MIT Center for Transportation and Logistics

MIT Industrial Liaison Program

Supply Chain Response to Terrorism - Planning for the Unexpected

Cambridge, MA

December 5, 2002

This report was prepared for the Center for Transportation and Logistics (CTL) by Andrea and Dana Meyer of Working Knowledge® meyerwk@workingknowledge.com and edited by James B. Rice, Jr. of CTL. Please contact Jim Rice (jrice@mit.edu or 617.258.8584) if you have any questions or if you would like to discuss this report.

Table of Contents

Report Overview

This document represents a report of the presentations and content of a conference held on the MIT campus on December 5, 2002 entitled "Supply Chain Response to Terrorism – Planning for the Unexpected." The conference was co-sponsored by the MIT Center for Transportation and Logistics and the MIT Industrial Liaison Program, and was intended to begin examining the landscape of commerce and supply chain management in an environment of increased uncertainty from potential disruption due to global terrorism.

This report is structured in two parts, reflecting an interpretation of the content in each presentation (A. Presentation Summaries) and a synthesis by the authors of the proceedings (B. Themes). As the reader will observe, there are many new issues for managers and leaders to consider, and much work to be done to develop comprehensive solutions to the problems and issues surfaced at the event. Hopefully this is a useful start for practitioners, government and academia to collaborate on creating new solutions.

A. Presentation Summaries

1. "Assessment of the Security Threat," John Deutch, MIT Institute Professor

The vulnerability of the logistics system is a priority security concern, Prof. Deutch said. Taking action to secure it will be a necessary part of business, and businesses will have to devote resources toward it. "Any firm would be foolish not to consider this matter with the appropriate seriousness," Prof. Deutch warned.

Before 9/11, U.S. citizens relied on the government to protect us and give us warnings of potential threats. The new threat of terrorism has changed the rules. "Classic" terrorists focused on a single attack such as the assassination of a minister or bombing of a bus. Such attacks were episodic, not disruptive to the whole economy, and they did not involve the deaths of thousands. The attacks of 9/11 signal a new kind of terrorism, "catastrophic" terrorism, which is qualitatively different from classic terrorism. The new terrorist organizations are well-financed, disciplined organizations with global reach. They operate simultaneously in different countries. It is feasible that these organizations have chemical weapons, and they have the potential to acquire nuclear weapons.

The U.S. public infrastructure is vulnerable, as the attacks of 9/11 demonstrated. Ironically, the peace and true security that the U.S. enjoyed for so long has made us woefully unprepared for such attacks. We don't have legal authorities and organizations in place to adequately defend ourselves against terrorist risks. Our organizations were developed half a century ago, when there was a clear distinction between wartime and peacetime, and a clear distinction between foreign threats and domestic threats. Today, these distinctions are not very clear. In the past, the CIA focused on foreign threats while the FBI investigated domestic crimes. In the age of potentially catastrophic terrorist attacks, these

previously separate organizations need to work together to pool their intelligence in order to analyze the full picture of the threats.

Five Steps to Protect the Supply Chain

Prof. Deutch offered five actions that businesses can take to protect the supply chain. The first and most important step is to know your employees. A few bad actors can create havoc, so conducting background checks and having full knowledge of all employees is vital.

Second, each firm should have an explicit back-up plan to allow operations to continue in the face of disruption. (See the review of Steve Lund's presentation below for an in-depth discussion of this topic). Third, firms with worldwide operations should recognize that they are at a greater risk than firms operating only in the U.S., because terrorists will have greater difficulty reaching the US-only firms. Fourth, in the face of an attack, businesses need to move quickly to a workplace that has secure communications and computers. (Most firms have vulnerabilities in their computer control systems). Fifth, companies will need to cooperate with law enforcement and government, but at the same time they should retain legal counsel so that they protect their customers, company and employees. In short, companies should cooperate with the government in a sensible way.

Counter-terrorism is not an impossible problem, Prof. Deutch said. It will cost time and money, but it must be regarded as an insurance cost. All the risks cannot be removed, but they can be minimized, and defining the nature of the risk is important. "Think first, analyze second, spend third," Prof. Deutch said, suggesting that organizations think about the problem, analyze the costs and benefits of various actions, and then implement selected actions. Ultimately, customers will want to do business with firms that are aware of and prepared for the threats.

2. "The World Security Situation After 9/11," Stephen Van Evera, Professor of Political Science and Deputy Director, MIT Center for International Studies

Al Qaeda poses a grave threat, Prof. Van Evera said, because al Qaeda is more ambitious than past terrorist organizations. In the past, terrorists did not aspire to mass murder. Terrorists sought to have a lot of people watching, not to have a lot of people dead. Al Qaeda is different; it seeks to strike a huge blow against the U.S. economy and claims the right to kill 1 million U.S. children and 4 million U.S. adults. Osama Bin Laden was quoted as saying: "To kill Americans...civilian and military -- is an individual duty for every Muslim who can do it in any country in which it is possible."

The Short-Term Situation

The war on terror needs to be fought on four fronts, Prof. Van Evera said. Currently, President Bush is focusing purely on the offensive front -- hunting down and destroying al Qaeda. Three other fronts need to be pursued just as vigorously:

1) The defensive front, in which U.S. intelligence plays a key role in counter-terror and ensures safe borders.
2) The "special teams" front, in which we secure the vast nuclear and biological weapons that remain poorly secured in the former Soviet Union. Currently, the unsecured nuclear materials in Russia are enough to make tens of thousands of atom bombs. The U.S. is only spending $1 billion per year to lock down these weapons, mistakenly seeing the money as "foreign aid to Russia" as opposed to the security priority that it really is. At the present low rate of progress, nuclear material will remain loose in Russia until 2018.
3) The "ideas" front, in which U.S. public diplomacy efforts are aimed at the Muslim world to correct the lies and misperceptions being propagated by Saudi satellite TV. Current efforts are half-hearted, and the Voice of America Arab language service was recently shut down.

The Role of Government and of Industry

Winning the war on terror will require innovation from government and industry alike. For its part, government needs to focus more resources into counter-terror functions as opposed to traditional military functions (such as Army, Navy, and Air Force). For example, more resources need to be devoted to intelligence efforts to find terrorists, to homeland security, to diplomacy to lock down nuclear weapons, facilities and materials, and to save failed states that are al Qaeda havens and breeding grounds for terror.

Industry has a significant role to play in the war on terror, especially in the area of homeland security. Companies can help to reform important parts of our trade and port system -- any company that ships things has a role to play. In addition, new insurance laws need to be established to give businesses incentives to minimize the threat, by preparing themselves (for example, to relocate air intakes on buildings so that terrorists can't easily introduce anthrax into buildings).

To deal with World War II, the U.S. built strong Army, Navy and Air Force organizations. To deal with catastrophic terrorism, we need organizations that will work cooperatively together: the intelligence agencies, local law enforcement, the U.S. Coast Guard, the Cooperative Threat Reduction Initiative, the State Department Office of Public Diplomacy, the Agency for International Development, and industry itself.

3. "Freight Security and the World Economic Forum," David Grubb, Supply Chain Security Practice Partner, Accenture

Transportation Security Model

Threats can be categorized using a 3-level framework that decomposes the entire transportation system and its associated threats by the mode, by the entry point, and by the threat areas. The first level is the mode of transportation. This includes air, maritime, highway, and rail. The second level is the entry

point and could include freight yards, border crossings, ports, delivery points, etc. The third area is the threat area, which could include employees, cargo, passengers, service providers, and so on.

