this year that APEC address this challenge by advancing secure trade initiatives. Recently APEC agreed and committed to a plan of action.

5.2.) Technological solutions

"To put it simply, the more technology and information we have, and the earlier in the supply chain we have them, the better," Homeland Security Department, Customs' Deputy Commissioner Douglas Browning told the House Government Reform Committee's National Security, Veterans' Affairs and International Relations Subcommittee.

Technology is believed to be the key to improved cargo security and management. Below you will find a list and review of the most common technologies that are available today.

5.2.1.) Electronic Seals:

Seals provide an easy and inexpensive way to verify tampering of contents within a container or other conveyance. They are designed specifically to detect unauthorized entry and or to leave evidence of an unauthorized occurrence. Compared to other technologies seals are easy to use and inexpensive

There have been notable developments in the seal technology area in the past five years. Strong and reliable mechanical seals are giving way to first generation electronic seals which, become powerful tools in a comprehensive security program, when backed by proper system protocols

Electronic seals are thought of as mechanical seals combined with specific electronic components. The result is a hybrid electronic seal that provides tamper evidence, physical security and data management. They indicate electronically whether the conveyance has been opened or tampered with. Electronic seals use RF (Radio Frequency), IR (Infra Red), and or fiber optics. Combined with these technologies, an electronic seal can also be compatible with GPS (Global Positioning System) and even cell phone technologies for a given applications.

Electronic seals are classified as active or passive. A passive seal is never electrified (AC or DC power) in anyway. Passive seals are intended for one-time use only and cost a few dollars. Active seals are electrified, are multi-use, and cost significantly more. The net price can be up to 10 times more the seals and necessary equipment. For example, readers are additional equipment required to interrogate the seal. An electronic seal can be interrogated manually or polled and interrogated remotely to determine if the seal has been breached. The seal can also be instructed to send an immediate signal or alarm via GPS.

An electronic seal consists of:

- 1) A type of housing for electronics
- 2) A cable or bolt seal
- 3) A unique and unambiguous identification number, which cannot be altered
- 4) A battery (power source)

5.2.1.1.) Design

A standard mechanical bolt seal combined with a data chip can record and store the seal number and other pertinent information as selected by the user. This combination provides basic barrier protection with the added benefit of basic data management tools, but not much more.

Electronic seals are valued for the ability to manage data including the seal number, conveyance contents, shippers contact information, and other manifest details. Most seals offer more details such as when the tampering of a conveyance may have occurred. Electronic seals can also guard against human error in logging seal numbers, thereby reducing the cost for administration usually associated with mechanical seals.

5.2.1.2.) Feature & Functionality:

Electronic seals combine the features and benefits of mechanical seals with advanced technologies offered by RF, IF, and fiber optics. These include such things as permanent unique seal identification numbers and seal memory to maintain any data required such as shipper, conveyance destination, and seal events. Adding GPS allows the seal to be polled remotely and interrogated for specific data.

5.2.1.3.) Integration & Information Management:

The essential risk of Who, What and Where can be managed manually with an electronic seal and a hand held reader. But more importantly, it can be done remotely and prior to the arrival of a conveyance. Technology providers and system integrators help make this a reality and the electronic seal then becomes a component of a larger service package.

5.2.1.4.) Procurement and Costs

Electronic seals range in price from \$5 to \$1000+ per unit, Additionally; they generally require computers, readers, and other equipment to function effectively. Pricing has come down considerably in the last two years along with less expensive technologies. However, pricing pressure remains intense, with many customers not yet prepared to pay for the additional equipment requirements,

Electronic seals, like mechanical seals, must be a part of a comprehensive security program and used in conjunction with proper system protocols. Electronic seals are in product development infancy. Testing needs to be done to ensure that manufactures claims are valid. These seals provide the best benefit when selected according to the application and when strict protocols are used. A "one size fits all" product does not exist. Electronic seals can be very good to assist with data management but more complicated than mechanical seals. And at the same time they are not necessarily more "secure". These seals (active) still have problems especially with their power requirements and are useless without a power source. There is also confusion regarding whether electronics seals can be polled and interrogated when containers are stacked at a port or within a cargo hold.

