MIT Center for Transportation and Logistics

# "Supply Chain Response to Terrorism: Creating Resilient and Secure Supply Chains"

Supply Chain Response to Terrorism Project

Interim Report of Progress and Learnings

August 8, 2003

This report was prepared by James B. Rice, Jr. of the MIT Center for Transportation and Logistics (CTL) and Federico Caniato of Politecnico di Milano for the Supply Chain Response to Terrorism Project team with contributions from team members Jonathan Fleck, Deena Disraelly, Don Lowtan, Reshma Lensing and Chris Pickett. This work was conducted under the direction of Professor Yossi Sheffi, CTL Director. Please contact James B. Rice, Jr. of CTL (jrice@mit.edu or 617.258.8584) if you have any questions or if you would like to discuss this report.

**Supply Chain Response to Terrorism Project:**
**Interim Report of Progress and Learnings**

# 1 Executive summary

Supply chain managers became aware of a new operating environment after the terrorist attacks on the World Trade Center and the Pentagon on September 11, 2001. These events exposed the pre-existing and latent risk of disruption to supply networks from terrorist attacks. The risk was there all along but the attacks made it real and foremost in our minds.

Furthermore, these events began to expose the more significant interdependence that exists between all firms in the supply network. The interdependence also includes reliance on those U.S. Government agencies involved with inbound material flows and transportation infrastructure. Given these interdependencies, if one firm fails in the supply network, the entire network performance is at risk. Understandably, this constitutes a new operating environment where firms need to think in terms of their supply network and not just their individual performance.

The new operating environment calls for designing security and resilience[1] into the supply network. Security and resilience are unique characteristics that require distinct plans in order to develop and create these characteristics within the firm. Fortunately, there are several actions that firms can take which will contribute to both improved security and resilience, although this is not always the case. The key takeaway is that it is critical to design for both security and resilience.

New organizational capabilities are also called for in this environment. Specifically, firms will need to pioneer new relationships with U.S. Government agencies that now share responsibility for making the supply network secure and resilient. Additionally, firms will need to develop deeper relationships with suppliers and customers throughout their supply networks to co-create a more secure and resilient network. Internally, the largest organizational challenge may be in establishing at the individual level a solid understanding of the interdependence of the systems, and the educational and training systems needed for robust network designs and planned responses to disruptions.

The Center for Transportation and Logistics' own response to the terrorist attacks and this change in the environment included initiating a research project – "Supply Chain Response to Global Terrorism" – to study how organizations have responded. Overall, we observed a broad range of responses, including many firms that were reactive[2], as well as firms that surfaced as being progressive.

The reactive firms appeared to be responding to government regulations and other mandates, often with a focus on observable and physical actions. The progressive firms appeared to be executing against previously established plans, honing and refining the security and resilience of their supply network beyond just the boundaries of their own firm.

Studying the practices of the progressive firms helped surface several characteristics that were common among the group and which are worth examining:

[1] One can think of supply network security in terms of maintaining the integrity of the product, processes, and information, in contrast to resilience which we define as "the ability to react to unexpected disruption and restore normal supply network operations."

[2] Exhibit 1 summarizes the four levels of security and resilience achievements for firms in the study.

1. Nearly all of the progressive firms (all but one firm) had previously experienced the impact of disruptions in their supply networks, and in response they built resilience and security into the current supply network.[3]
2. These firms revisited their existing supply network design, and actively redesigned their supply networks for resilience through a combination of flexibility and redundancy initiatives. Often, the firms elected to apply these in a 'layered'[4] fashion to create a system comprised of layers of security and resilience.[5]
3. In developing plans to respond, the progressive firms often focused on 'failure modes' – those limited number of ways that operations can be affected by the countless sources of disruption.[6]
4. The progressive firms developed resilience and security by leveraging their organization rather than through technology solutions. In particular, these firms built and deployed organization skills through active education, training, drilling, hiring, and personnel screening. This amounted to 'socializing' security and resilience into their organization's daily operations and processes (and often in their suppliers and customers organizations).

While these are factors common to the progressive firms, they do not prescribe any one particular supply network design. The net effect is that these firms have created resilient and secure supply networks by using the same principles applied to their respective business situations, resulting in many different supply network designs.[7] As often is the case, there is no one single answer or design that works for all firms. The range of practices and approaches does provide managers with a wealth of options for designing a secure and resilient supply network.

These efforts however, will likely fall short of success unless they make a compelling business case for investing in network security and resilience. Those firms that found success in making the business case did so by quantifying the potential impact from disruption, and they used fairly creative methods to quantify the impact[8]. As one responded noted, "Ultimately, you need to tie risk (of attack, disruption) to business performance."[9]

This report expands on these insights and altogether hopefully makes for a useful foundation for managers to use in designing their response in anticipation of future inevitable disruptions to the supply network.