The reason for this decomposition is twofold. First, it helps in systematically enumerating the various potential threats to the supply chain -- creating a systematic list that can be more consistently tackled. Second, it helps in aggregating threat scenarios and best practices across seemingly disparate threats. For example, the threats and best practices associated with an entry point like a border crossing are similar, regardless of the mode of transportation. Alternatively, threats associated with employees can be addressed with practices that work for all modes and all entry points. The result is that this framework can help organizations develop responses to the threat of terrorism on a more efficient and effective basis.

Threat and Response

Mr. Grubb noted that the systemic nature of the threat calls for a more systemic response. Individual action and specific initiatives are inadequate. What is needed is a overall vision that works across modes and threats to provide better continuity of security. Companies and governments must also realize that the threat is fluid -- the terrorists will attempt to adapt to any countermeasures. Finally, more analysis is needed to examine the impact of security on supply chain efficiencies -- looking for ways to maximize security and minimize cost.

Freight Security Initiative

The 2002 World Economic Forum served as the genesis for the Freight Security Initiative where the World Economic Forum, Accenture and MIT will explore relevant industry-wide issues. The program is designed to research, identify, and communicate security issues to industry, governments, and controlling entities. The effort includes both executive interviews (with suppliers, shippers, government, and insurance agencies) as well as a broader survey. Ultimately, the goal is to mobilize resources and develop a comprehensive, coordinated approach to freight security.

Key Hypotheses & Key Focus Areas

Mr. Grubb posed five key hypotheses that provide a basis for Accenture's research on the issue of supply chain security:

1. Industry does perceive the threat to be highly relevant.
2. Security initiatives are underway, but they have not significantly reduced the threat yet.
3. Government initiatives are taking a controlled response to security, but they still lack unilateral measures.
4. Shippers will rely on carriers to provide security.
5. Freight security will increase supply chain costs, but the exact economic model is unclear.

The results of the research could help focus industry efforts in a number of areas. These areas might include:

* assessing and certifying the facilities and operations of supply chain participants

* creating a standardized shipment data repository
* developing and deploying tracking and anti-tampering technologies
* pre-emptively screening suspect and high-risk shipments
* deploying reactive countermeasures that can electronically stop suspicious activities

4. "Supply Chain Response: UPS Perspective," Robert Bergman, VP of Public Affairs for UPS

Businesses face the question of how to balance security and efficiency. The rules have changed -- security must become part of our thinking in a way we didn't imagine before 9/11. Security will be necessary for business. The good news is that taking measures to make the company more secure will help with making the company more efficient as well.

UPS is a global company that supports open markets. Not only does it ship 13.5 million packages a day, but one million of those packages cross international borders. Moreover, UPS is the 11 largest airline fleet in the world and is one of the largest users of railroads in the U.S. and ocean-going fleets. Thus, UPS is itself potentially a big target and at the same time has a big stake in transportation safety. The company has security measures in place to protect its employees and assets. At the same time, the company feels that it is important to prevent well-intentioned but misguided regulation from achieving what terrorists could not.

A Layered Approach to Security

It would be simplest, but naive, to think that UPS needs to examine every package in an attempt to detect harmful material. Such an approach would be unrealistic and would bring deliveries to a halt. There is a role for inspection, but that role must be taken within a broader context.

UPS takes a three-layered approach to security:

1) *Business Practice*: UPS drivers are trained in consistent processes that not only improve efficiency and cut costs but also make it harder for anomalies and violations to occur. Consistent business practice and attention to detail minimize infractions.
2) *Information*: Information is essential for security. With shipments, the vital information includes who shipped it and where it is going. Information helps UPS operate better and improves visibility. A new law requiring 24-hour advance notice of shipment manifests to Customs lets customs see what is coming into the country, which improves security.
3) *Physical Security*: UPS uses a variety of methods for inspection, but the key is that the technology must work in real time to keep shipments moving. A key success factor here is people, because people must know what they are looking for during the inspection process. Technology cannot be foolproof, so the focus is to look at how the system fails and design it to fail smartly. For example, when one person in an airport dashes through security, it shuts the whole

airport down. A better approach is layers of security with overlapping, cross-checking steps and human intervention.

Public-Private Partnerships

Government actions are key to the whole endeavor of keeping the supply chain secure. To be successful, government actions must be coordinated. Agencies can't operate effectively in silos. Private industry also needs to be involved, because many of the assets are privately owned and industry has extensive expertise in supply chain operations. At the same time, private industry needs government-provided intelligence on threats.

Another area of cooperation is regulation. The key to regulation is that the regulations need to make sense and be made by people with knowledge of transportation, not just knowledge of regulation, so that the regulations don't disrupt commerce. In the rush after 9/11, regulators adopted rules that don't necessarily enhance security, and that is a problem. For example, when passing the Transportation and Passenger Act, the FAA issued the mandate to secure cockpit doors. This mandate makes sense for passenger airlines, but the law extended to cargo planes. In cargo planes, the law doesn't make much sense because many cargo planes don't have cockpit doors. The regulators need to understand the nature of transportation, and working with private industry will help share this vital expertise to the benefit of all.

5. "Supply Chain Security," Yossi Sheffi, Director, MIT Center for Transportation and Logistics

The threats to the supply chain take many different forms -- chemical, biological, bombings and cyber attacks that target infrastructure: agriculture, transportation, financial, medical and government systems. Given this, we can learn from past disasters and apply these learnings to the impact from potential terrorist attacks. For example, the Bhopal chemical disaster parallels a chemical attack. The Chernobyl nuclear accident simulates the effects of a dirty bomb. The influenza epidemic in 1918 parallels a biological attack, and hoof-and-mouth disease in the UK parallels an attack on agriculture.

Two lessons emerge from these disasters. First, recovery from the disasters was quicker than expected. Second, government response to the disaster often created a worse problem. For example, the quarantines and slaughter of cattle in the UK cost less than $1 billion to agriculture, but much greater damage (some $2-$4 billion) was caused by the government closing down certain geographic locations. The government acted as if agriculture was the country's most important industry, which it is not. Similarly, after the Kobe earthquake, the government provided free hospital care to the injured. This action almost bankrupted most of the private hospitals, which couldn't compete with free care offered by the government.

Supply Chain Preparedness

Companies can take specific actions that will mitigate the effects of threats and disasters. First, companies may want to carry more inventory, but this move is not a move away from just-in-time and toward just-in-case inventory policies. Rather, companies need to manage strategic inventory like they manage strategic reserves.

Second, companies should think about backing up their knowledge. That is, developing back-up processes not just for computers but also of processes. Standardizing processes and cross-training employees is useful because it lets a company move personnel around if needed.

Third, operating the supply chain under uncertainty means improving visibility and collaboration. Transportation visibility needs to be maintained across multiple hand-offs and requires detailed handling and independent data acquisition. Collaborative processes such as vendor-managed inventory (VMI) can be supplemented with joint emergency planning (such as developing alternate shipping methods or suppliers) and sharing best practices in security measures.

New Business Trade-offs

Businesses must now grapple with a series of trade-offs.

Efficiency vs. Redundancy: Making sure that despite lean operations and just-in-time practices, the company has some redundancy and flexibility to respond quickly. The key question in this dilemma is who pays for the redundancy.