5.2.1.5.) Standards

Currently there are no government standards for electronic seals. A standard is in the process of being developed and written by the International Organization for Standardization (ISO). In all likely hoods, this will become a pre-qualifier for all seal manufacturers interested in being a certified vendor.

5.2.1.6.) Access Control

Access control plays a critical role in any security implementation. Access control is a system combined of hardware and software that in its basic form replaces the key with an intelligent credential, usually in the form of a badge or plastic laminate card. This credential can be verified to the user through the use of biometric (Physical trait or characteristic) information such as hand geometry, facial recognition, Iris scans, Fingerprint and others.

Access control features can be extended through the use of software, As an example, Access Control can grant or deny access based on permissions and authorizations for access to a particular door, during a pre-determined schedule, while insuring that the person requesting access is a valid employee to work at that location.

Access control plays a critical role in securing not only the supply chain but also in securing access to any relevant facility. An access control implementation would provide not only increased security but also many other distinct advantages including control access, record movement, asset protection, universal credential and flexible security.

Access control use a system that combines hardware and software to grant or deny access to any area or facility based upon pre-determined criteria. The access control system focuses on the door as the primary element, this doesn't necessarily have to be a door, it could be a vault, shipping container, vehicle barrier, turnstile or any other hardware device designed to control an access point.

As mentioned earlier, the hardware and software have historically been coupled; meaning users were forced to buy a combined hardware/software system, all from the same manufacturer. This is similar to computing 15 years ago when a computer was a combined and proprietary hardware and software system. Recently companies have developed technology that allows the decoupling of hardware and software, this software is called Security Integration Software.

5.2.1.7.) Hardware and software

A variety of hardware is used to implement access control; it all starts at the door. Access control hardware can be categorized into three types:

- 1) Access control cards
- 2) Door hardware
- 3) Software

1.) Access control cards:

The access control card is the credential used for requesting access to the facility. Access control cards can be categorized as smart and dumb.

Smart Cards:

- Can be written to and read by a reader
- Must be inserted into a reader (Contact Smart Card)
- Can be read without inserting into a reader (Contact Less Smart Card)

Dumb Cards:

- Can only provide data
- Can emit a signal and can be read from a distance (Proximity Cards)
- Must be swiped through a reader (Swipe Cards)
- Cards that contain bar code information (Bar Code Cards)

2.) Door Hardware

Hardware located at the door.

Door Contact: A small switch at the door to determine if the door is open or closed

Request to Exit Device (REX): The REX is a motion detector that is used to determine if the door was opened from the inside or "Forced" open from the outside.

Card Reader: The card Reader is used to capture information from an access control card that is presented when someone requests access to a facility.

Locking hardware: This device type allows the system to lock, unlock or grant access (unlock for a pre-determined period-5 seconds). This hardware can be part of the door hardware, installed in the doorframe or attached to the door itself.

Field Panels or Controller: The field panel is the local intelligence for the doors, The field panel includes a small circuit board, processor, back up power supply and memory. The field panel is designed to run independent of the "Back End Software".

Access Control Work Station: The backend software is used to manage monitor, control and program multiple field panels. In most cases this software is installed on a workstation that is connected through a serial or network connection to the field panels.

3.) Software

There are essentially three types of software used in access control systems:

- Panel firmware
- Backend software
- Security integration software.

Panel Firmware: Firmware is the software that is installed on each field panel. This firmware is a small portion of the back end software that can control the doors attached to the field panel if communication is lost between the field panel and back end software. This firmware is usually running on an embedded processor in the field panel.

Back end Software: The back end software for access control is usually a client server application and database running on an access control workstation that is connected (either serial or TCP/IP) to field panels. This software is the user interface for the system, it controls all aspects of the panel including configuration of the field panels on how to respond if connection to the access control workstation is lost.

System Integration Software: Most systems in the security industry are closed and proprietary. Security Integration software is used to integrate similar systems from the same manufacturer as well as the other system types.

5.2.2.) Biometrics:

Biometrics can play a critical role in access control. Biometrics is the use of unique physical traits as a tool in the identification and verification of an individual. The use of biometrics can be broken down in two categories:

- Identification
- Authentication

Identification: Identification entails using Biometrics to identify a person independent of other means. Simply put, the biometric attribute (fingerprint as an example), is the only input to identify any individual. This process is somewhat less reliable and time consuming. Once the system captures a biometric value, it must then compare that value to set of values in a database and attempt to match the two values.