[3] The exception was a firm that took significant action in response to a board-level external corporate security audit that noted weakness in the network and required progressive action.
[4] "Making the Nation Safer" National Research Council, 2002 notes that "A layered security system, in which multiple security features are connected and provide backup for one another, has particular advantages. Defeating a single layer cannot breach such systems." Pp 14-15.
[5] For security, this may entail having multiple passwords and authentication required at different phases of facility or system access. For resilience, this may entail using a mixture of flexibility and redundancy measures that provide back up to the back up systems.
[6] The key failure modes loss or temporary delay in supply, production, transportation, communication and/or personnel capacity.
[7] See Appendix 7, Many Paths to the Same Destination for examples.
[8] E.g. Including time-to-impact-at-the-customer, cost per day of disruption, franchise-level impact for missed promotions, cash-flow and liquidity impact for disruption to revenues, and collateral benefits accruing from security and resilience investments.
[9] Company 19

# 2 Research introduction and background

## 2.1 Introduction

After the attack to the World Trade Center and the Pentagon on September 11, 2001, many firms are starting to realize that the threat of terrorism is affecting their ability to operate and successfully carry on their business. Not only have several firms been directly hit by the destruction of the Twin Towers (those having their offices inside those buildings), but also nearly all supply chains were affected by the closing of US airspace and by the slowdowns at the borders that immediately followed. Many manufacturing firms could not receive supplies on time and had to slow down or even stop production. Ford, for example, shut down five of its U.S. plants and production for the fourth quarter dropped 13 percent below the plan, partly because it could not get enough parts from suppliers in Canada.[10] It is important to note that the direct cause of such a vast disruption was not the terrorist attack itself, but the reaction of the U.S. Government.

The U.S. Government response not only affected business operations in the aftermath of the attack, but it is still influencing international shipments through new regulations and new initiatives intended to increase system security. By virtue of these efforts, the impact extends to all global firms conducting business across US borders. U.S. Customs is now strongly encouraging importers and freight carriers to certify their sources and assume responsibility for cargo security (Custom-Trade Partnership Against Terrorism).

To investigate the broad issue of how the threat of terrorism is affecting the supply chain, a comprehensive research initiative, "Supply Chain Response to Global Terrorism" was initiated and is currently under way at the MIT Center for Transportation and Logistics.

This report provides an initial review of the observations and findings to date on the project, with particular focus on how companies have been affected, and how they are now reacting and responding to the threat.

## 2.2 Background Research

Research on responding to terrorism so far has focused on many issues that can help provide useful insights on how to deal with the threat of terrorism, but only a few authors have focused directly on this specific issue for the supply chain. A full review of the relevant literature can be found in Appendix 1.

The limit of all the contributions is the scarce use of empirical evidence: some of the studies are purely theoretical and others are based on examples of reaction to past events, but none of them investigates the current corporate response. To this point there has been no clear assessment of the actual preparedness of companies to supply chain disruptions, and its not clear that the road map to change is yet defined for increasing security and resilience.

[10] Andel, 2002, Martha and Subbakrishna, 2002

## 2.3 Project Overview

As noted above, this research project was initiated to investigate how terrorism and the threat of terrorism are affecting supply chains. The project is entitled "Supply Chain Response to Global Terrorism" to recognize that there have been a number of different responses which affect a firm's ability to handle disruptions such as terrorism.

To fully appreciate the impact of the responses on the firm and its supply chain, the project scope initially entailed studying the response to terrorist attacks (and similar disruptions) from several different perspectives: the risk management community and insurance industry response, the U.S. Government response, the response from shippers and carriers and agents along the supply network,[11] the experience of past disasters, and the use of real options[12] to assess the potential value of flexibility in supply chain design in responding to disruption.

The research to date has included a broad literature review from these different perspectives as well as base interviews with 20 firms (primarily shippers). The data from the interviews and literature review were synthesized and analyzed into this body of observations and insights. A more detailed review of the methodology and limitations on the use of the data is included in Appendix 2.

# 3 Context of the Corporate Responses

To fully appreciate the response that firms are making, we sought to understand the environment in which the firms were operating. This provided a better understanding of the issues that the firms were addressing and hence the actions that were being taken. Two main aspects of the environment were studied, including the insurance industry response and the government response (as it relates and affects business operations and commerce).

## 3.1 Insurance Industry Response

### 3.1.1 Insurance Coverage

One initial area of research explored the response from the insurance industry. Regarding insurance policies covering corporations from losses resulting from terrorist attacks, a relatively immediate commercial response was the modification of existing policies at the annual renewal point, many of them on January 1, 2002. The modification entailed rate increases, reductions in coverage (higher deductibles and lower overall coverage), and in some cases discontinuation of coverage.[13] Data from the interviews with firms confirmed this, revealing that few if any of the interviewed companies rely on insurance for protection on losses arising from terrorist attacks.