Collaboration vs. Secrecy: "Hazardous Material" tags alert partners but they also alert potential bad actors about container contents.

Centralization vs. Dispersion: Centralization may make a company more vulnerable if one of its key distribution center is hit. On the other hand, dispersion makes a company more vulnerable to cyber and communication attacks.

Taking Action vs. Doing Nothing: Preliminary Research Findings

Prof. Sheffi described some preliminary findings of companies that are taking active steps to secure their supply chain compared to those who are not. It appears that companies that are taking action often have had a previous bad experience, have a corporate culture that supports action (being in the defense business, working in dangerous places around the world) and have security departments staffed with experts. The companies that are taking little to no action ('doing nothing') often regard 9/11 was a one-time event, can't find a way to pay for security measures, and believe that the primary responsibility for security lies with the government. Currently, a majority of U.S. companies are in the do-nothing category.

How to Take Action

An initial observation is that companies taking action are employing several activities to build resilience in their supply chains. These include building redundancies, tightening collaboration, working with the

government, and using technology (such as RFID and GPS) to support new security measures. In most cases, these firms are also investing in education and awareness, creating contingency plans, and conducting drills with partners. Taking action to secure the supply chain is a long-term adjustment, but the good news is that there are collateral benefits to supply chain operations. Benefits include: better collaboration, better visibility, better controls (which reduce theft) and improved IT processes. In addition, actions taken in participation with local communities bring better contact with local citizens.

6. "Securing the High Tech Supply Chain," Steve Lund, Director Corporate Security, Intel

Actions which Intel took to prevent cargo theft brought it collateral benefits that helped it be better prepared to deal with terrorists.

Intel's Freight Security Model

Intel's freight security model includes physical security of company premises, procedural security, and metrics that guide progress and provide accountability. Intel formed the Technology Asset Protection Association (TAPA) when one of its customers, an original equipment manufacturer (OEM) called Intel to say, "You have good security, can you share it with me?" TAPA is an association of security professionals from high technology companies. TAPA's mission is to find best practices in security and supply chain protection and then to proliferate those practices within the technology industry. The association works to identify practices that are reasonable and not cost-prohibitive. TAPA has 450 member companies with a collective $1.25 trillion dollars in market capitalization.

Intel's Process

Intel began its efforts with a senior task force, signaling the importance and urgency of the security issue. The team began by analyzing single points of failure: what facility or process, if it was down, would cause the death of the company, and what can we do to mitigate it? Steps to ensure business continuity had to come from the experts, so ownership of those measures is held at the business group level.

Intel used a risk assessment model to examine its critical assets and the types of threats that would impact those assets, including what the impact would be, and what steps would lower the risk level. In some instances, the exact nature of the threat is less important than the simple fact that the facility is out of commission. The key focus is how to get it back into operation or how to find alternate ways to accomplish the activities of that facility.

Corporate Emergency Operations Center

Intel has set up a corporate emergency operations center as well as several local emergency operations centers (EOCs) to deal with major business disruptions, whether they are terrorist attacks or natural disasters such as earthquakes. The purpose is to have a coordinated response globally. Each EOC is locally managed by employees from security, public affairs and site services. Intel has response

templates for each type of crisis that can occur. Each center also has redundant communications systems (satellite, PBX phone lines, dedicated copper phone lines, local channel radios, satellite phones and ham radio operators). This redundancy ensures that EOCs can communicate and that all sites can put out a consistent message.

Supply Chain Drills

Intel performs some 10-12 drills quarterly that simulate response to various threats, such as an anthrax response, aviation disaster response, function-specific business recovery, and a dirty bomb scenario. Each threat has a corresponding roadmap which employees enact (for example, responding to anthrax includes test kits and training mailroom personnel for awareness).

Intel expanded its drills to include key suppliers, who can play a role in business continuity as well as identify gaps in existing procedures. The drills involve accelerated timelines, roleplaying, and supplier engagement. For example, Intel ran a drill that simulated the loss of a key manufacturing facility in the Philippines. Employees measured the impact to other sites and measured capability that could be regained within 72 hours and within 7 days. Communication to employees and shareholders was also included in the drill. The end goal was to develop an integrated response capability.

7. "International Port Assessments," Charles McCarthy, Infrastructure Protection and Operations Division, Volpe National Transportation Center

The John A. Volpe National Transportation Center is the R&D arm of the Department of Transportation. One portion of the center's work includes supply chain and transportation security. While previous efforts have emphasized cargo crimes, terrorism is now a major concern.

International Port Assessments

The Volpe Center is in the process of conducting a series of international port assessments. The intent is to gain a full picture of both the practices and the vulnerabilities at ports.

At each port, a three-person team examines operational security, physical security, information technology, and information systems security. The team interviews both the managers of the port and frontline personnel to understand actual procedures at the port. The team also speaks with appropriate government personnel, local logistics organizations, and even local maritime schools to gain better insight into operations.

Integrated Channel Analysis

Volpe's International Port Assessments use integrated channel analysis that examines the distribution channel, the communications channel, and the financial channel. This analysis starts with the distribution channel and includes understanding the physical movements of cargo, inspections, container terminals,

carriers, and who has physical access to the container. The physical security of the port and the containers is a key element of the assessment.

Integrated channel analysis looks beyond the distribution channel because securities practices must go beyond the security of the physical distribution channel. Each channel plays a role in securing the supply chain. For example, the financial channel protects against terrorists and criminals hiding money transfers. The communications channel embodies all of the information that helps security personnel track and screen the flow of cargo. The communications channel also encompasses the IT systems that facilitate port operations. Finally, the communications channel has additional security needs in terms of passwords, firewalls, and back-door modems.

Dimensions that Impact Best Practices

International Port Assessments is intentionally surveying a very diverse group of ports. The study runs the gamut from Singapore's massive automated container port to the smaller traditional bulk-goods and livestock port of Hamriyah, United Arab Emirates. Other ports in the assessment include Rotterdam, Naples, Malta, Vancouver and others. These ports include transshipment ports, with their sprawling container yards, and intermodal ports with truck and rail connections.

There is no one set of best practices that work for every port because of differences between ports. Dimensions mentioned by Mr. McCarthy that impact best practices include:

* government vs. private control of the port
* the relative amounts of labor vs. technology in port operations
* the level of transshipment vs. import/export activity
* whether cargo is being transferred ship-to-ship vs. intermodal

Preliminary Best Practices

Mr. McCarthy listed some the best practices found to date. These include:

* adding seals to all containers and notifying authorities of any unsealed containers
* minimizing the time in the terminal
* limiting access to the port to authorized personnel with verified IDs
* sharing tips and information with the Customs authorities of other countries via regional networks

8. "Using Real Options Methodology for Corporate Response," Richard de Neufville, Professor of Engineering Systems, MIT Civil and Environmental Engineering

The notion of "real" options draws on the extensive theory of financial options to help managers think about the costs and benefits of flexibility. Flexibility is crucial in an age of uncertainty, whether that

uncertainty is driven by natural disasters, terrorist attacks, or the changing needs of consumers. The essence of flexibility can be embodied by an option.