Authentication: Authentication is the use of biometrics as an escalation of security to verify that the person presenting the credential is the same person to whom the

credential is assigned. This process is proven and reliable, it compares a known biometric value of the person identified with the credential.

There are a variety of Biometric solutions available today. Some such fingerprint and hand geometry are proven and other such as facial recognition are currently being evaluated. Each implementation of access control may require a different type of Biometric.

The critical factor when designing an access control system with Biometrics is insuring you maintain the flexibility to add different biometric technologies to meet the unique needs of each implementation. Weather, moisture, temperature, egress speed and many other factors should also be considered.

5.2.3.) CCTV

Closed-circuit television (CCTV) has been a primary requirement for all new security applications. The reason is that its ability to remotely monitor and store video images creates incredible use and versatility for any multi agency organization leveraging CCTV as a resource that manages information, the government, and operating entities. Far-flung offices could also realize not only increased security but also improved operational efficiency.

CCTV could accomplish three objectives:

- ❑ Expedite inspection
- ❑ Increase the amount of cargo that is inspected
- ❑ Reduce the cost per inspection

Expedite cargo inspection: As an example, if CCTV systems were used to record the loading of a container, federal law enforcement and government officials could virtually inspect the container by having access to the archived video. This remote inspection could be accomplished while the cargo is in transit.

Increase the amount of cargo that is inspected: Cargo can be virtually inspected, thus increasing time spent on individual inspections. Today an inspection begins when the cargo reaches a port. By implementing CCTV Federal law enforcement could thereby manage the load by centralizing resources and spreading the inspection tasks among remote operators in a call center.

Reduce the cost per inspection: The process of centralizing resources for cargo inspection would reduce costs. The budgetary contrast of a cargo field inspector to an operator in a large inspection station is much less. Not only would the review process be accomplished faster, and the central inspector could easily move from container to container to accomplish more inspections than a field inspector.

Enhancements to CCTV components and systems now facilitate deployment of CCTV and expand how the technology can be utilized.

In addition to innovations, two recent technological trends have significant impact on the CCTV industry:

- Digital Video
- Network Deployed CCTV

Digital Video: Standard National Television Standards Committee (NTSC) video information can be converted to a digital format. Thus the video data can be managed with more versatility, essentially making traditional VCR obsolete.

Network Deployed CCTV: After the video data is converted to the digital format, the private or internal network can convey video and other types of security data.

CCTV is a critical component of every security system, and through the use of it, events can be observed in real time, or archived for review. A CCTV system illuminates an operation and allows an archival of image-based events that are deemed relevant.

5.2.4.) Container Sled: Cargo Transfer Apparatus and Method

This is a device and method to combat terrorism worldwide by offering a superior methodology in the handling of cargo carried in standard ISO containers.

The Container Sled creates automatic inspection of 100% of cargo container contents without impending port operations. The sled is a low (approximately 6 inches in height) platform whereupon any dry cargo can be securely loaded. It can easily be inserted into and extracted from a standard ISO container.

The sled method can be implemented without changing configurations of either ships or containers and no special equipment of any kind is required.

Container sled along with existing and proven technologies like AS/RS warehousing will solve container-repositioning problem, improve port land use and relieve port congestion.

5.2.5.) RFID

For those of us who are not technology savvy let us take a minute and understand what RFID is?

These devices typically incorporate a silicon chip and an oscillating circuit that can transmit a brief signal when interrogated by a reader. In simple terms, RFID is a form of automatic data collection technology like bar code, but it is electronic, it has the capacity to store more data even when network is not present, these tags can be made writable.

It is emerging as a viable alternative to bar codes for many enterprises, particularly those tracing large reusable assets or with environmental conditions that preclude the use of bar codes.

RFID systems can identify and trace people, assets and inventory.

5.2.5.1.) How does it work?

RFID uses Radio Frequency waves to transfer data between a reader and a movable item to identify, track or locate that item. RFID tags communicate by radio signals with RFID readers to form a wireless connection.

The signal of each tag is then monitored by a cellular system of readers that receive and relay the tag's location to a host computer. The location information is then displayed on a LAN or across the web. By continuously monitoring signals from the tags, Real Time Location Systems (RTLS) can identify item locations, providing managers with a real-time picture of supply chain movement and workflow.

