THE EUROPEAN
FREIGHT AND
LOGISTICS
LEADERS FORUM
HO – BRUSSELS

SUPPLY CHAIN SECURITY

Working Group Report n°20

April 2007

THE EUROPEAN FREIGHT AND LOGISTICS LEADERS FORUM

SUPPLY CHAIN SECURITY

Results of the F&L Working Group chaired by Mr Miklós Horvath - MASPED (Hungary)
April 2007

Preamble

Terrorism affects us all, individually and collectively, no country or society is exempt from its threat. Therefore we share a common duty to tackle terrorism. Although the target of terrorist attacks have always been humans so far and there has been no evidence of plans against transported cargo up to now, nevertheless cargo security has become a more relevant issue among shippers and the whole logistic world.

The satisfactory operation of supply chains is about predictability and accuracy and this makes it vulnerable. The actors in the supply chain are focusing on shortening cycles and creating more complex supply chain structures. If in such a complex network between supplier and manufacturer or manufacturers and customers breaks down or is interrupted, it could have very vide ranging consequences even at the level of the world economy.
It is, therefore, well understood that supply chain security should be one of the key area of the logistic research and an important concern of all stakeholders in corporate manufacturing.

The main concern of manufacturers and retailers, particularly just-in-time operators, is the need to ensure continuity and reliability of supply. For carriers, it's largely a matter of preventing losses of their own assets and their customers' consignments – and avoiding the consequent claims. For governments, it's very much an issue of national security.

And by the way, for security consultants the whole business is a cash cow.

The members of the F&L are large companies who fully understand the importance of this issue but as practical operators of large number of logistic networks they also consider other aspects of the security systems. Speed or lead times and costs are also factors which are the key elements in the supply chain design process.

Today there are a large number of ongoing initiatives concentrating on supply chain security. The European Union has also played its part in the response to the terrorist threat. But shippers are not convinced of the possible advantages of security certification referred to in the draft regulation of the Commission, nor are they convinced of the effectiveness of the regulation in terms of security in the supply chain. This caused jitters among shippers who feared that it will slow the free movement of goods and hit global supply chains.

But new events on the EU level over the last couple of months have brightened security prospects for 2007. A number of controversial initiatives have been suspended; Commissioner Barrot and MEP Hennis Plasschaert agreed to put the Commission's proposal on enhancing supply chain security on hold. Furthermore, the UK Home Office announced that it will freeze its own unilateral security proposals on the basis that they no longer regard it feasible to collect data on a blanket or routine basis.

There is also controversial news from the US. Plans to increase ports and shipping security which would have involved the scanning of every sea container consigned to the US have been withdrawn after concerted lobbying by American business. An amendment to the Improving America's Security Act currently being considered by the Senate was defeated 58-38 due to opposition from Republicans and a number of Democrats. The amendment required that within five years 100 percent of containers from all ports should be scanned before arriving in the United States.

In fact, there are several issues left open for the future. For example it would be necessary to make the internet a hostile environment for terrorists and the EU should also continue promote higher airport security standards in third countries through its technical assistance program.

Should the terrorists target identified weak spots in our security and succeed in exploiting these causing the break down of some important supply chains related to crucial resources, then the regulatory initiatives around supply chain security would no doubt heat up and receive much higher priority.

The F&L Working Group started to work on the security subject already in late 2005. The participants realized that this topic is not clearly defined with various aspects and their interpretation changing with time. The ongoing intensive debate in different international bodies is producing a flood of new assertions and statements. New studies conducted by research organizations and business are published frequently.

Under these changing circumstances the WG had to adopt a stop-go approach to its work. Accordingly, this report has been revised after review.

Discussion

The global business environment today is characterized by greater vulnerability to business disruption and increased awareness of threats leading to new regulations demanding more attention to compliance. In this environment the ability to respond to change becomes an important factor in maintaining competitiveness. As a result, security is taking on a new significance, forcing companies to see investment in supply chain security as necessary. CEOs are not only concerned with creating shareholder value, but increasingly ask themselves the question : 'What can destroy our brand?' In a recent survey of the 800 companies who experienced a supply chain disruption reported in the media, the average drop in shareholder value wasp 25 per cent and they underperformed the market by 40 per cent for a full year.

Quoting one definition, "the term `supply chain' describes an overall process that results in goods being transported from the point of origin to their final destination and includes the movement of the goods in warehouses and transportation, the shipping data and the associated processes as well as a series of dynamic relationships."

Supply chain security is becoming one of the unavoidable issues in the real world of logistics. The impact of an increasingly politically violent world combined with sophisticated and organised crime has disproportionately affected the logistics sector. Terrorism, though, is just one of the security issues that businesses, the public and Governments face. While it represents the most poignant and perhaps dramatic threat, other traditional areas of concern are as significant for modern businesses. In parallel, natural disasters such as Hurricane Katrina, as well as many other unforeseen events such as product contamination and adulteration, shortages, border closings and strikes by ports, made firms more aware of the vulnerability of their supply chains, and encouraged them to seek ways to reduce risks of such unforeseeable situations and increase stability along their supply chain.

Companies with a global perspective are realizing more and more that the objective of physical and transportation security is more than just theft prevention; it's also about not becoming a channel for illegal activity. If cargo can be readily stolen from the supply chain, it will also be an easy target for

tampering or for introducing an unauthorized item into the supply chain-or for creating an artificial shipment under your name. Multinational companies must demonstrate that their security plans apply to all operating locations, which are subject to audits.

Government authorities require importers and other companies involved in global trading such as carriers and Logistics Service Providers (LSPs) to comply with some security regulations. Failure to comply with these regulations might result in imported goods not being allowed into the country.