[11] The terms shippers and carriers are common in the logistics field but may need clarification. A shipper is a firm that produces a product and which hires a carrier to physically move the product to a downstream firm or user. Carriers include firms that transport products using rail, air, ocean, and land-based modes. They can be asset-based or non-asset based firms.

[12] Ibid., this research is being conducted by Prof. Richard de Neufville of MIT. For additional information about this subject matter, refer to <http://ardent.mit.edu/real_options>

[13] While the Terrorism Insurance Act of 2002 may oblige insurers to offer insurance, it does not mandate the rates or coverage offered.

As of early 2003, it appears that 'expert judgments' are the basis for most terrorism insurance premiums, and the result is that these policies are prohibitively expensive. As an example, Delta Air Lines terrorism insurance premiums increased from $2 million in 2001 to $152 million in 2002. [14]

This is an example of how firms have not resorted to extensive financial investments to protect their business without a quantified business case to support the investment. In this case, firms elect not to purchase insurance coverage even when it is available because the cost-benefits tradeoff does not warrant such an investment based on the assessment of the risk (the probability of loss and the potential loss or impact), the assessment of the costs, and the assessment of the benefits of various investments. This raises the important issue: how can the firm assess the risks, costs and potential benefits to make rational business decisions?

### 3.1.2 Insurance Industry Risk Assessment

As suggested above, firms need to assess the risks, costs and potential benefits of investments in order to make informed business decisions. The insurance industry remains dedicated to using actuarial methods for assessing risk, and at this point industry leaders indicate there is not enough data to make informed assessments yet, even at industry level, estimating that it could take several years to develop the means to provide coverage. [15] For the firm, this provides no useful insight given that the limited number of incidents makes it impossible to use actuarial data to truly assess the risk of terrorist attack on any particular firm that has not experienced an attack in the past.

Leaders in the risk management community have developed some modeling tools to help provide some insight on the likelihood of attacks. These models are high level and are focused more on assessing the likelihood of an attack by a particular militant group rather than an assessment on a particular business. Crude assessments have been done based on property characteristics – property symbolism/cache, proximity to hazmat material facilities, and proximity to large populations to cite a few – although these do not provide deep insight and utility to the majority of firms, which do not own trophy properties in downtown areas or near nuclear power stations for example.

Most firms have developed their own methods for assessing risks, although the majority of firms have not yet translated this into quantifiable business impact. Nearly every firm conducting some sort of a risk assessment uses a different method, with a majority of the assessments falling short of truly quantifying the impact. Effectively, qualitative assessments dominate the analysis, likely resulting in fewer investments to respond by virtue of failing to make the business case for investments. (See section 4.4.3 for examples of quantified risk assessments).

### 3.1.3 Summary – Insurance Industry & Risk Management Response

In summary, securing insurance coverage so far has not been a viable or common response for corporations to the threat of terrorism, no matter how serious the threat is perceived by the firm. Processes and tools to assist firms in risk assessment do not appear to be broadly

[14] Written testimony of Leo F. Mullin, Chairman and CEO of Delta Air Lines, before the Senate Commerce Committee October 2, 2002. Page 8.
[15] Martha, J. and Vratimos, E. "Creating a Just-in-Case Supply Chain for the Next Inevitable Disaster" MMC Views, Viewpoint, Autumn 2002

available, aside from actuarial methods and some higher level tools that may be useful at a national level but which are not productive at the firm level. It appears that firms are not making significant investments into responding, and an initial hypothesis is that the firms lack useful and productive tools to assess the risk of loss, the probability of loss, and the potential impact on the customer.

## 3.2 U.S. Government Response

The U.S. Government has taken a number of actions in response to the terrorist attacks on September 11, 2001. These actions can be broadly characterized as fiscal, legislative, memorial, operational policy development and organizational. For purposes of this research initiative, the focus is primarily on those fiscal, legislative, and organizational actions taken that affect business operations and commerce.

### 3.2.1 Infrastructure & Interdependencies

Managing supply chains entails managing the three fundamental flows of the supply chain: materials, information and funds. Given this, public infrastructure plays an integral role in supply chains for the unimpeded movement of each of these flows. These examples illustrate the dependence of supply chains on public infrastructure:

- Materials, from raw materials to finished products, move by air, ocean, road, and rail. Government organizations (federal, state, and local) play a leading role in the development, maintenance, and regulation of each of these modes.
- Information is captured either in paper form or electronically. When captured on paper, the information moves effectively like a materials move (although there are fewer customs concerns and constraints on paper movements as there are on physical material movements). When the information is captured electronically, it is typically transferred over a series of computer and telecommunications systems, portions of which are not owned by the companies sending or receiving information, and portions of the telecommunications systems are regulated by governmental agencies.
- Funds, like information, may move in either paper form or electronically. For the purpose of this work, funds flows are electronic and are hence dependent on distributed computer and telecommunications networks.