Options as a Right, not an Obligation

Options provide the right, but not the obligation, to take some specified action in the future. Thus, an option provides the flexibility to take an action only if it is warranted. The most common options are financial stock options, which give the owners of the options the right to buy or sell stock at a fixed price regardless of the current price of the stock. Financial options can let someone sell stock at a high price even if the stock price has fallen, or to buy stock at a favorable price, even if the stock price has risen. The point of financial stock options and of real options is that they reduce risks in situations where some crucial variable is fluctuating in an unpredictable fashion. The rights provided by options embody the flexibility to cope with or capitalize on uncertainty.

Real Options for the Supply Chain

Flexibility represents both insurance against unfortunate incidences and the capability to capitalize on opportunities. In the realm of the supply chain, real options help cope with variations in supply and demand. For example, redundant inventory provides the right, but not the obligation, to use those inventoried items to cover for either fluctuations in the supply (e.g., a terrorist disruption of the supply chain) or fluctuations in demand (e.g., a hit best-seller product). Another example of a real option might be a contract with a secondary supplier to provide emergency capacity. A third example might be a flexible, platform-based product design that lets a company substitute different components.

Buying Flexibility: Cost vs. Benefit

Real options buy flexibility. In the preceding supply chain examples, the company spends money to have the right, but not the obligation, to react flexibly in uncertain situations. For example, the company might spend money to buy and carry emergency inventory, or to sign a contract for backup capacity, or to engineer extra flexibility into a product. The value of the option is defined by the value of having flexibility -- being able to recover from a disruption or capitalize on an opportunity. This value is a function of the probability of needing the flexibility and the incremental performance improvement created by having that flexibility. Thus, the value of flexibility depends on the range of scenarios that might occur for the company.

Real Options vs. Traditional Optimization

Too many management decisions are based on single-outcome optimization, Prof. de Neufville said. Many supply chain decisions are based on optimizing for the average or expected outcome as opposed to optimizing for the uncertain range of possible outcomes. Real options provide a means of changing the shape of the range of outcomes -- reducing the depths of the worst-case scenario and improving the heights of the best-case scenario. The change promoted by options thinking is a shift away from optimizing decisions for specific expected circumstances toward obtaining more flexible decisions to cope with a range of outcomes.

Summary

Real options do add cost, complexity, and time to business processes. In return, the company is poised to perform at a higher level over a much broader range of scenarios and conditions. Options thinking helps managers consider the value of flexibility and create a more adaptive organization.

9. "Maritime Supply Chain Security," Rear Admiral Vivien Crea, Commander, First Coast Guard District, United States Coast Guard

Commerce vs. Security

The U.S. Coast Guard will play a major role in protecting America's global supply chain. The greatest challenge of this role is balancing commerce and security. Transoceanic and intracoastal shipping play a major role in the U.S. economy. An oil tanker can carry as much oil as 1000 tanker trucks and does so at less than 1/10 the cost. Cutting off the flow of goods would certainly stop terrorists, but it would also cripple the economy. The challenge is to push America's borders outwards without impeding the flow of legitimate commerce.

Operation Safe Commerce

Operation Safe Commerce was a testbed for technology and procedures for advanced supply chain security. This public-private partnership created and tracked a specially-instrumented container from a factory in Slovakia all the way to the U.S. This trip used a number of modes (truck, rail, and container ship) and crossed numerous international borders. The goal of the project was to get more information about shipments. A Phase II project will look at barge shipments from Halifax.

The project also examined vulnerabilities during the trip. For example, some movements of the container took inexplicably long periods of time to complete (one 45-minute journey took 24 hours, which nobody could explain.) Another, somewhat humorous, vulnerability was the fact that one strange-looking, antenna-encrusted container failed to elicit suspicion on the part of any Customs officials along the container's long journey.

Security for LNG Shipments

Rear Admiral Crea showed a photograph of a massive LNG (Liquefied Natural Gas) tanker in Boston harbor, with the buildings of the Boston skyline in the background. Although the physical properties of LNG make for a low likelihood of catastrophic explosion, the U.S. Coast Guard is not taking any chances when these vessels come near heavily-populated ports like Boston. Because the shipments are a closed loop system (a small number of ships cycle between Boston and natural gas production facilities in Trinidad) security can be especially tight. Armed escorts, concentric security perimeters, inspection, and security at all points of the journey make these ships highly secure.

Security Working Groups

Rear Admiral Crea also described some the working groups that are part of the Boston Model Port effort. For example, the Bulk Liquid Working Group is examining the security of Canadian debarkation points to better restrict access to vessels. The Large Passenger Vessel Working Group is improving systems for getting and processing passenger information. The Container Working group is looking at increasing the flow of supplemental information, doing better pre-inspection, and improving the off-loading of suspicious cargo.

Maritime Transportation Security Act

New legislation, such as the Maritime Transportation Security Act, is part of the government's response to terrorism. For example, the Maritime Transportation Security Act extends the jurisdiction of the U.S Coast Guard from 3 miles out to 12 miles into the ocean. The Act also calls for assessments of foreign shipping ports and new security regulations with these ports. Just as the government must work with private companies to improve security, so, too, the U.S. government must work with international bodies (such as the International Maritime Organization) and foreign governments to create mutually acceptable bilateral agreements on maritime security.

Summary

Rear Admiral Crea listed the following key issues for improving the security of the global maritime supply chain:

* cooperation between private enterprise, local authorities, the U.S. Coast Guard, and international authorities
* creation of embedded value in new security-enhancing business processes
* international standards for more uniform security
* R&D and applied technology for more efficient and effective security
* joint effort between government and industry to create more secure supply chains

10. "U.S. Customs Perspective," Philip W. Spayd, Director of Field Operations, North Atlantic, U.S. Customs Service

As a field operations manager, Mr. Spayd knows firsthand the volume of traffic that flows through the nation's ports (40% of all U.S. trade arrives by water). About 15 million containers are on the move everyday. Much of the new policy is geared toward pushing the borders of the U.S. outward to prevent a terrorist weapon from even coming into port. This includes working with the largest ports in the world to improve overseas security and to station U.S. Customs inspectors at these foreign ports.

Safer Containers

Mr. Spayd presented a nightmare scenario in which the terrorists modify a container (not the cargo) to be a bomb. They then put the container back on the shipping lanes and wait for it to eventually get to the U.S. several voyages later. The Container Security Initiative is designed, in part, to address these concerns by tracking the history of the container and flagging containers that may have visited insecure ports sometime in the past.

Customs-Trade Partnership Against Terrorism (C-TPAT)

C-TPAT is a certification initiative to work with carriers, brokers, and warehouse operators to improve the security of the nation's ports. It includes collaboratively-defined guidelines to address issues such as procedural security, physical security, conveyance security, training, etc. The program is only open for a limited time because the Customs Service wants only the strongest and most interested parties to apply. Members of the program will enjoy expedited Customs processes because the required security measures will make member's shipments of lower risk.

100% Inspection of High-Risk Containers

Given the stakes involved, the Customs Service is dedicated to inspecting every container that might be a threat. Part of this effort includes distinguishing between high risk and low risk shipments. Overall, the Customs Service expects to inspect about 2% of incoming containers. Mr. Spayd listed four key elements of the new inspection efforts:

* Identify high-risk containers and shipments
* Pre-screen shipments in foreign ports
* Use technology to inspect containers
* Deploy technology to inspectors

Plea for Public-Private Cooperation

Mr. Spayd concluded with a plea for greater cooperation and reciprocity between government and the private sector. He argued that improved security systems benefit both public and private interests. Companies have a new opportunity to add both value and security. He suggested that some of the savings generated by improved logistics efficiency should be reinvested in the security of these same logistical systems.