But there are concerns that politics and emotion can sometimes dominate security regulatory processes, because mandatory or voluntary initiatives put a significant financial burden on companies, and many of them find it difficult to provide a business case to financially justify these investments.

On company level the risks faced by executives around the world are increasing in number and severity. The problems are all the greater when dealing with supply chains that are both more international and leaner. For companies, especially those that make extensive use of global sourcing, have to calculate with longer lead times and extended delays due to tighter security procedures for imported goods.

Therefore the question how to balance shipment speed with secure supply chain is a high priority for supply chain and logistic managements. Large and influential group of industry leaders are lobbying for security with the goal of ensuring the efficient flow of commerce. Actors alongside of the supply chain monitor both security and speed. All of the interconnecting points are critical nodes. The answers are more and more complex and varying. To achieve organizational resilience the companies could increase flexibility of their operations (e.g., by using interchangeable or generic parts, cross-training employees, postponing differentiating process steps to a later point in the production process, or diversifying their supplier base and portfolio of locations) and/or to make changes in corporate culture (e.g., encourage continuous communication among informed employees, and empower employees to take necessary actions in the face of unexpected events).

Governments could be facilitators by providing incentives to invest in security and, wherever possible, working to ensure that multinationals are not forced to comply with incompatible country-specific security requirements. But the difficulty is that currently there are multiple new supply chain security programs, standards and regulations on their way. Therefore global technology, equipment and best practices standards are urgently needed.

Some companies are skeptical about the introduction of new security regulations or programs. They argue that in a Europe where land based logistic services are the dominant modes of transportation, maintaining security has always been the traditional task of the major corporations with quite sophisticated security practices. Security standards have been incorporated in most large logistic contracts.

Nevertheless risk reduction even by self-regulation, requires significant levels of investment. Unfortunately, so far many organizations have found it difficult to provide a business case to justify security investments, and are, therefore, reluctant to invest in security beyond the minimum necessary. In our opinion, one of the main reasons for this reluctance is that companies have been focused largely on direct expenses related to security initiatives, and not on the collateral benefits that can be realized from such investments. There are various ways in which companies are able to realize their benefits coming out of a new security standards put in place. For corporations to prosper in our dangerous world, putting in place effective strategies to control risks has never been more crucial. Practicing risk management for corporations is the only healthy life style.

Terrorism versus crime

Europe has a long tradition in dealing with the more and more sophisticated methods of organized crime and European companies have well proven crime prevention systems related to logistics as well.

To be able to have a better understanding of this issue we have to examine the differences between terrorism and crime when creating a comprehensive security program that combines anti-theft techniques with anti-terrorism strategies

The definition "terrorist risks" should be understood widely. It covers the risks, where motive is

- Vandalism
- Politics
- Money or other economical motive
- Faith, ideology
- Commercial interests (competition)

Vandalism is often plain hooliganism, without an obvious or visible motive, but political or racial hatred is often in the background. The damages caused by vandalism may be anything from minor to very large.

Politics as a motive covers nationalistic and ethnic discontent as well as political motivation.

Money or other economical motive is often linked with other motives. The terrorist action may be used to finance illegal activities or action may be "outsourced" to professional criminals. In fact it is often difficult to define the motives when a terrorist group demands a ransom.

Faith and ideology covers not only religiously motivated terrorism but also other motives with fundamentalist features when values or way of life or devotion is threatened. Again here the category is not clear, sectarian divisions may be along wealth lines.

Commercial interests linked with competition may also be a motive

As we are focusing on terrorist threats here, we are not analyzing criminality as a security risk. It should, however, be noted that we face the most dangerous form of terrorist threat when terrorists ally themselves with organized crime.

According to the U.S. Census Bureau's Foreign Trade Statistics, China exported $38.5 billion worth of high-tech goods to the United States in the first 11 months of 2004, while the European Union exported $9.6 billion, Japan $13.6 billion and Malaysia $16 billion. While cargo theft is a global problem pegged at more than $50 billion annually by the US International Maritime Bureau-high tech being one of the hardest-hit industries, a sustained terrorist threat is seen as potentially far more devastating.

But what if, instead of being hijacked for gains, those stolen goods had been somehow transformed, like computer viruses, into weapons of mass destruction-aimed at sectors that rely on efficient operation of electronic equipment-and reintroduced into the supply chain? That's the new threat.

On the interrelationship between cargo-crime and anti-terrorism, many companies believe the two issues are "very complimentary." Apparently many companies are treating the two issues as essentially

separate. Though corporate security departments are most often responsible for loss prevention and cargo-crime, corporate responsibility for the new anti-terrorism security has not always fallen there. In some companies, corporate security already oversees these. In other companies, the programs fall under the transportation or logistics department. Still other companies assign the responsibilities to different areas, perhaps divided between regulatory compliance or counsel, supply chain or procurement, or even human resources.

The challenge to industry is the harmonization of corporate anti-terrorism initiatives that have emerged since 9-11 with the cargo-crime initiatives that corporate security departments have perfected for decades.

Based on a recent survey a few companies (15%) believe that cargo-crime is decreasing either "slightly" or "greatly" for their company. More than half (53%) believe it is staying stable, while 33% believe it is increasing "slightly" or "greatly."
In terms of value the greatest losses in last year have been sustained in mobile phones, non-electronic goods and cash/bullion, in that order.

In the fight against organized crime we have already have some success stories in Europe. We should make a special mention of the recent well publicized successes sustained by the UK based Operation GRAFTON team. Apart from their own dedicated efforts associated with Heathrow they have played a key role in a multi-team effort in carrying out a large and well coordinated swoop on a number of locations around London resulting in the arrest of many high profile criminals. The result demonstrating very clearly what can be achieved by a well organized cooperative effort between Government, LEA's and industry.