The infrastructure that supports these movements of materials, information, and funds also depends on energy. Hence, in a second order relationship, government actions, investments, policies, and regulations related to energy may also influence the availability or reliability of other infrastructure and systems that will affect supply chain flows.[16]

Hence, the dependence of supply chains on public infrastructure and systems coordinated or effected by the government represents a newly appreciated vulnerability for businesses, now more heavily dependent on the government than previously recognized.

[16] Although not a focus of this research, these infrastructures have been targeted as vulnerabilities by the government and in response, Information Sharing and Analysis Centers (ISACs) have been established for the most important infrastructures to facilitate coordination and emergency response. Additionally, several other initiatives and organizations have been established by the government focused on infrastructures, including the Critical Infrastructure Assurance Office and the National Infrastructure Protection Center.

### 3.2.2 Organizational – Department of Homeland Security

As suggested previously, the most prominent action taken by the U.S. government recently has been the creation of the Department of Homeland Security (DHS), a cabinet-level organization with nearly 200,000 employees, and a $36.2 billion budget for 2004. This was accomplished by bringing together 22 previously separate government organizations, thus representing the largest federal reorganization in fifty years.[17]

Overall, the new Department is beginning to develop its internal operations, and there is the potential that there will be greater collaboration among the various agencies than there has been in the past. Most important to infrastructure and supply chain operations, DHS includes the U.S. Customs Service, the Transportation Security Agency, and the U.S. Coast Guard along with several infrastructure-protection and numerous other relevant agencies. It is these specific groups and their associated legislation that have had the most tangible impact on supply chains.[18]

### 3.2.3 Operational Policy – Initiatives with Industry

The government has initiated several programs and efforts intended to support the improvement of materials flows via improved security and systems across the supply network for US businesses. Most notable are the Customs-Trade Partnership Against Terrorism (C-TPAT), Op-Safe Commerce (OSC), Container Security Initiative (CSI), and Free and Secure Trade (FAST) Programs.

The U.S. Customs Service and seven leading importers established the Customs-Trade Partnership Against Terrorism (C-TPAT) in April of 2002. Founding companies include: Ford Motor Co., General Motors Corp., Motorola, Sara Lee, Target, BP America, and DaimlerChrysler.[19] One main goal is of C-TPAT is for "businesses to ensure the integrity of their security practices and communicate their security guidelines to their business partners within the supply chain."[20] Originally limited to the first 2000 applicant businesses, over 3000 are said to be in the various stages of application for C-TPAT compliance. C-TPAT basically provides guidelines for companies to self-assess supply chain security related to the following areas: procedural security, physical security, personnel security, education and training, access controls, manifest procedures, and conveyance security.[21] C-TPAT compliant firms will be able to move products through US Customs operations with less inspection and will therefore pass through more quickly (some estimate a difference of 2-3 days for C-TPAT compliant firms to 10-12 days for non-C-TPAT firms).

For reference, one firm has estimated the initial and ongoing cost for C-TPAT compliance. Hasbro, a global leader in the toy industry spent approximately $200,000 to become C-TPAT compliant, and estimates that future expenditures will be $112,500 annually. For perspective, Hasbro revenue for 2001 was $2.9 billion and the firm is #45 in the U.S. for container import

[17] Figures and quote from Department of Homeland Security web site: www.dhs.gov
[18] See the appendix for additional details on the new Department of Homeland Security and relevant Directorates.
[19] "US Customs, industry team up on border security." CNN web site: www.cnn.com 4/16/02
[20] "C-TPAT Frequently Asked Questions and Fact Sheet." Customs web site: www.customs.gov
[21] "Trade Security: A Wildcard in Supply Chain Management." ARC Advisory Group. Sept. 2002. page 9.

volume.[22] (Almost 21 million containers arrive annually in the United States by ship, truck, and rail.[23]) Additional work is required to determine whether these costs are representative across industries, but in the least we can say these are not inconsequential additional burdens on the business.

The U.S. Customs Container Security Initiative (CSI) was launched in early 2002 to increase security for the maritime trading system by focusing on the top 20 ports by volume of cargo containers shipped to the United States.[24] By early 2003, only 11 of these top 20 ports had agreed to participate. The Container Security Initiative has four primary aspects:

1. Use of automated information to identify and target high-risk containers.
2. Pre-screening high-risk containers before they arrive at U.S. ports.
3. Use of detection technology to quickly pre-screen at risk containers.
4. Use of more sophisticated, tamper-resistant containers.

This is an ambitious initiative, the success of which is largely dependant on availability of accurate advanced information and successful coordination by a large number of ports, agencies, companies and governments.