With this system in place, Ford has been able to instantly locate specific vehicles to fulfill dealers' custom orders or to find any vehicle on hold for quality control. Moreover, should anyone try to remove a vehicle from the lot without proper authorization, the system can trigger an alert.

5.2.6.) Real Time Location Systems (RTLS) and cargo security?

Real-time location devices have a key advantage over forms of automatic identification — they keep tabs on items automatically even while sitting in a warehouse. The most commonly used type of automatic identification - bar codes - requires the act of scanning to determine location of an object.

Either the bar-coded item must pass by a reader on a conveyor, or an individual with a gun must press the trigger to take a reading. "You can gather data automatically with real-time location systems," says IDAT Consulting and Education's Moore. To date, though, companies have not had a pressing need to take note of the location of their inventory automatically. But one analyst thinks that government security regulations will

push companies into making the investment in this type of technology. "People are having a hard time justifying the expense of this technology," says Gerry McNerney, analyst with AMR Research in Boston. "The driver they are looking for is coming in the form of government regulation."

Because of concerns about terrorism, McNerney believes that the federal government may soon impose regulations requiring companies to engage in asset visibility and tracking. Companies will deploy real-time location systems to meet their legal requirements under these new security laws, which will mandate that companies exercise a high degree of control over shipments and products of interest to terrorists. Warehouses storing chemicals and other hazardous material products would become prime candidates for real-time location systems.

"Security will be the number one driver for this technology," says McNerney.

Regardless of whether security regulations propel interest in these systems, Meta Group's Klappich believes the technology should gain ground for marking high-value products over the next few years, especially in environments which occlude the lines of sight required for bar code reading.

"Costs are coming down," Klappich notes, "but it will be three to five years before we see this take off."

RFID clubbed with other technology like seals can provide a hybrid security system. The new electronic seals will combine EchoPoint, Savi's latest, sixth-generation, active radio frequency identification (RFID) technology, with OneSeal's design and manufacturing skills for high-security locks. The partners plan to introduce a widely affordable product by early next year that will dramatically improve the security and management of cargo containers moving throughout the global supply chain by ship, rail and truck. This low-cost electronic seal will be designed to seamlessly integrate with Savi's SmartChain real-time software platform and Transportation Security System software application.

The plastic-coated metal seal, which will include an active smart tag with an integrated circuit board and miniature RFID antenna, will be engineered for the security of all kinds of cargo containers moving an estimated \$12.5 trillion of merchandise traded worldwide. The initial products will target the approximately 200 million intermodal containers on oceangoing vessels that move 90 percent of world trade between seaports annually.

5.2.7.) Other Systems and Technologies

Acoustic: An ultrasonic transducer is put into contact with the container and scanned. A sensor then detects the resulting reflection from objects inside and forms and image of them. The technology is useful only in Liquid (tanker truck) environments.

Gamma ray: The use of an active (radioactive) element to produce gamma rays aimed at the object under inspection. The rays interact with the object that are detected and displayed as an image. Gamma ray systems are transmission only.

X-ray: The use of a source and appropriate beam forming to generate x-rays aimed at the object under inspection. The X-rays interact with the object, are detected and displayed as an image.

Radiation Detection: A detector measure the ionizing radiation or other characteristic radiation such as neutrons naturally emitted from a radioactive substance, Typically, the indication is an audible signal or a reading meter. This type of system us used to detect the presence of a nuclear device or other radiological threats.

Vapor Detection/Trace Detection: A "sniffer" type sensor collects air samples emanating from the container, and then analyzes the sample using a variety of spectrographic methods. Alternatively, a physical "wipe" collects particulate matter from the surface of the container, and this wipe is placed in a device and analyzed as above. The results are used to determine the molecular nature of the material within the container. This is particularly important for detection of presence of biological weapons.

5.2.8.) Tracking Technologies

The tracking technologies that are popularly used are:

5.2.8.1.) GPS/ Commercial Telematics - Global Positioning Systems

The Global Positioning System (GPS) consists of satellites transmitting their exact time and geographic information to GPS receivers worldwide, which in turn calculate their "real-time" position.

GPS equipped vehicles provide real-time information allowing routing analysis and visibility throughout the supply chain.