This effort is interesting to mention because still UK continues as the primary source of concern in Europe, with 60% of the criminal reports received by the TAPA, the well established worldwide security organization.

Arguments in favour of security initiatives at company level

The new fear is that if customers or suppliers are uncomfortable about doing business with a company because of security concerns, they are likely to take their business elsewhere. To maintain a level of trust, companies will need to extend security initiatives deep into the supply chain. That means encouraging their partners and customers to do as they do, and adopt the latest security measures. These cannot be limited to single measures, but a combination of the best supply chain practices, logistics systems, data capture and communications tools, and security-enhancing technologies available. Let's consider some of them.

Security Initiatives of the Manufacturers

Manufacturers could have different motives for implementing supply chain security measures. Some companies implemented security initiatives just to strengthen the security of their supply chains. For example, companies that operate in the high-tech industry often times manufacture goods characterized by a small size and high value. Such goods are a likely target for theft, and so it has traditionally been essential for these companies to secure the goods to prevent theft and consequent sale in the black market, as well as to prevent diversion of products to the gray market.
Other frequent targets of theft are fast-moving consumer goods manufacturers. These companies have had in place for many years various physical site security mechanisms, such as fencing, ID badges, access limitations, etc.

For different reasons, chemicals companies—especially those that deal with hazardous and flammable materials, also invest heavily in physical site security, personnel security, as well as cargo and transportation equipment security controls.
Shippers have realized that as a byproduct the security of their supply chain could have been improved as well. More sophisticated tendering processes, more careful carriers selection and the necessary implementation of a track and trace tool, providing them with more visibility about their goods while in transport.
While the motivation for putting this measures in place was to gain such benefits as reduced inventories, improved on-time deliveries and fewer incidents of stockouts, as a byproduct, the track and trace capabilities also improved the security of their supply chain.

In addition, many companies decided in the last few years to take voluntary steps to enhance security within the four walls of their organizations. One of the necessary area of dealing with should be the deployment of a Risk Assessment tool to quantify and address unacceptable risks in the supply chain, as well as an Expected Loss forecast tool that analyzes historic losses and predicts future losses, so as to help the company to set realistic goals to mitigate risk.

To minimize disruptions along the supply chain, in addition to security initiatives taken within the four walls of the organizations, companies have also been working with their business partners to improve the security of their operations. Shippers started to set up security standards for their logistics service providers as well. They now place more explicit security related requirements on them, and list those requirements in detail in their contracts. For example some shippers have adopted the TAPA freight security requirements as minimum security standards in their logistic contracts or require TAPA membership from them.

Benefits gained form an improved security

There are various ways in which companies are able to realize their benefits coming out of a new security standards put in place. Shippers can receive information in advance about some of the raw material arriving at their production facilities. This information allows them a better controlling of their ordering and receiving processes and to improve their inventory management.

Many shippers have already established security systems for many and these can see very few collateral benefits following the adoption in recent years of government regulations or voluntary initiatives but still there are other benefits which we propose to be considered:

1. Internal inventory management - in the receiving process of incoming material could bring a reduction in incorrect quantity received.

   - Product safety - better security practices allowed the companies to be more successful in protecting their products and could result in a reduction in theft, tempering and damage of their products.

   - Customer service - service level to customers could be also improved in a number of ways more careful selection of logistic service provider will bring improved on-time deliveries.

   - Cost savings - the above mentioned impact as improved inventory management could bring in theory some cost savings but it would be difficult to quantify those benefits

Generally speaking putting more emphasis on the supply chain could lead to a decrease in

- the number of back-orders;
- the frequency of cancelled orders; and
- the defective products delivered.

Several shippers who had experienced hijacking of high-value products, which were later sold in the black market forced their logistics service providers to invest in security, such as the use of Global Positioning System (GPS) and started the joint evaluation of Radio Frequency Identification (RFID). Other requirements are the use of locks and high-security bolt seals on containers, driver background checks, use of driver teams rather than a single driver and use of two-way cellular/satellite communications.
These investments have been extremely successful, resulting in major reduction of theft.

2. Visibility or improved supply chain visibility -following their investments in supply chain security, companies will be able to improve their visibility to the location and condition of their goods as they move along the supply chain. In particular, the following benefits should be mentioned:

    - Access to supply chain related data
    - Timelines of data
    - Data accuracy

    Improved supply chain visibility will generate higher Efficiency in the chain as

    - improved product handling
    - process improvements

Although a major benefits shippers with global business model could realize as a result of their C-TPAT certification the fewer and less intrusive inspections at the ports, which also provided less opportunity for damage to the imported goods.

Security Initiatives of the Logistic Service Providers

Because of their involvement in the global trade nearly all of the ocean carriers port operators, container freight managers had advanced security measures in place for many years. For other European service providers who are only involved in land based logistics security were more an issue dealing with theft and other crime events. For both of them the security measures helped them to keep track of and protect their clients' products as they moved through their system, which is a necessity for service providers in this industry.

In conclusion we can say that service providers will not be able to comply with the new regulatory requirements unless they invest in IT systems and change their working procedures.

In addition to other security initiatives LSPs and ocean carriers decided to take part in voluntary programs like C-TPAT or TAPA. However we can see that at least some of the companies adopted such security measures more as a "business imperative" rather than purely to enhance security.
Shippers have also started to check whether their LPs are regulated or not and security often times been a prerequisite for participation in new bids.