Operation Safe Commerce (OSC) is a public/private partnership launched in 2002 by the Department of Transportation (DOT) and Customs. The goal is to "…provide a test-bed for new security techniques that have the potential to increase the security of container shipments."[25] One early pilot has been completed – the tracking and monitoring of a test container from origination to destination. This test made sure the container was routed as planned and stayed sealed at all times.[26] Pilot projects with the three largest U.S. ports (Los Angeles/Long Beach, New York/New Jersey, Seattle/Tacoma) have received funding and are in the early stages of development.

The Free and Secure Trade (FAST) Program is a bilateral initiative between the United States and Canada to allow clearance of low-risk shipments. There are three components to FAST processing:

1. Importer Registration: this includes completing applications to customs agencies in both the U.S. and Canada, complying with relevant laws and regulations, and participating in C-TPAT.
2. Carrier Registration: this includes completing applications to either Canada or the United States, or both (carrier decision). The application includes a security profile and risk assessment. Carriers will also be C-TPAT compliant.
3. Commercial Driver Application: Drivers must complete an application for review by both the United States and Canada, then be interviewed, fingerprinted, and have a digital photo taken. Qualified (low-risk) applicants will receive a FAST-Commercial Driver Card.

As of March 2003, FAST processing was available at 6 major U.S./Canada border crossings.

Smart and Secure Trade Lanes (SST) is an industry initiative being driven by three port operating companies, which account for 70% of the world's container port operations. This initiative utilizes the U.S. Department of Defense Total Asset Visibility (TAV) network. It

[22] Robert Fantini, Hasbro Director of Security, at CLM New England Round Table event. 3/13/03
[23] Schiesel, Seth. "Their Mission: Intercepting Deadly Cargo." New York Times. 3/20/03
[24] US Customs web site: www.customs.ustreas.gov 2/25/03
[25] US Customs web site: www.customs.ustreas.gov
[26] "Trade Security: A Wildcard in Supply Chain Management." ARC Advisory Group. Sept. 2002. page 11.

includes the use of automatic data collection through RFID, GPS, sensors, and scanning systems.[27]

Overall, these initiatives have a significant impact on business operations that move products into and out of the United States. Still in their infancy, these initiatives offer the potential of improved flows (smoother, higher levels of security), but there are many issues that need to be addressed for any potential success.

In addition to these initiatives, several other high profile efforts are worth mentioning although the impact on the supply chain appears to be negligible so far. The Transportation Security Administration (TSA) was established in late 2001 through the "Aviation and Transportation Security Act." TSA is responsible for the improvement of airport bag and security procedures. Due to the limited scope of this organization (i.e. covering a single mode of transportation, which happens to have the lowest volumes) it may not have far-reaching effects on most companies' supply chain activities.

The "USA PATRIOT Act" includes the acronym for "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism." This act was also passed in late 2001 and has an objective "to prevent terrorist financing and money laundering."[28] This legislation primarily impacts financial institutions.

### 3.2.4 Issues with Government Response

The government response had a more significant impact on commerce than the attack itself, and industry leaders seek to have a voice in planning emergency response and at the point of emergency response.

Several of the immediate government responses to the attacks on September 11, 2001 actually had a far greater impact on commerce and supply chains than the actual attacks. In particular, closing the US airspace and slowing down material flows across the borders affected supply chains far outside of the impact areas in New York City, Washington DC and Pennsylvania. (This was also the case with the U.K. Government response to the Foot and Mouth Disease as the travel restrictions imposed by the government damaged the tourist industry to a greater extent than the disease had on the animals).

While a gut-reaction may be to accuse the governments of overreaction, given the circumstances and the uncertainty at the time, it may not be unreasonable for political leaders to take what in retrospect may seem like extreme measures. Politically, it is far more tolerable for leaders to over react than it is to under react, and more importantly it is critical for leaders to build public confidence to avoid a panic reaction. Therefore, one can expect an extreme reaction may come from a government response, and hence firms should anticipate this and build their supply networks accordingly.

In addition to anticipating an extreme response from government entities, firms may also consider working with government agencies to review the potential consequences of various

[27] Ibid.
[28] "Trade Security: A Wildcard in Supply Chain Management." ARC Advisory Group. Sept. 2002. page 7.

responses, particularly 'extreme' responses. Given the stated dependence of industry on the government infrastructure, and based on the interviews and informal discussions held with the firms, it is clear the firms shared a concern regarding the government response to any subsequent terrorist act. These leaders called for a greater 'voice' for industry in the planning for the improved security and emergency response, and in the emergency response itself. As noted, we can expect an extreme reaction but one can argue that some of the initiatives to secure the material flows across borders and to improve security of containers have come at a significant economic expense, and that some of the initiatives could have been executed with better coordination between industry and government, with less waste (e.g. the cost to reinforce airline cockpit doors cost $240MM[29] and was mandated on cargo flights which do not carry passengers and therefore would not need reinforced doors). While there are many different initiatives to potentially integrate the government and industry, it's still not clear how industry could and should be represented in emergency response.