11. "Concluding Remarks," Yossi Sheffi, Director, MIT Center for Transportation and Logistics

Prof. Sheffi closed with a few summary comments about the conference. Like many in the audience, he found the initial sessions to be quite sobering. Yet everyone must face the new realities of international terrorism, and companies will have to learn to contribute to supply chain security. More companies

need to move out of the "do nothing" category and take responsibility for the security of their part of the global supply chain.

Fortunately, the conference also provided some frameworks and ideas for accomplishing the daunting task of preventing and coping with terrorism. Frameworks such as real options theory can help companies consider the risks and countermeasures to those risks. Sharing best practices and cooperating with government initiatives also hold the promise of both preventing attacks and accelerating the recovery from any attacks that do occur.

B. Themes

1. Summary of Threats

A grim list of terrorist threats faces the U.S. and its Western world partners. Both Prof. Deutch and Prof. Van Evera described some of these threats, their relative magnitude of impact, and their relative probability of occurrence. Understanding these threats is both sobering and a motivator of action. The events of 9/11 are minor compared to the potential for mayhem and destruction of other more terrible weapons.

Of the threats discussed, nuclear weapons pose the greatest potential for damage -- the potential to destroy a major city in a single blast. After the dissolution of the Soviet Union, a large quantity of nuclear materials and expertise became far less controlled and secure than it was previously. The potential for diversion of fissile Uranium or Plutonium is high. Fortunately, the technical hurdles for constructing a nuclear bomb are relatively high, and diversions of dangerous quantities of nuclear materials have not yet occurred. Unfortunately, these hurdles continue to drop as more nations work on nuclear technology. In particular, newer nuclear states have far less security and safeguards on their nuclear arsenals, making theft of a usable bomb an increasing possibility. A related threat is a so-called "dirty" bomb -- a bomb the uses conventional explosives to disperse a dangerous quantity of radioactive material. Prof. Sheffi noted that the aftermath of Chernobyl is a reasonable analog of the aftermath of a dirty bomb.

Biological weapons are also a major concern because many have the potential to spread and reach epidemic proportions. Unlike the anthrax attacks of 2001, a smallpox attack would lead to widespread disease and fatalities. Prof. Sheffi also noted that crops and livestock could be targets of biological attack. Although governments are less likely to use biological weapons in conventional warfare, terrorists are actually more likely to use biological weapons because they are easier to obtain and deploy than nuclear weapons. Given the increasing power of off-the-shelf biotechnology, these weapons are a more likely threat than nuclear weapons.

Chemical weapons are another concern. Many common chemicals are precursors to dangerous chemical weapons, and the processes to synthesize these chemicals are not especially difficult. Counterterrorist experts fear what a terrorist group might concoct in a garage or how they might subvert

the chemical factories in sympathetic nations to mass-produce nerve gas or other agents. Moreover, companies routinely ship hazardous chemicals both domestically and internationally. Attacking a facility or shipment could lead to a dangerous release of chemicals.

The most surprising lesson from 9/11 was the terrorists' use of commercial airliners as missiles. The single-minded willingness of the terrorists to die in the attack obviates the traditional negotiating tactics for hijacking situations. The potential for using available materials in a dangerous fashion makes every airplane, tanker truck, chemical factory, or nuclear power plant a potential weapon for the terrorists. For example, the U. S. Coast Guard is quite concerned about the threat latent in large ocean-going tankers such as the LNG (Liquefied Natural Gas) tankers that come into Boston harbor on a regular basis. For this reason, these shipments are now heavily secured at all points of the journey and especially upon entering the harbor.

The problem with terrorism is that it is paradoxically small and large at the same time. It is small in the sense that a terrorist cell can operate with a small number of terrorists and modest resources. It is large in the sense that a single terrorist attack (e.g., 9/11) can create tens or hundreds of billions of dollars in damage to the economy and kill thousands or millions of people. The small size of a terrorist force makes detection and prevention that much harder. The large consequences of such an attack can lead to draconian countermeasures that may be worse than the direct damage of the attack.

2. Shifting Social Contract with Companies

The Historical Social Contract between Companies and Government

Perhaps the most important lesson from this conference is the realization that government cannot solve the terrorism problem on its own. In the past, the social contract between companies and governments was one in which the companies pursued their private aim of efficient production of goods and services while government maintained a safe and civil haven for its citizens and businesses. In the past, government's approach to its end of the bargain was twofold. First, entities such as the State Department, the Department of Defense, and the CIA handled relationships and threats from foreign governments. Second, entities such as the FBI, state and local law enforcement handled the detection, prosecution, and punishment of domestic criminals. Government's approach to its side of the bargain worked well when miscreants were either small-time criminals or foreign governments.

Prof. Deutch described how ill-suited these current government entities are to fighting terrorism. First, a terrorist cell is not a like a massive army that is visible from space and controlled by another government. Leaving aside the issue of state-sponsored terrorism, organizations such as al Qaeda are small, tightly-knit, transnational organizations that respect neither national boundaries nor the rules of diplomacy and war. Terrorist operatives located within the U.S. are out of reach of foreign-facing organizations such as the CIA or Defense Department.

Second, the new al Qaeda-style terrorist cell is hard to combat with traditional domestic law enforcement. Until they perpetrate their planned attack, the terrorists are largely invisible and

noncriminal in nature. Although their intent is highly criminal, their initial activities are not criminal (prior to 9/11, taking piloting lessons or carrying a knife on board a plane was not illegal). The fact that these terrorists are only *planning* attacks makes them less accessible to U.S. law enforcement agencies such as the FBI or local police.

Shifting Nature of Terrorist Attacks

Prof. Deutch also stressed the more serious nature of 9/11-style terrorist attacks. Previously, government counterterrorism officials assumed that the terrorists wanted an audience, not massive numbers of dead bodies. Yet al Qaeda's stated goals and the 9/11 attacks suggest that these groups seek more than publicity. Thus, they are likely to perpetrate attacks that are far worse than the highly-visible, but ultimately superficial, attacks that were done by other terrorists in the past (e.g., assassinations or bombing a small target such as a nightclub or bus). Moreover, the willingness of the attackers to die in the attack defeats the underpinnings of the criminal justice system (deterrence through punishment) and traditional negotiation tactics.

In the past, isolated miscreants perpetrated crimes on individuals and companies. The limited scope of their crimes meant that solving such crimes and penalizing criminal activity was an adequate response. Police, criminal investigations, and the judicial system created a disincentive to crime. Also, the procedures used by law enforcement are more geared to collecting and sequestering evidence of a crime rather than openly collaborating with other law enforcement agencies in the proactive prevention of uncommitted crimes. In short, traditional law enforcement procedures are ill-suited for detecting and preventing terrorism.

Impact of the Shift on Companies

Detecting terrorists requires collecting data on the individually-innocuous but collectively-suspicious activities of potential bad actors. Because the terrorists are quite willing to use our own supply chain infrastructure against us and because much of this infrastructure is in the private sector, the private sector must play a larger role in counterterrorist activities. This private sector responsibility is twofold. First, it implies monitoring supply chain activities to help detect suspicious activity. Second, it includes securing company and supply chain resources that could be misused by the terrorists.