Apart from external triggers, all participating LSPs and ocean carriers began voluntary initiatives to improve, or better control supply chain security. One area in which all companies invested in recent years is human resources. Some of the examples provided by the participating companies include an assignment of security officers to all ships and terminals, posting of additional security guards at warehouses, assignment of two drivers rather than one to high-value transportation lanes and an overall increase of security personnel. In addition, companies developed special training programs; some for all employees while others were tailored for specific job functions (such as security officers, drivers, or marine terminal employees).

Collateral benefits of the improved security

There could be a number of improvements in this area, mainly ones that are related to keeping the goods safe and free of damage. Even though most companies could not specify any cost savings attributed directly to these improvements, nevertheless it should be clear that given their liability for any losses while the goods are in transport, these measures can potentially have a positive impact on related costs.

Below is a list of the improvements LPs could realized by the participating in any security program.

- Excess to business: In recent years, as customers—especially the larger ones—became more aware of the importance of having appropriate security measures in place, they started asking their LSPs about security and/or required them to meet C-TPAT security criteria. Now new items have been included in their Request for Quotes (RFQs) specific questions related to security.
  Therefore, it has become essential for LSPs to have various security measures in place, and in particular be C-TPAT certified, in order to retain their current customer base and acquire new customers.

- Product safety: Product safety is a serious concern for LSPs because on many occasions they are held liable for damages or losses that occur while the goods are in their responsibility. Improved security will deliver reductions in tampering in theft/loss/pilferage in fraud in damages and also in defective products delivered.

- Customer service: KPIs are already a common part of the logistic contracts and any improvement in this area is in the interest of the LP. As a result of improving compliance programs and information flow to customs and due to heavy investment in IT systems will always bring increase in reported on-time delivery and better KPI figures.

- Customer Relationship: Improved customer relationship seems to be one of the more significant benefit areas, an improvement in the relationship with their customers following their investments in security measures.

There are other areas where the LPs could gain some internal advantages which generally could deliver better market acceptance and improve the company related figures as well. There are:

- Increase in customer confidence and increase in customer satisfaction.
- Companies also experienced an increase in the number of e-mail exchanges with customers and in the number of face-to-face meetings with customers or other joint customer activities

- As the 24-hour rule mandates have been introduced companies provide cargo information prior to loading on ocean vessels. This information cold help the LSPs to plan for more efficient loading, better management of space and also cross docking—all of which could reduce the cargo handling as general

A new study from the Stanford University quantifies for the first time the significant businesses value of global supply chain security investments, confirming a broad range of benefits that can have a positive impact on a company's bottom line.

Among the study's major findings, the companies collectively:

- Reduced their Customs inspections by 48 percent;
- Increased the automated handling of their imports by 43 percent;
- Saw a 29 percent reduction in transit times;
- Improved their asset visibility in the supply chain by 50 percent;
- Improved on-time shipping to customers by 30 percent;
- Reduced time taken to identify problems by 21 percent;
- Reduced theft in inventory management by 38 percent;
- Reduced excess inventory by 14 percent; and
- Reduced customer attrition by 26 percent.

Risk management (What it is? Why we need it?)

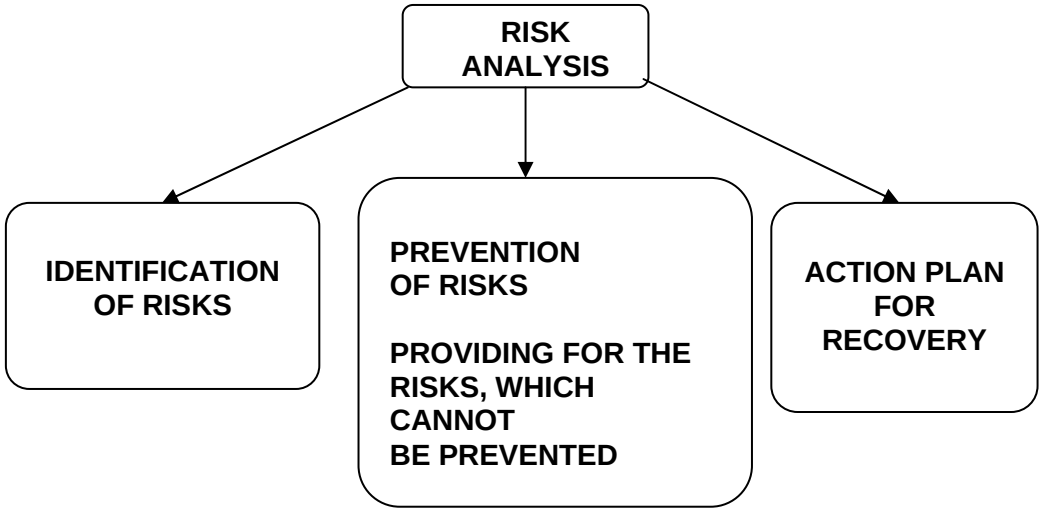
For corporations to prosper in our dangerous world, putting in place effective strategies to control risks has never been more crucial. Risk management is like a health check. It is a process used to manage the response and recovery from critical incidents or business interruptions that cannot be adequately handled within the normal scope of business operations.

(For example according to recent surveys: approximately 50%of business that experience a fire or critical incident go out of business within two years and 44%of companies that lose records in a disaster never resume business.)

Every organization should carry out a risk analysis as a part of its risk management. It is a method to identify existing or potential risks and it is also a method to evaluate the readiness of the organization to face these risks.