New Public-Private Partnerships are required but this will entail pioneering new territory.

Compelling reasons for government and industry organizations to coordinate are growing, especially as there is shared interest in improving the security and smooth flow of goods through the supply chain. The benefits of working together in preparing for future disruptions (due to terrorism, natural disaster, or other catastrophes) include avoiding duplication of efforts, avoiding actions and efforts that may adversely affect the other, and developing efforts that are mutually beneficial.

In addition to these shared interests, it is becoming evident that both the government and private industry are increasingly dependent on each other to achieve their respective and shared goals as well. The government is dependent on private industry to take several critical actions:

- To assess the security practices of each supplier in their respective supply networks
- To implement the various new security improvement initiatives (C-TPAT, FAST)
- To maintaining business operations that serve as the economic engine for the US economy[30]

While implicitly the government has been dependent on private industry in the past (e.g. the generation of tax revenues), these new dependencies represent step changes rather than incremental changes in the importance of the government – industry relationship.

Similarly, private industry is dependent on the government to provide several critical services:

- For smooth, efficient and fast flow of cargo through customs
- For security infrastructure investments in technology
- For robust and secure transportation, energy, and other relevant public infrastructure
- For rational, thoughtful emergency response policies and actual emergency responses to disruption

These represent an elevated role for the government in private industry, a contrast to the traditional private industry preference for less government involvement in business operations. In this environment of shared threat and network risks, it appears that private industry has higher needs to coordinate efforts with government agencies.

[29] Source – D. Disraelly

[30] The estimated $150B cost for the 10 day West Coast port lock out in October, 2002 illustrates how the economic impact of supply chain disruptions is significant.

These new interdependencies call for new relationships, which we refer to as new Public-Private Partnerships. Developing these new Public-Private Partnerships requires defining how these respective organizations will coordinate actions in the future. This includes fundamental governance issues:

- Scope – What is in the scope of the initiatives, what systems will the group work to develop?
- Coordination – How will new systems be coordinated?
- Ownership – Who will own the new systems?
- Control – Who will control the new systems? How will decisions be made and by whom?

Ultimately these issues will need to be addressed in order to make systems that work for both industry and government and that more importantly provide for higher levels of system performance.

This will be a significant challenge, bringing public agencies together to collaborate with private industry. Even the government's initiatives to coordinate among the various relevant agencies has fallen short of expectations and needs,[31] illustrating only one aspect of the coordination challenge ahead.

## 3.3 Role of technology

While this study did not focus on the use of technology, it is important to recognize that technology does play a role in making the supply network more secure and resilient.

There are a number of technology solutions related to security available – the Pentagon received over 12,000 proposals in the first 5 months after September 11[32] for starters. These solutions are almost exclusively "point solutions," however, only addressing single aspects or small ranges of supply chain management. Perhaps more importantly, the human element of terrorism and other intentional disruption seems to reduce the efficacy of technology.

Some of the solutions include the automation of the filing and exchange of import-related information, indicators, and sensors on containers to track 'chain of custody,'[33] and overall five technologies with potential application:[34]

- Sensors.
- Biometrics.
- Electronic seals.
- Loading integrity tools.
- Mobile communications platforms.

[31] A recent study and report issued by the General Accounting Office indicated that "Nearly 20 months after the Sept. 11 attacks, many federal agencies are still failing to share critical information …. with other agencies because of both cultural and technological barriers" from "Agencies Still Fail to Share Information, Reports Say" by Eric Lichtblau, The New York Times, April 30, 2003

[32] "Trade Security: A Wildcard in Supply Chain Management." ARC Advisory Group. Sept. 2002. page 12.

[33] Scott Kirk, EJ Brooks, presentation to CLM 3/13/03, electronic seals can record time, location, and container status.

[34] Michael Wolfe, North River Consulting, presentation to CLM 3/13/03.

With advances in economic and risk assessments, or identification of collateral benefits of security, the role of technology may become clearer or more justified.

## 3.4 Learning from past events

Although there is not a large body of data available on the impact of terrorism on supply chains, it may be possible to make meaningful observations of past supply chain disruptions, both man-made and natural catastrophes alike.[35] This may give further insight into a variety of prevention and response mechanisms. Possible events to analyze include, but are not limited to the following:

- The 1918 influenza.
- The 1995 Kobe, Japan earthquake.
- The 1986 Chernobyl nuclear disaster.
- The 1998 Quebec ice storm.
- The 1995 destruction of the federal building in Oklahoma City.
- The 2002 European floods.
- Other major weather disasters.
- Major labor strikes against either large companies or single industries.

This work has been recently examined in great detail as part of this research team's efforts, and the findings are reported separately in two theses published in June, 2003. [36]

# 4 Corporate Risk Assessment[37]

Companies interviewed illustrated the importance of risk assessment as one aspect of analyzing how the firm should respond. There are two dimensions of corporate risk assessment that were considered – risk assessment methodology and type of risk. These are reviewed in the context of the perceived threat.