Moreover, companies cannot expect that the government will catch every terrorist or thwart every attack. Thus, it behooves private companies to prepare for terrorist attacks and the consequences of those attacks. Companies cannot necessarily count on overwhelmed government agencies to restore services; they may need to actively help themselves. Much of this preparation can utilize the same types of procedures and resources that a company might use to cope with other disasters, such as an earthquake, hurricane, or fire at a crucial facility.

Several presenters commented on this shift. Indeed, prior to a recent conference on terrorism, 90% of companies surveyed thought that government was responsible for counterterrorism. The percentages were reversed however, after the conference when the companies realized both the magnitude of the problem and how much of the company's future is at stake under various gloomy scenarios. Prof. Sheffi noted that the organizations that already know that they need to implement counterterrorism supply

chain initiatives are those that have dealt with terrorism before. Other companies are slowly realizing the need to take action.

3. Frameworks

Some of the presenters offered different frameworks for thinking about the problems of and the response to terrorism-based disruptions to the supply chain and commerce in general. These ideas can help companies and government agencies to develop new approaches to supply chain security in this new age of terrorism.

Threat Decomposition

Mr. Grubb of Accenture presented a 3-level decompositional framework for understanding threats to the supply chain. This transportation security model is useful for analyzing and cataloging potential threats:

* transportation modes (air, highway, rail, maritime)
* entry points (e.g., airports, pickup/delivery points, border crossings, etc.)
* threat areas (e.g., passengers, employees, cargo, shippers, etc.)

By working through the combinations across the levels, companies can catalog potential threats and address them. By aggregating threats within the categories on each level, companies can understand the commonality of responses to potential threats. For example, a company might examine the commonalities of threats associated with the maritime mode or consider the commonalities of threats associated with employees regardless of mode. This framework can help companies catalog, organize, and generalize the analysis of threats and the creation of responses to those identified threats.

Analysis of Prior Disasters

Prof. Sheffi described how analyzing past disasters provides useful insight into potential terrorist attacks. Examples include:

* the 1917 explosion of a naval ship in Halifax, Nova Scotia (analog of a large bomb in a port)
* the 1986 nuclear plant disaster at Chernobyl (analog of a dirty bomb attack)
* the 1918 Spanish Flu worldwide epidemic (analog of a biological weapons attack)
* the 1984 Union Carbide incident in Bhopal, India (analog of a chemical weapons attack)

The impact and responses to these and other disasters can help companies and government tune responses to future disasters. Analyzing past disasters helps managers understand who was affected, how they were affected, and how responses to the disaster helped or hindered recovery.

Real Options

Prof. de Neufville presented a framework for thinking about the costs and benefits of risk management actions. Drawing on the vast theoretical underpinnings of financial options, the notion of real options can help a decision-maker think about managing risk. Options theory is a formal way of defining and analyzing flexibility.

An "option" gives the holder of the option the right -- but not the obligation -- to perform some specified action at a later time. In the context of supply chain management, a real option might include safety stock inventory that provides the right, but not the obligation to use those inventory materials. Another example is a contract for reserve capacity at a back-up supplier, which provides the right, but not the obligation, to use that capacity. The buyer of an option pays a premium for the option, a notion which Prof. Deutch referred to as insurance cost. Buying options buys flexibility.

The goal of using options is to change the range of outcomes that can occur. Most often, real options would be used to limit the worst-case outcomes (e.g., disaster recovery). Options can also be used to maximize returns of best-case scenarios, such as when a product becomes a smash success and strains the capacity of the system. Because options (whether real or financial) have a cost, the use of options can reduce the average performance level somewhat.[1] The point of Prof. de Neufville's framework is to provide a useful means of thinking about the trade-off between average performance and risk.

As one audience member pointed out, however, lack of useful data is a challenge with any numerical framework for analyzing costs and benefits of risk management. Although Prof. Deutch and others noted that some threats are more likely than others (e.g., chemical and biological weapons are easier to construct than nuclear weapons), the exact probabilities of these events are unknown. In moments of gloom, the probability of terrorist attack seems to be 100%, while in moments of optimism the probability is much lower. Despite the uncertainty, the real options framework does help a company examine the costs of ameliorating unusual scenarios to reduce risks.

Sharing Best Practices

Companies and government agencies can improve security by sharing best practices. Intel described TAPA (Technology Asset Protection Association), which is a private-sector organization devoted to improving supply chain and transportation security for high-tech companies. By sharing best practices and creating improved standards for security, TAPA hopes to foster the spread of better practices that benefit all parties. The Volpe National Transportation Center is also working to learn and aggregate

[1] Prof. Sheffi is leading research at MIT to examine whether investments in supply chain resilience and security actually create benefits offsetting the cost of the investments. Much like the 'quality of free' observation of quality expert Philip Crosby ("Quality is Free" 1979, McGraw-Hill), it may be that 'security is free' for companies making investments in developing resilience in the supply chain. This is yet to be determined. An initial treatment of the benefits is presented later in this report. For additional information, visit the research web site at http://web.mit.edu/scresponse/

best practices for port security. By studying ports around the world, the Volpe Center is learning new practices and gaining a better understanding of remaining security risks.

4. Response: Prevention

A primary goal of a response to terrorism is prevention. Prevention is aimed at both catching terrorists before they act and deterring terrorists from even attempting an attack. Intelligence and inspection activities help catch terrorists by detecting their activities and thwarting their deliveries of people, funds, and materiel. These activities, in addition to other physical security measures (such as protecting cargo and facilities), help deter terrorists by convincing them of the futility of an attempted attack.

Prevention: Catching "Bad Actors" Before They Reach the Border

Both the U.S. Coast Guard and the Customs Service noted the need to catch high-risk shipments before they reach American shores. In particular, the fear of a nuclear bomb, "dirty" bomb, or biological weapon reaching a major port city motivates these agencies to push the boundaries of this country further out into the sea. In these scenarios, the terrorists could detonate their weapons in port before Customs Service inspections occur. Because the majority of the flow of goods coming to this country is in the hands of the private sector, some of the burden of prevention falls on the shoulders of the private sector (domestic importers, international carriers, or foreign suppliers). The U.S. Coast Guard noted that companies need to create a more secure chain of custody for goods and assets.

Various initiatives should help secure the country's borders. In particular, the Container Security Initiative (CSI) calls for 24-hour advance notice of the manifests of all shipments from selected foreign ports prior to loading. CSI also addresses the potential threat of the container itself -- the potential that the terrorists could modify a container to explode or disperse radioactive, biological, or chemical agents. Thus, CSI considers the history of the container, not just the contents of the container. CSI also places U.S. Customs Inspectors in foreign ports to help catch suspicious cargo and containers prior to loading and shipment.

A second initiative, C-TPAT (Customs-Trade Partnership Against Terrorism) is a mechanism for companies to work with the U.S. Customs Service. The intent is for companies to become known entities to the Customs Service and become a more trusted importer of goods to the United States. Companies that join C-TPAT can expect faster processing at borders and thus provide value to their customers. Registration for C-TPAT may only be open for a limited time because the Customs Service wishes to induct only the most willing participants into this program.

The U.S. Coast Guard also noted that the recently signed Maritime Transportation Security Act includes a number of measures to prevent terrorism. These include moving the border of the U.S. to 12 miles from the coast, conducting foreign port assessments, and establishing security requirements for ports. The U.S. government will be working with the IMO (International Maritime Organization), the United Nations, and various foreign port authorities to create needed bilateral agreements.