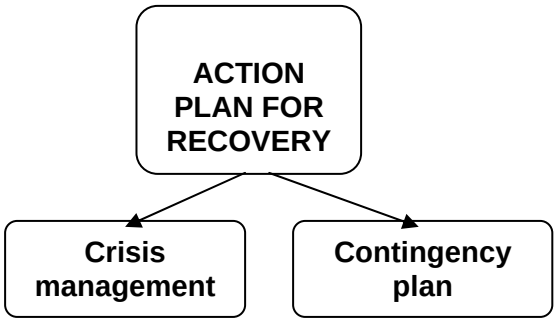
Risk analysis consists of the following elements:

- Risk identification
- Risk prevention,
  - For risks which have been identified and which can be prevented
- Minimizing consequences
  - For risks which cannot be prevented or which were not identified



The results of a properly conducted risk analysis are two specific plans, by which the organization is prepared to tackle risks. These are a crisis management plan and a contingency plan. Both of them are action plans, which are dormant but ready for use as soon as needed. Every organization should have a crisis management plan and a contingency plan. These must be kept up-to-date.

The risk analysis can and it should be conducted on various organizational levels. It may cover whole organization, parts of it, all functions or some of them. Risk analysis should be carried out by the organization itself, with assistance of external experts or persons from other branches of the organization.
As a part of risk management an organization needs an after-disaster action plan. It consists of two plans; crisis management and contingency plan.



Crisis management plan looks backwards. Its purpose is to minimize the losses and to see to after-care. Crisis management plan consists of

- alarm system
- mobilization of contingency plan
- after-care
- minimizing losses

- recovery actions against the party who caused the loss
- analyzing
- learning
- actions to be taken

Alarm system is inter-organizational system to reach the key persons. Mobilization of contingency plan tells how contingency plan comes into operation. After-care refers to actions to be taken after the risk has become materialized. Minimizing losses covers actions to taken to prevent further losses. Recovery actions against the party who caused the loss ease, if successful, the financial loss. Analyzing the loss leads to learning and actions to be taken to prevent similar loss in future,

Contingency plan is forward-looking document. It includes the processes and resources for a recovery and continuation of business as close to usual as possible. Contingency plan consists of

- action plan
- organization; permanent organization and ad hoc-organization
- costs, both external and internal
- resources, external and internal
- pre-loss operations
- post-loss operations
- information

Generally a risk management plan can cover all in details the following areas:

Facility management

- Facility protection and monitoring
- Access control
- Facility layout
- Inventory management

Cargo management

- Prevention, detection and reporting of anomalies
- Inventory control
- Inspection solutions
- Tracking solutions
- Anti-tempering solutions

Human resources management

- Personal background checks
- Training
- Organizational and job specification
- Security marketing

Information and Communication management

- Protection of business information
- Data exchange solutions
- International standards for data protection

Business network and company management systems

- In-house security management

- Business partner evaluation
- Collaboration with authorities

Crisis management and disaster recovery

- Business continuity plans
- Formal security strategies
- Emergency control centers
- Incident management

Risk Management is an on-going & shared throughout the Supply Chain
Companies don't have to invest a lot of money to carry out their risk analysis and to set up related plans and training activities. The key message is that in near term don't obsess about perfection and zero-tolerance, do what you can and keep improving. Focus on what your real vulnerabilities are and have in place a safety and preparedness plan for all hazards. With this approach you don't have to invest a lot of money. Response and recovery is as important as deterrent defense.

Searching every piece of the cargo is unrealistic Multinational collaboration lays on trustworthiness beginning at the factory were goads are loaded trough the transport companies caring the cargo in and out of the ports, custom officials and warehouse workers as well.

It is essential that we should pay more attention to contracts and agreements. They should clearly define mutual obligations. Contracts with clear and understandable language based on standard terms relating to the security related obligations of both parties would be desirable.

International initiatives

When it comes to supply chains that begin in one country and end in another, the issue becomes complicated. It would be so much easier if there were global industry standards. But different countries have different business practices, different customs requirements, and different government regulations – which change constantly as policy makers are obliged to update the rules to keep pace with increasingly innovative criminals.

Collaboration here is the key. On a domestic level, shippers, carriers, ports, etc. can all work together and push industry standards and best practices; on an international level, governments can co-operate with each other to aim for a set of homogeneous security directives; and multi-national companies can take the lead and set superior standards for international cargo security.

Because usually an extraordinary number of participants are alongside the supply chains therefore global standards would be urgently needed regarding to technology, equipments and best practices.

The difficulty is that there are multiple new supply chain security programs, standards and regulations are on their way:

1. Global /voluntary
   - ISO 28000/1/3/4
   - WCO SAFE
   - TAPA, ASIS..
2. Global and mandatory
   - ICAO
   - IMO/ISPS
   - Dangerous goods´…

3. North America /voluntary
    - C-TPAT
    - CSI
    - Known shipper
    - PIP (CA)…
4. EU /voluntary
    - StairSec (SE)
    - Known consignor
    - Secure operator
    - EU AEO…
5. Latin America /voluntary
    - BASC…
6. Asia Pacific
    - Accredited client (AU)
    - Secure export partnership, NZ STAR

To achieve some clarification in this regulatory jungle we have to make differences between Standards Regulations. Standards are consensual and voluntary. But standards can take on the force of law. It could be:

- Self-imposed (for example, ISMA)
- Client-imposed (Wal-Mart and RFID)
- Government-imposed (CBP and 17712?)

The response of national authorities to security challenge has meant that companies face a barrage of different of regulations in dealing with security. In the US, '9/11' resulted in a dramatically more stringent customs environment, typified by the C-TPAT regulations. In parallel both shippers and logistics service providers have had to face increasingly onerous customs checks for problems such as narcotics smuggling and illegal immigration.

When it comes to supply chains that begin in one country and end in another, the issue becomes more complex. It is even so if supply chains are bridging continents.