There are three types of GPS systems:

- Active
- Passive
- Hybrid (Active and Passive)

Active: Active GPS systems specialize in automatic location identification of the mobile asset/vehicle. At a preset time interval the mobile unit sends out its latitude and longitude as well as its speed and other technical information.

Passive: Passive GPS is an onboard computer within each vehicle logs the location and other information that the GPS receiver provides and uploads it to an office-based PC on the mobile assets return to base. This system does not require Internet access and typically allows for more in-depth information management and analysis.

Hybrid (Active and Passive): Hybrid GPS combines the best features of both active and passive management for companies that want the advanced management information available from passive solutions plus the ability to locate a vehicle instantly on a real time basis.

5.2.8.2.) Cellular based location services

Extensive coverage of cellular network has given opportunities for the rise of new tracking methodologies. These technologies basically leverage the existing networks and arrive at the location using the triangulation pinpoint methods.

Cell-ID: Cell-ID is the most basic location-based technology. The area covered by a cellular service provider is broken down into cells. A city is a network of these cells. At any given time when you are in the network area the subscriber belongs to or is attached to one cell. Using it, a mobile-network operator can determine a mobile-terminal users location by identifying the cell site (Antenna Location) from which the user is accessing the network.

Enhanced Observed Time Difference (E-OTD): E-OTD technology was pioneered by Cambridge Positioning Systems and now receives support from Nokia. It measures how long it takes radio waves from two different base stations to reach a users mobile terminal, and then locates that terminal using the triangulation pinpoint methods.

5.2.8.3.) Assisted Global Positioning System (A-GPS)

A-GPS is a popular location-based technology for uses on code division multiple access (CDMA) networks. It combines elements of the Global Positioning System (GPS) with wireless-network capabilities. As with GPS, A-GPS requires the mobile terminal to "see" the location satellites. However, a terminal cannot do so when inside a building or in some dense urban areas. In these cases, the solution has to use cell-site triangulation as the sole means of determining location.

5.2.8.3.) Other emerging technologies

Use of Digital TV frequencies to track mobile assets is a technology that are going to make tracking a commodity and at the same time available across the people. Each

system has its share of advantages and disadvantages ranging from cost to accuracy. Each system is suited for a particular type of tracking.

The choice of technology depends on the need of the organizations and physical factors come into play like the geographical area in consideration.

5.2.8.4.) Extending tracking information

In the section above, a basic understanding of the technologies has been provided but to really get the benefits of the technology you need to integrate this system with other systems, to provide real time alerts when the goods/mobile asset is not in the planned route/location.

Like in the case of a cargo theft it helps in recovery of the goods as the goods can be tracked at all times providing the enforcement agency with the required location information. Most of these solutions come with their own alert system so when the alert is pressed immediately the command center knows that there is a problem and knows the location the problem has occurred. To gain further benefits they can integrate them with external systems, such as the systems from the security agency the law enforcement agencies and providing them with real time information.

Extended tracking information can also facilitate and identify problem areas such as bottlenecks of the mobile assets or particular customers that hold up the schedule by not being ready for pick up. Slow and inefficient drivers can be identified and by placing sensors in appropriate spots, it is also possible to monitor temperature or fuel usage. Last but not the least tracking solutions helps keep an eye on the goods that are vital to the organization at all given times.

5.2.9.) Summary of technological solutions

We are still a long way from the ideal state of "Total Asset Visibility and Authentication" in the supply chain and logistics chain. And there are technologies that should be further tested and considered for implementation in the near term (less than one year), intermediate future (less than two years), and in the future. At the same time, significant impediments for implementation remain, which should also be addressed. They include cost, lack of standards, proprietary platforms, infrastructure, and national laws.

The ideal state of "Total Asset Visibility and Authentication" would integrate the necessary technologies and provide:

- Loading of shipments in a secure facility
- Access by authenticated personnel
- Verification of contents of the shipment
- Securing the container in transit

- ❑ Transmitting the content information and manifest information to customs and other stake holders upon loading
- ❑ Be able to identify container tampering
- ❑ Allow customs to verify the integrity of the container and its contents in a non-intrusive manner at point of entry.

We should continue to move towards this ideal state by resolving the impediments to implementation. Any implementation of technology will have the supporting infrastructure that includes laws, policies, procedures, standards, and international treaties to be effective. Technology by itself is not the answer.