## 4.1 Corporate Threat Perception

Most of the interviewed companies declared that the threat of terrorism to the supply chain is between "serious" and "very serious." There was little agreement on the most significant supply chain vulnerabilities, terrorism-based or otherwise, although the source of supply may be seen as a more common source of risk. Altogether, the most common vulnerabilities included manufacturing, availability of supply from international or sole sources, freight security, ports, and communication systems.

[35] Sheffi, Y. (2001), "Supply chain management under the threat of international terrorism", *International Journal of Logistics Management*, Vol. 12, No. 2, pp. 1-11.
[36] See theses by Reshma P. Lensing and Christopher Pickett, MIT Theses June 2003.
[37] Risk assessment may be considered one aspect of 'managing uncertainty', which is a broader concept and representative of a holistic approach to addressing the changes in the operating environment. Ultimately 'managing uncertainty' may be similar to proactive network design for resilience and security.

One conflict in the data was that while most of the respondents indicated a perceived threat as being serious or very serious, only a few firms actually took action to address this serious or very serious situation. zGiven the adage 'actions speak louder than words' we attempt to assess the perception by considering both the verbal assessment as well as the list of actions taken aimed at protecting the company and the supply chain. We believe this will be more reliable than the same assertion not supported by any initiative.

It is not clear why some firms perceive a serious threat yet do not take commensurate actions. Two potential explanations occur to us. One is that the firm may not be accurately assessing the risks to their specific supply network, and therefore the firm underestimates the risk. Secondly, it is also possible that the firm is much less exposed than other firms to industrial, geographical or any other specific risk factors. For example, those firms operating solely in the United States with no materials coming into or going out of the country are genuinely less susceptible to supply disruptions if the airspace or ports are closed at some point in the future. Also, firms that completely outsourced operations are less exposed to the risk of internal operation disruption (although they are potentially at higher risk for supplier disruption or supply disruption).

## 4.2 Corporate Risk Assessment Methods

Most of the firms interviewed performed some risk assessments, although almost every company used a different method, tool, or data set to assess risk. For example, some firms' risk assessment methodology illustrated an elaborate and generally comprehensive approach, while others described a more intuitive approach or did not provide any description of the method employed. This distinction suggests that the reliability and the comprehensiveness of the assessment performed can be very different, leading to a broad range in the accuracy of the risk assessment.

In many cases, the firms focus risk assessment on internal risks, rather than on supply chain or network risks, and the tools used are largely internally developed rather than commercially available. While the practices varied by firm, many of the firms indicated that there were different parties involved with assessing different risks, suggesting that risk assessment was not always a centralized or coordinated process. Additionally, most of the assessments reflected a qualitative rather than quantitative process.

Given that the firms are exposed to vulnerabilities outside the auspices of the firm (risks associated with the other firms in the supply network), a more formal process to assess the network risk seems appropriate. Comparing this need with the data collected, the existing methods and tools fall short of a desirable and robust system for risk assessment. Specifically focusing on internal security and operations does not address the aforementioned dependence on infrastructure or the external supply network system. [38]

[38] "How far should business go to protect itself against terrorism?" Strategic Management Wharton. 2/26/03. Additionally, the private sector owns or operates approximately 85% of U.S. infrastructure

### 4.2.1 Examples of Risk Assessment Methodologies

Several examples of the risk assessment methodologies illustrate the range of qualitative to quantitative methods. The majority utilized qualitative measures that did not clearly connect to a business impact. These examples illustrate the more quantitative methods observed.

In lieu of focusing solely on the risk of a terrorist attack effecting their business or supply network, some firms[39] instead considered the impact of a terrorist attack as one of many different types of disruption. These firms noted that the impact of a terrorist attack (direct or indirect) was similar to the impact of other sources of disruption (both a tornado and a bomb blast have a similar effect on the operations – a delay or loss of capacity to operate/produce). By aggregating the risk associated with various sources of disruption, these firms noted the ability to detect patterns of disruption that could then be considered in subsequent business continuity plans. The most progressive perspective on this was shared by Rob Carter, EVP and CIO of FedEx:

> "Predictability around the inevitability of event-based disruptions is the key. Things happen every day in our networks: weather, maintenance, FAA issues, air traffic delays, global turmoil, etc. The key to running a predictable network is to expect these events and be able to respond to them."[40]

Effectively, FedEx recognizes disruptions as part of an inevitable pattern of disruptions that the firm should prepare for, rather than be surprised by it.