Most of the new initiatives taken by the U.S. government to assess and minimize the risk involved in international transportation of goods have been related to overseas container traffic.
Therefore it is worthwhile to handle this area in more detail:

How typical risks to containers could be identified

A very high potential safety risk in the supply chain is the container and everything in relation to the container. The containers are passing through several places in the chain, creating a potential risk at each and every place. It is ideal to interfere somewhere in the Supply Chain, manipulate people and use as a base for terrorist attacks elsewhere. Containers also could be seen as a very high potential risk, to be used by organisations in connection to build up a platform for terrorist attacks by well organised terrorist organisations. The major risks are placing of material in containers for use in terrorist attacks or smuggling people into a country or facility for further attacks in that country or facility.

How typical risks at ports are identified

One high potential risk is the port, to be used for transporting and smuggling people and equipment for future terrorist attacks.
The major risk is unwanted organisations operating inside any port and interfering with people in the port in order to be able to enter ships or containers. By entering ships and containers, people and material can be moved to strategic places for a future terrorist attack.
The port is also a place with a lot of people and cargo moving around.
One major risk, starting to be considered during the implementation of the ISPS code, is the entry to port/ships via the waterway.

How to prevent the risks at containers

In relation to 9/11[h], several initiatives have been introduced, mainly pushed by the US to limit risks of future similar attacks.
Two major factors, improving the safety of containers were in the implementation of the ISPS code (International Ship and Port facility Security code) and C-TPAT (Customs-Trade Partnership Against Terrorism). C-TPAT is focusing on the trade into or out from US. One part of these codes is the container seal policy.
By establishing standards of High Security Seals, the total view and safety awareness among shippers and receivers have increased. Today almost nobody is discussing the necessity of high security seals. Several companies are also looking at further development of seals and especially around electronic seals and possibilities to read real time information about the seal and also inside the container: today you can have electronic tags installed; reading every movement of the container and cargo online. Both shippers and service providers s can also have all details about the condition of the cargo and any unwanted incident en-route to final receiver. All this information is transferred online via satellite.

How to prevent the risks in the ports

Several initiatives have been introduced after 9/11, mainly pushed by the US authorities.
The major initiatives are the ISPS (International Ship and Port facility Security) code and C-TPAT (Customs-Trade Partnership Against Terrorism). The latter mainly focusing on US import and Export.
The ISPS code was implemented to:

- gather, assess & exchange security related data with appropriate Contracting Governments
- maintain communication protocols for ships and port facilities
- prevent unauthorized access to port facilities and their restricted areas, as well as introduction of unauthorized weapons, incendiary devices or explosives
- system to raise the alarm in reaction to security threats or security incidents
- require port facility security plans based upon port facility security assessments
- conducting training and drills/exercises

The C-TPAT is focussing on securing and authorizing all steps in the Supply Chain involving the exporter to US, importer into US, Brokers, Forwarders, and Carriers etc.
In terms of ports, the ISPS code is the major factor for increased security awareness and controls. Today all ports having international traffic, needs to be certified according to the ISPS code.
All ports have gone through a program in order to minimize risk of any unwanted activity in the ports, leading to an attack elsewhere. The standard of safety is controlled by the customs authority in each country. Each port has been assessed according to the protocol of the ISPS code. The controlling body has issued recommendations and have also pinpointed the potential weaknesses of the assessed port. The report contains timelines to fulfil in order to reach or maintain the status of an approved port. The next step will be when all ports shall be re-assessed and how to handle all comments raised during the implementation of the ISPS code. Will all ports keep to the safety standard and have all points raised during the first assessment been implemented.

The main focus in the ports are increased usage of fences, avoiding processes with too much involvement of individuals to minimize the risk of manipulation of the system, together with systems to control ships entering a port in a better way. The latter mainly involves ships not having an "International Ship Security Certificate". This certificate is mandatory when entering a US port. Each port needs to have patrolling guards to avoid entry via the seas as well as checking the fence regularly to avoid entry via land.

Finally the ISPS code became extremely important to ports as a non-approved port will not be allowed to have any international traffic.

We have to mention here also the Advanced Manifest Rule (AMR)/Advance Cargo Information (ACI), instituted by U.S. CBP in conjunction with the Trade Act of 2002, and fully implemented in 99 percent of the ports by January 2005. It requires detailed cargo data for all modes to be submitted to U.S. CBP prior to arrival. An ocean container is allowed into the United States only if detailed contents information has been provided electronically to Customs at least 24 hours before the container is loaded on the ship at the foreign port of origin. The information is useful for pre-screening questionable containers prior to arrival to U.S. ports and for selecting containers for inspection at ports of departure and entry.

Multiple security initiatives are also taking place outside the U.S. One of them is the publication in 2005 of the ISO/PAS 28000:2005 standard, a "Specification for security management systems for the supply chain" by the ISO.