Risk-Weighted Inspection

The U.S. Customs Service has a mandate of inspecting 100% of high-risk shipments. Programs like CSI and C-TPAT are geared toward narrowing the field of high-risk shipments and making the job of inspection both more tractable and more fruitful. UPS, which carries some 1 million international packages daily, also uses a similar philosophy of inspecting an appropriate fraction of inspection-worthy packages.

Inspection technology is a crucial element of the effort. UPS noted that one of the greatest challenges to non-intrusive detection technologies (e.g., bomb sniffers, x-ray machines, and gamma ray inspection machines) is the speed and reliability of these systems. Miracle machines that can detect dangerous materials in a single item in a lab setting may not be practical for use in the high-volume, high-speed supply chain flows present in ports, truck yards, and airports.

Standardized Business Processes

Bob Bergman of UPS suggested that standardized business processes can help combat terrorism. When a company uses highly routine business processes, any anomalous behavior is obvious. This makes it harder for bad actors to tamper with the supply chain or divert materials from it. As a side benefit, standardized business processes also improve business efficiency.[2]

5. Remediation and Amelioration

Although the total prevention of terrorist attacks is an obvious goal, this goal is not necessarily attainable. The massive scale and openness of America's borders make absolute prevention impossible. Thus, companies must think about what they will do if the unthinkable occurs. Remediation is the other half of risk management -- creating contingency plans and prearranging needed resources to reduce the impact of catastrophic events. Phil Spayd of the U.S. Customs Service suggested that companies should invest the savings created by supply chain efficiency initiatives into supply chain security efforts.

[2] One downside is that highly efficient routine operations may potentially breed complacency and limited flexibility. Given this, supply chain drills as described and so actively implemented by Intel are one way to protect against complacency and rigidity.

Redundancies, Redundancies[3]

Both Prof. Sheffi, Prof. de Neufville, and others noted the need for supply chain redundancies as part of coping with terrorist attacks. Redundancies are especially important in tightly-run companies that use techniques such as JIT or lean manufacturing. Such redundancies might include:

* local inventory of imported components (redundant inventory)
* contracts with secondary suppliers (redundant capacity)
* multiple distribution centers for dispersed inventory (redundant locations)
* cross-training of employees (redundant skills base)

Several presenters noted that such redundancies do add cost. Using Prof. de Neufville's real options framework provides a means for companies to estimate the costs and the contingent benefits of such redundancies.

Knowledge Backup

Prof. Sheffi noted the need for off-site backups of all of an organization's knowledge and information. There is the very real possibility that physical or cyber attack could destroy or incapacitate a company's central IT resources. For example, many New York-based financial services firms lost IT, telecom, and data systems when the World Trade Center buildings were destroyed. Of special importance is operational and customer data that help the company minimize the disruption it causes for its customers -- minimizing the ripple effect that any attack is likely to have on the broader economy.

Unfortunately, IT systems do create a point of vulnerability. Fortunately, the ability to easily replicate enterprise resource planning (ERP), supply chain, and customer relationship management (CRM) data to protected off-site data centers more than makes up for this vulnerability. In contrast, systems based on paper hardcopy and the knowledge inside employee's heads are far more vulnerable to attacks that destroy buildings and kill key employees.

Standardization

Bob Bergman of UPS stressed the role of standardization in prevention of terrorist attacks, and Steve Lund of Intel and Prof. Sheffi noted the use of standardization in surviving such attacks. Standardized business processes help a company re-establish operations from remote sites. If all divisions of a company use similar practices, then unaffected divisions are in a position to help those affected by any attack or consequential disruption. Standardized processes are also more likely to be documented, which reduces the time required to train new or other employees to cope with any shortage of workers (such as during an epidemic).

---

[3] Resilience of the supply chain may be accomplished by various methods, including adding redundant resources and systems, developing flexible/responsive systems through system design (e.g. use of postponement strategies, risk pooling, multi-skilled labor systems). The terminology has not been refined to clearly differentiate between these various methods although Prof. Sheffi's research team is currently working to clarify these alternatives. For additional information, visit the research web site at http://web.mit.edu/scresponse/

Business Continuity: Intel

Steve Lund of Intel described its extensive business continuity efforts -- part of the company's "only the paranoid survive" philosophy. An element of this effort is a network of EOCs (Emergency Operations Centers) that serve as nerve centers in the event of an actual emergency. These centers use standardized procedures based on a set of templates that cover a wide range potential disasters (both natural and man-made). The centers include heavily redundant communications systems (from backup Internet connections to ham radio). Intel's preparations for a terrorist attack are a natural extension of the company's long-standing efforts to prepare for nature disasters.

Part of Intel's business continuity efforts are drills to practice the company's response to various scenarios (e.g., the loss of a site in the Philippines or an earthquake in Oregon). By executing some 10 to 12 drills per year, the company can both train its employees to efficiently deal with problems as well as refine its emergency procedures. Drills ensure that crucial backup systems will be ready if and when they are needed. As an example of the system's effectiveness, when 9/11 occurred, the company implemented a global response to the event within 1 hour of its announcement.

Failing Smartly

Bob Bergman of UPS also noted that security systems should fail smartly -- that managing the consequences of the failure is as important as reducing the probability of failure. No security measure can be 100% foolproof, so managers need to plan for the failure of security and limit the damage of such failures. As a counter-example, UPS noted how current breaches in domestic airport security lead to a shut-down, evacuation of the airport, and rescreening of everyone. It is not a smart failure when a single impatient tourist can bolt through security and delay the operations of that airport (and others) for hours. One good example of failing smartly was offered by Prof. Sheffi: when an earthquake in Taiwan disrupted supplies to Dell, Dell restructured its prices and offerings to steer customers toward PCs that it could build with available components.

6. Is the Cure Worse than the Disease?

At this point, no one has a good understanding of the collateral damage that counter-terrorism policies (by governments or businesses) will have on unlucky individuals, companies, and foreign nations. Some of these policies could be quite damaging to the economy. For example, one of the easiest (but extreme) preventative measures is to close down the movement of goods and people. That way the terrorists cannot use our own infrastructure to deliver attacks. Yet this preventative measure accomplishes one of the principle goals of the terrorists -- shutting down Western world capitalism.

Even a heightened level of precautionary inspections leads to economic damage. Philip Spayd of the Customs Service noted that it did not close the borders after 9/11, yet even the slowing of goods at the border created a de facto halting of the smooth flow of goods. Prof. Sheffi cited how a number of companies that use lean manufacturing techniques ran into trouble after 9/11 when supply lines were

effectively cut by delays at border crossings. In some of the scenarios discussed at this conference, much of the damage to the economy comes from the disruption of normal supply chain operations.

Prof. Sheffi cited a number of examples of government responses to natural disasters that had unintended, deleterious consequences. For example, Britain's efforts to contain hoof-and-mouth disease in cattle caused more damage to the tourism industry than it saved in the agriculture industry. Bob Bergman of UPS suggested that the private sector's superior understanding of the detailed workings of the economy made industry input into regulation essential. Prof. Deutch emphasized that although companies should cooperate with the government, they should also retain counsel to ensure their rights.