6.) Concluding summary – and general recommendations

Moving forward, it's clear that companies must develop auditable security processes that comply with customs and government regulations currently under development.

The immediate focus for improved security must be taken into consideration. Find below some of the most important steps your company need to prepare yourself for.

- ❑ Investigate the physical security and integrity of plants, both within the enterprise and those of suppliers
- ❑ Find out background history of employees
- ❑ Security practices of logistics partners and carriers
- ❑ Shipment routes (i.e. countries of origin and interim stops)
- ❑ When shipping from one destination to another, always use pre-numbered security seals. Seals will indicate whether the cargo containers have been tampered with. Seals are effective safeguards only if you adhere to rigid seal procedures.
- ❑ After a theft has been committed, have it aggressively investigated rather than simply filing a police report or insurance claim. Too many firms take it on the chin, which has resulted in cargo thieves brazenly striking with little concern for the consequences.
- ❑ Develop an effective cargo theft reporting system
- ❑ Improve your understanding of the nature of transportation crime
- ❑ Build a transportation theft task force
- ❑ Increase law local enforcement expertise
- ❑ Introduce the latest and most effective security technologies
- ❑ Determine where you are today in terms of meeting security requirements and develop an action plan to close the gaps.
- ❑ Develop stronger relationships with government agencies, particularly US Customs, the FAA, and Department of Transportation.
- ❑ Take greater responsibility for ensuring compliance with both trade and security regulations, not only within your company but also across your supply chain.

-
- ❑ Establish closer, more collaborative relationships with suppliers, carriers, and other partners that are capable and willing to meet security requirements and phase out partners that fail to make progress.
 - ❑ Invest in technology that facilitates compliance, such as global logistics software (GLS) and "smart tags" that can monitor the status of a container.
 - ❑ Acquire better visibility of inventory and supply chain activities by implementing a Supply Chain Process Management (SCPM) solution or participating in a collaborative network.
 - ❑ Properly securing staged, loaded containers in storage yards is another important safeguard. Sophisticated video technology can now be interfaced with electronic alarm protection. When utilized strategically, this state-of-the-art equipment can provide an enhanced level of electronic protection and monitoring to those areas where high-value cargo is kept staged.
 - ❑ Place an undercover operative into a logistics operation has become a widely used technique because it is particularly effective at exposing internal theft and fraud.
 - ❑ Have unannounced audits by security professionals who will:
 - Evaluate the level of adherence to established security policies
 - Identify loopholes that could be exploited.
 - ❑ Establish an 800-tip line is another effective technique. There's a reason that the FBI and other organizations always post an 800 number after a major crime has been perpetrated. It is because a large percentage of these cases are successfully concluded only after receiving an anonymous tip. The same holds true in the private sector. Furthermore, a hotline that is effectively promoted and offers anonymity to caller's serves not only to bring serious problems to the surface but as an effective psychological deterrent.
 - ❑ While imperfect, GPS does have its deterrent capabilities. In states known for cargo theft (such as New York, California and Florida), global positioning satellite technology may help you quickly locate a container after it has disappeared. Newer versions of GPS even come equipped with concealed duress buttons so drivers can send out an immediate signal if they feel that a hijacking is imminent.
 - ❑ Lobby for strengthen laws and prosecution

6.1.) Adaptive Supply Chain Networks – is that the solution?

The Sep 11 event closed the ports down for 3 days causing a financial damage of a couple of billion dollars and theft claims a loss of \$40 billion US, to improve this the incorporation of cargo security measures is a must this would reduce the probability of cargo terrorism and place a check on cargo theft but organizations need to take one more step to make them immune to losses caused by incidents of this kind that is to make their supply networks "**adaptive**".

Manufacturers static and linear supply chains prevent them from quickly responding to supply chain net expectation – or seizing unexpected business opportunities. To make

adaptive supply networks a reality, manufacturers will create a technology-enabled cycle to help:

- ❑ Sense and interpret
- ❑ Decide and act upon notification
- ❑ Learn and transform

6.1.1.) Sense and interpret

To predict future risks and opportunities, manufacturers will identify, assemble and continually track directional indicators that measure operational performance – and alert partners when a major deviation is detected.