The World Customs Organization (WCO), WCO members have developed the Framework of Standards to Secure and Facilitate Global Trade (SAFE Framework), which outlines a strategy that aims to secure the movement of global trade in a way that does not impede but rather facilitates the movement of that trade. By June 2006, a total of 135 countries have expressed their intention to implement the WCO SAFE Framework, including 25 member states in the European Union (E.U.)
As part of this initiative, the European Commission presented a series of measures to accelerate implementation of the WCO SAFE Framework security related provisions, including the Authorized Economic Operator (AEO) program.
The commission published a Communication and a proposed regulation on supply chain security on 27 February 2006. The objective of the proposal is to provide better protection for freight transport, through a voluntary "secure operator" accreditation scheme. The supply chain security proposal is closely connected to the Community Customs regulations whose development and implementation are being managed by DG TAXUD. The objective of the proposal is to provide better protection against attack for freight transport, through a voluntary "secure operator" accreditation scheme in each Member State.
This scheme would include all links in the supply chain: the preparation and
dispatch of goods at the point of origin, freight forwarding, goods transport as well as the operation of transfer and warehouse facilities and inland terminals.
Unfortunately, the proposal to improve supply chain security raises a number of significant practical concerns. The proposal would, in its present form, be a constraint on the transportation process and lead to cost increase for the economy as a whole, which is not compensated for by extra security.
At the same time the Commission is working on proposals for the protection of European critical infrastructure, covering all sectors. A program was envisaged in the DG JLS Green Paper in November 2005. The aim of this initiative is to identify European critical infrastructure, and establish Europe-wide preventative measures and procedures for the prompt restoration of normal working in the event of a serious incident (terrorist attack, natural forces).
In addition to these government initiatives, businesses have also proactively been seeking ways to mitigate supply chain risks. Another way that companies have thought to improve their freight security is through the establishment of the Technology Asset Protection Association (TAPA), which was

founded in the United States in 1997 and now has chapters in Europe and the Asia Pacific. TAPA was formed by several high-technology companies that sought to establish consistent Freight Security Requirements (FSRs) that could be implemented across the industry. Today, TAPA also provides its members a common, centrally located and continually updated pool of information related to criminal activities.

Costs and Benefits - Who Pays for Supply Chain Security?

It might be that in the US this debate began already a few hours after the 9/11 attacks but there is no end in sight to the debate affecting global trade and the logistics world. Many questions have emerged and remain to be answered :

- Where does primary responsibility lie for cargo security costs?
- Should the government foot the entire bill?
- Should the costs be passed on to consumers, or should a target tax plan be installed on trade entities?
- Should trade sectors be risk-assessed and charged fees in accordance with risk?
- Or should a combination of some or all of the above be constructed, legally and commercially?

As a general rule, it can be concluded that the financing of transport security measures which are imposed by law and which are connected with the exercise of powers which are typically those of a public authority do not constitute economic activities.
A recent US survey asked separate questions regarding who respondents believe should be responsible for the costs. One question focused on anti-terrorism efforts, the other on cargo-crime. Each question asked respondents to weight the responsibility for each of four entities: shippers, consignees, transportation providers, and government.
There was a difference in response to the questions. To combat anti-terrorism, the answers focused heavily on: a) the shipper, and b) government entities. To combat cargo crime, the answers spread responsibility fairly evenly throughout the supply chain and government, with a higher responsibility on transportation providers.

The European approach to this issue is quite different from the US one. In the US government are willing to cover a big part of these cost but in Europe all EU initiatives are based on the principle the whole business community have to cover the entire bill. On national government level the enforcement of the different regulations seems to remain as a necessity.
Considering that most of the European trade is serviced by land based logistics, clearly this involves less security cost than any transatlantic cargo. On the other hand, given the massive Asian presence in the global trade of our century the total security cost for the products could be enormous.

Within the EU to the involvement of Member States in the funding of the implementation of security measures, reflecting the different philosophies Member States may have on the role of the State in this matter. The heterogeneity of approach and the lack of transparency in generating revenue that is wholly for the implementation of security measures means that there is a possibility of some distortion of competition. This is particularly relevant in cases where Member States require additional, more stringent measures than those imposed by Community legislation.
However, distortions may also arise on a global level due to different approaches towards the funding of security measures around the world. This issue needs to be addressed, so as not to disadvantage the Community's transport industry in comparison with its competitors from outside the European Union, with its consequential negative effect on EU economic growth.

Figures related to security are available but are also very controversial.

A private-sector analysis conducted by the International Monetary Fund (IMF) estimates the increase to business costs due to higher security costs at $1.6 billion per year, the extra financing burden of carrying 10 percent higher inventories at $7.5 billion per year 29. Another study estimates an increase in commercial insurance premiums of 20 percent at about $30 billion per year30. New security measures following 9/11 are estimated to cost the U.S. economy alone more than $150 billion, of which $65 billion is for changes in supply chains. Based on an other US survey participants reported that most cargo security budgets, for both crime and anti-terrorism, are below 1% of the company revenues (57%) with 37% reporting budgets between 1% and 5%, and a few (76%) reporting over 5% of company revenue. These percentages translate into, in most cases, less than $100,000 USD annually (56%), with 24% between $100,000 and 500,000, and 15% in upper ranges, between $500,000 and $5 million.
It has been estimated in Europe that the cost of implementing the security measures could be 130.000 EUR per year for SMEs.

It might be expected that a new security regime merely will necessarily increase logistics costs, however there are new reports put together by academics or research people which, suggests that these systems are actually improving aspects of shippers and LSPs' operations. There are also other voices like that our industry had to commit its time and resources to protecting the world from terrorism.

The cost of these new measures need not be to sacrifice time of movement and to create cost burdens on shippers and consumers that they cannot afford. Every change in commercial operations has its consequences, often at a very basic and technical level.

The report asserts that the superior controls that greater security systems demand result in more, not less, effective supply chains. Those companies with strong supply chain security systems reported improvements in inventory management, product safety and customer service. These efficiencies resulted in double-digit savings.