Other responses to terrorism can paradoxically reduce security. For example, Charlie McCarthy of the Volpe National Transportation Center noted that speedy movement is a best practice for reducing security risks. Thus, some argue that the process of delaying shipments and opening them for inspection actually adds more risk than it removes. Inspection processes can make shipments easier to tamper with because a stationary package is more accessible than a moving one. Additional handling steps provide a natural cover for tampering by corrupt or subverted inspection personnel, and excessive inspection could train recipients that opened and resealed packages are not suspicious. Likewise, GPS tracking of shipments might expose those shipments to attack if the terrorists can hack into the databases with the tracking information.

7. Tough Trade-offs

In addressing the issue of terrorist threats to the supply chain, companies face some tough trade-offs. These trade-offs go beyond the basic cost vs. security trade-off to include more subtle issues. Prof. Sheffi suggested three trade-offs. These were echoed by the comments of other presenters. The trade-offs are:

Efficiency vs. Redundancy

Many of the presenters worried about the trade-off between efficiency and redundancy. On the one hand, redundancy is key to both prevention and remediation of the terrorist threat. Redundant security measures improve the effectiveness of screening efforts --- each layer catching another fraction of potential terrorist actions. Redundant systems also help a supply chain recover in the event of a terrorist attack. Yet redundancy is inefficient, adding to the costs of supply chain operations. Worse, redundant systems can also reduce security by providing additional avenues for attack by terrorists in the form of additional facilities or additional points in supply chain processes that could be subverted.

Collaboration vs. Secrecy

The dissemination of information is a double-edged sword. Prof. Sheffi noted that visible HazMat signs on shipments increase the risk that terrorists could target that shipment of hazardous materials. Others noted that global tracking of shipments make them more vulnerable if terrorists hack into any of the

numerous databases (shipper, carrier, recipient, or government office) that could contain the tracking data. Finally, Prof. Deutch noted that government agencies are also wrestling with this trade-off -- deciding how broadly to share sensitive or classified intelligence data. Secrecy has risks, too, however. HazMat signs help local authorities cope with spills and accidents. Tracking information is intended to reduce the chance of diversion and tampering, and sharing intelligence data helps all parties develop a more complete integrated picture of the threat.

Centralization vs. Dispersion

Highly centralized systems create both single points of failure and invite targets of attack. Yet, dispersed systems contain redundancies and rely on vulnerable information technologies which are vulnerable to attack. Prof. Sheffi illustrated this trade-off in noting that McDonald's dispersed distribution network makes it less vulnerable than The Limited's single-distribution center strategy. Prof. Sheffi did caution that a dispersed strategy, while less vulnerable to physical attack, is far more vulnerable to cyber attack.

Security vs. Civil Liberties

The increasing emphasis on security will probably involve a loss of personal civil liberties. Perhaps the most unfortunate aspect of the response to terrorism is the lack of due process for those caught in its web. That a job applicant is turned away or an employee is fired because their name is coincidentally similar to some suspected (not even proven) terrorist is a travesty of what America holds near and dear. Yet the high potential for extreme damage makes it hard to uphold the ideal of "innocent until proven guilty."

8. Benefits

Speakers from both government and industry stressed the role of collateral benefits to companies' responses to terrorism. The arguments for having additional benefits were twofold. First, government recognizes that the private sector will embrace security measures more if those measures are seen has having additional business-only bottom-line benefits. Second, businesses realize that if they are forced to implement mandated regulations, they might as well implement the security measures in a way that creates additional business benefits. MIT President Charles Vest suggested that businesses will embrace security in the way that they embrace environmental issues -- although it does add cost, it is good business for competitive, ethical, and moral reasons.

Improved Visibility, Lower Uncertainty

A number of the security initiatives can improve visibility into the supply chain by providing information on what is where and when. The CSI (Container Security Initiative) mandate to provide 24-hour advance submission of shipping manifests prior to loading cargo onto U.S.-bound vessels in foreign

ports is one example of this.[4] Improved visibility can improve asset utilization for carriers and permit higher service levels for shippers and their customers. More trustworthy data on the location and disposition of containers, ships, and goods will aid in managing shipping operations by reducing the uncertainty along the supply chain.

Reduced Theft

One obvious side benefit of security is a reduction in theft from the supply chain. Tighter control of warehouses and shipments makes it hard for criminals to steal goods. Tracking containers and trucks via GPS means that they cannot be waylaid for too long before someone notices the anomalous movement of the goods. The same methods that prevent terrorists from accessing facilities and shipments also prevent the activities of other criminals.

Improved Partner Reliability

Part of the response to terrorism comes in the form of analyzing and certifying a company's business partners. The goal is to ensure that foreign suppliers are not using a company's commercial channels to import terrorist materiel. Many fear that terrorists could use legitimate business activities to hide preparations for nefarious acts.

Thus, companies can be expected to spend more time scrutinizing their business partners, especially foreign business partners. Even domestic supply chain partners can expect greater scrutiny. For example, part of Intel's business continuity preparations include assessing crucial domestic suppliers that might be disrupted by a natural disaster or terrorist attack. From this scrutiny can come more reliable supply chain operations. Certified, trustworthy partners are more likely to have better service levels in both good times and bad times.

Improved Employee Reliability

Companies will also come to know their employees better as a result of security measures. Background checks, instituted to catch potential terrorists, will also ferret out criminals (e.g., those that have outstanding arrest warrants or unacknowledged prior convictions). This can help reduce a company's risk of theft, embezzlement, or workplace injury.

Accelerated Flows at the Border

Greater scrutiny of international shipments is inevitable, and this security will add delays to companies' supply chain operations. Programs such as the Customs Service's C-TPAT are intended to ameliorate these delays. By working with Customs officials, companies become more known and more trusted entities. Companies that work with the government to implement secure supply chain operations will

[4] The CSI 24-hour notice initiative also has some unintended downside as the requirement as initially structured eliminates the ability for shippers to adjust shipping plans en route. In-transit modifications of shipping plans is a common practice among shippers that affords significant flexibility.

enjoy faster flows and fewer delays than those companies that ignore the need for higher levels of security.

Security as Value-Added Service

Although each company must take some responsibility for its security, the partners of a company can help. Dave Grubb of Accenture noted the potential for inefficiency and redundant effort if everyone in the supply chain is forced to inspect and document goods multiple times. Trusted business partners can provide value when they deliver secure, well-documented cargo. Although companies should never assume that cargo from a trusted partner is safe, the effort required to maintain security with flows from a secure partner is less than that required for insecure partners.

Thus, suppliers and carriers might create competitive advantage through offering security. Special certifications are one way to accomplish this. For example, C-TPAT (Customs-Trade Partnership Against Terrorism) is a mechanism for companies to work with the U.S. Customs Service and become a trusted importer of goods to the U.S. Companies that join C-TPAT can expect faster processing at borders and thus provide value to their customers. This benefit is especially important to supply chain service providers such as carriers and international port facilities.

Improved Business Continuity During Natural Disasters

Steve Lund of Intel's presentation highlights another crucial ancillary benefit of a company's preparations for terrorism -- improved business continuity when other, non-terrorist, disasters strike. An earthquake, natural epidemic, port strike, or a fire at a key supplier all have nearly the same impact on a company as a terrorist attack would. Indeed, Prof. Sheffi suggested that government officials and businesses could learn much from studying past natural disasters (from the Spanish Flu of 1918 to the Kobe earthquake of 1995). Recovering from a disruption of normal supply lines, facility operations, or employee attendance is a competence that every company might need.