6.1.2.) Decide and act upon notification

Supply chain partners will decide which action plan is most appropriate under current conditions and then rally shared resources.

6.1.3.) Learn and transform

Partners will turn exceptions into insights into change altering their organizations underlying processes and objectives, and reshuffling their coping strategies portfolio to better handle similar situations.

6.1.3.) Supply chains must evolve into adaptive supply networks

Supply chains must evolve into adaptive supply networks, which is demand driven support decisions made on the fly based on actual conditions and reduces the response time for unforeseen events.

Existing supply chain applications don't help manufacturers sense or respond to changes in their operations network because they:

- ❑ Insulate static plans from dynamic execution reality
- ❑ Rely on centralized problem-solving frameworks
- ❑ Ignore the billions of physical supply chain devices

Supply chain applications need to grow in capability to support Adaptive Supply Networks.

Future Cargo Security Reports and Events

eyefortransport is at the moment running focused Cargo Security Events with representations from leading industry professionals, the next event is:

The eyefortransport cargo security forum, Brussels, May 2002

Please go to <http://www.eyefortransport.com/cargosecurity/> for more information or email Cal Foster on: cal@eyefortransport.com

eyefortransport is also producing a Cargo Security Report entitled “**Developing a Seamless Cargo Security Strategy - across the global logistics chain**”. If you are interested in buying this report please email your full contact details to cargosecurity@eyefortransport.com for more information, there is also a synopsis at the end of this report.

List of References

1. eyefortransport
<http://www.eyefortransport.com/>
2. US Customs
<http://www.customs.ustreas.gov/>
3. SupplyChainBrain
<http://www.supplychainbrain.com/>
4. SecurityVoice
<http://securityvoice.co.uk/>
5. National Cargo Security Council
<http://www.cargosecurity.com/ncsc/>
6. The Brookings Institution of Washington
<http://www.brookings.org/>
7. Federal Computer Week
<http://www.fcw.com/>

The information and opinions in this document were prepared by eyefortransport (“First Conferences Ltd.”) and its partners. eyefortransport makes every effort to use reliable, comprehensive information, but we make no representation that it is accurate or complete.

In no event whether in contract, tort (including negligence) or otherwise shall eyefortransport (First Conferences Ltd.) and its partners be liable for any damages, losses, expense, loss of data or profit caused by your use of the material or the contents of this report.

This information may not be sold or redistributed without the written consent of eyefortransport (First Conferences Ltd.).

Europe Cargo Security Forum 2003

June 16-18, 2003, Grand Hotel Mercure Royal Crown, Brussels

Strategies and technologies that will provide a secure cargo environment and still retain a fast, reliable and competitive supply chain

Conference * Exhibition * Workshops * Networking

The only event where you will find out the solutions to counter cargo theft and terrorist threats across the global logistics chain...

A unique opportunity to benchmark your cargo security initiatives and find out the answers to these burning questions...

- Which companies are implementing the best supply chain security programmes - how can you benefit from their experience?
- How can you dramatically reduce cargo crime by collaborating with your transportation partners?
- Which security technologies and initiatives will deliver fast ROI?
- How much will it cost you to ensure adequate security for your transportation chain?
- How can the trade community and government agencies collaborate to ensure an effective future security programme?
- What are the best strategies for effective risk profiling?

Please send me more information on the Europe Cargo Security Forum 2003

Name	
Company	
Job Title	
Email	
Telephone	
Street	
Town	
State	
Post code	
Country	

SPEAKERS INCLUDE

Transportation providers

- Lufthansa Cargo
- TNT Express
- KLM Cargo
- Danzas
- DHL
- Exel
- Rutges Cargo
- Hapag Lloyd Container Line

Shippers

- Boeing
- Lucent Technologies
- Microsoft

Government agencies

- European Commission Directorate General for Energy and Transport
- European Commission Taxations and Customs Union Directorate-General
- US Customs

As well as experts from

- FEPORT
- AMS Systems
- TT Club
- EUROWATCH
- Freight Transport Association
- QUALCOMM
- North River Consulting
- World Customs Organization

And more...

**For the most up to date information go to: www.eyefortransport.com/cargosecurity
Or contact Cal Foster directly on +44 20 7375 7520 or cal@eyefortransport.com**