Several types of costs relating to transport security can be identified:

- Costs of administrating security rules, including compliance monitoring
- Costs resulting from applying legislation
  - Fixed costs, such as capital investment in security equipment, and selection and initial training of security staff;
  - Operating costs, such as maintenance of security equipment (including technology upgrades), the wages of security staff, recurrent training costs;
  - Exceptional costs, such as those of additional temporary measures to raise security levels during periods of higher risk.
- Costs resulting from terrorist attacks

These costs are only partially related to transport and can include the cost of repairing damage to the target itself, ancillary costs resulting from the disruption caused by the attack and damage claims of victims, both direct and indirect. Indeed, even in the case that the transport medium (e.g. aircraft, ship, train) is the object of a terrorist attacks and is not used as a weapon; the damage may go by far beyond the transport sector. It is difficult to estimate the scale of such costs, but it is quite possible that they may be of such an extent that no single transport operator could be in a position to finance them. Also, the cost of damage may go significantly beyond what insurance may be able to cover at a

reasonable price. In addition, depending on its nature, the consequences of a terrorist attack may extend beyond the territory of a single Member State and may be of such a scale that even the Member State where the terrorist attack has taken place cannot bear the costs.

Summary and Conclusions

- Specific links in supply chain are more secure, but the supply chain system is NOT secure
- There is no magic bullet, multiple measures are needed
- "Soft" measures relating to information flows, personnel need more attention
- Policy makers have not given event response and recovery measures much attention
- Analysis of policies should estimate effects of policy measures on performance of supply chains (efficiency, reliability, transparency, fault tolerance, resilience)
- Security and efficiency are linked but distinct – increasing fault tolerance and resilience will require creating redundancies and slack
- Supply chain security must be balanced with the free movement of goods
- Companies have been focused largely on direct expenses related to security initiatives, and not on the collateral benefits that can be realized from such investments

The goals of this study were to demonstrate that investments in supply chain security can improve organizations' business performance and whenever possible to quantify those improvements. We have focused on collateral benefits of security investments to manufacturers and LSPs/ocean carriers.

Supply chain security can help organizations to improve internal operations, strengthen relationships with their customers, and overall increase their profitability. Therefore, such investments in security should not be considered just as a financial burden that should be kept to the minimum level necessary, but rather as an opportunity for improving business performance and profitability. We therefore recommend to companies that are seeking ways to determine a business case for their security investments to focus on these benefit areas identified, as it is likely that their organizations may be able to experience similar types of benefits.

Attachment 1

F&L Securing the Supply Chain, Best Practices.

1. Facilities.

a) Are buildings constructed of materials resistant to unlawful entry and intrusion?

b) Are outside and inside facility doors, windows, gates and fences adequately locked?

c) Are international, domestic, high value and dangerous cargoes marked and segregated in distinct, secured areas within the warehouse?

d) Is each facility adequately lit, inside and outside including parking areas?

e) Is private vehicle parking kept separate from shipping, loading dock and cargo areas?

f) Are gates under surveillance by security / management personnel?

g) Are alarm and communication systems in place to alert internal security or local police?

2. Access.

a) Is access to shipping, loading dock and cargo areas restricted by clear, enforced procedures (identification, logging and tracking of all employees, visitors and vendors)?

b) Are procedures in place for challenging unauthorized / unidentified persons, including requirement to search them?

c) Are vehicles, containers and other conveyances routinely moving into, out of and within accessible areas regularly checked for unauthorized personnel, materials or signs of tampering, with procedures for reporting irregularities?

d) Are vessels, aircraft and rail cars secured from unauthorized boarding, with accessible alarm systems and procedures in place for alerting internal or external security personnel?

3. Procedures.

a) Does a designated security officer supervise introduction / removal of all cargo?

b) Is inventory fully and properly marked, weighed, counted and documented and then verified?

c) Are procedures in place for affixing, replacing, recording, tracking and verifying seals on containers, trailer and rail cars throughout the move?

d) Are procedures in place for detecting and reporting shortages and overages?

e) Are procedures in place to track the timely movement of incoming / outgoing goods?

f) Are empty and full containers stored properly to prevent unauthorized access?

g) Are empty containers examined on receipt?

h) Is hazardous cargo properly labelled and stored separately?

i) Is there a container loading verification procedure to screen for un-manifested containers?

j) Are procedures in place to notify Customs and law enforcement agencies of irregularities or suspected illegal activity?

4. Personnel.

a) Are employees adequately screened and interviewed before hiring, including background checks and application verification?

b) Are employees restricted in their access to shipping, loading dock and cargo areas by specific job classification and function?

5. Education and Training.

a) Is a security awareness programme in place that educates employees in recognizing suspicious activities, maintaining product / cargo integrity and determining and addressing unauthorized access?

b) Is there an incentive programme in place for active employee participation?

c) Are internal security audits conducted?

6. Documentation.

a) Are shipping documents complete, legible and protected against exchange, loss or inclusion of false information?

b) Are procedures in place for verifying accuracy of basic information such as shipper and consignee names and addresses, first and second notify parties, and cargo description, weight, quantity and unit of measure?

c) Are procedures in place for reporting / investigating documentation discrepancies, including inventory shortages / overages?

d) Are procedures in place for tracking movement of incoming and outgoing goods?

e) Is computer access to shipment information adequately safeguarded?

f) Is manifest information complete, legible, accurate and submitted on time to customs?

Supply Chain Security Working Group Participants :

Miklós Horváth, Working Group Chairman, MASPED

Horst Tschurtschenthaler, Borealis

Pietro Mastrogiuseppe, Polimeri Europa

Kees van der Vleuten, Philips

Asko Raty, Storaenso

Eric Peetermans, SNCB Holdindg

Kevin Greene, UPS Europe

Luc Cassier, Bertschi AG

The European Freight and Logistics Leaders Forum
Avenue de Tervueren 270 Tervurenlaan
1150 Brussels
Belgium

Phone: +32 (0) 2 741 86 85 FAX: +32 (0) 2 741 86 86
E-mail: felforum@europeanfreight.org - www.europeanfreight.org