Another interesting method entailed analyzing and quantifying the potential impact of the disruption by measuring how soon the disruption would affect the customer, basically using a customer service measure to drive the assessment.[41] The risk of the disruption at the customer is then categorized into low, medium or high level, enabling the business leaders to make more informed decisions on how to deal with the risk. This offered a useful clarification of the risk as illustrated by one firm that noted a one-day disruption might not impact the customer until two days later. This provided great relief to the firm by allowing the response team to use the defined time period – up to the entire 48 hours – to focus its efforts on taking appropriate measures to regain capabilities, avoiding knee-jerk measures to solve the problem 'as soon as possible.'[42]

Some companies used less quantitative assessment methods but still succeeded in identifying the impact of the risk on the business. In one case, the firm indicated that a significant disruption would result in 'losing the franchise'[43]; in another case, a major disruption to the supply chain would jeopardize the ability to meet a time-specific market opportunity (e.g. 'back-to-school' or holiday sales periods). Despite not being entirely quantified, these potential outcomes provided convincing arguments to executives and represented the threat as relevant.

[39] This is in particular the case at company 19, somewhat at company 4 and subsequently articulated by FedEx (although FedEx was not a participant in the study)
[40] From informal interview and exchange between R. Carter and J. Rice, April 30, 2003
[41] This is in particular the case of company 17 and company 18.
[42] Company 18
[43] Representative from company 15, Regional Security Manager – he tells the SBU the potential impact and asks if they want to risk not having their product on the shelf for an extended period of time, which apparently is enough to motivate the SBU or product category leaders to fund security measures significantly

One final example illustrates fatalistic approaches. In attempting to assess the risk, some firms had difficulty in assessing the probability of an attack. In some cases, the firms considered the impact as recoverable; in other cases, the firms believed that the impact would have equal impact across the industry and competitors. In these cases, the firms elected to take no or very limited actions.

The wisdom we may derive from reviewing these more quantitative examples is captured in this simple quote from one respondent: "Ultimately, you need to tie risk to business performance."[44]

## 4.3 Types of Risks Considered

Most firms primarily considered a traditional set of risks (such as risk of natural disaster, fire, theft), and the risk of a terrorist attack proved to be a difficult risk to consider for many of the firms. Only a few of the firms addressed the risk of specific terrorist or cyber attacks, and consistent with the previous assessment of the process, the methods and tools to assess risk of terrorism are lacking. The general opinion of interviewed firms was that company facilities are an unlikely target for terrorists, although data indicates otherwise. Since 1968 when the federal government first started tracking terrorism, 80% of attacks on U.S. interests have been on businesses,[45] making the risk of attack on business the likely target. The probability that any one particular business may be attacked is appreciably lower, although there were no defined ways to assess this. The failure modes are briefly summarized in the Table below.

*Table . Basic Supply Network Failure Modes*

| Failure Mode: A Disruption in … | Description |
|---|---|
| …Supply | Delay or unavailability of materials from suppliers. |
| …Transportation | Delay or unavailability of the transportation infrastructure or various modes. |
| … Facilities | Delay or unavailability of plants, warehouses, office buildings, facilities used in converting products. |
| …Communications | Delay or unavailability of the information and communication infrastructure. |
| …Human Resources | Delay, loss or unavailability of human resources to continue operations. |

### 4.3.1 Focusing on Failure Modes

As suggested above, rather than focus the risk of a terrorist attack, the firm may aggregate the various sources of disruption and instead analyze the risk of disruption. Hence, while there are many different types of risk, there are but a limited set of potential outcomes or impacts from any of the various risks. The term 'failure modes' was used by several firms[46] to connote this limited set of outcomes, effectively the few ways that the system could fail, regardless of the actual source of the disruption. Each failure mode could be generated by

[44] Company 19
[45] Ambassador L. Paul Bremer, Chairman of the Crisis Consulting Practice at Marsh, Washington D.C.
[46] Company 8

different causes, but the effect on the supply network is the nearly the same (e.g. the previously mentioned comparison between a bomb in a plant and a tornado); the slow down of goods entering the U.S. after September 11 was not very different from the impact of the 1998 Quebec ice storm on Canadian imports or the west coast port lockouts in October 2002.

'Failure mode' focus makes for a much more manageable process to develop continuity plans only because there are far fewer eventualities to consider. This approach is particularly appealing because it allows the firm to exploit the similarity between traditional and new threats, leveraging existing tools to both assess risk exposure and reduce the vulnerability. Perhaps the most significant contribution of this approach is its power of synthesis: despite the high number of threats and possible sources of disruption, the relevant failure modes are just a few, and they will probably remain the same even if new menaces appeared.

The supply chain failure modes, or vulnerabilities, can be more or less critical for a company, depending on a series of factors, such as the industry, the business model, the geography, etc. This section expands on the failure modes that emerged from the interviews (introduced in the above table):

1. **Disruption in supply:** Some firms companies perceive the availability of raw materials and parts as the most vulnerable aspect of their supply chain, since a disruption could lead to the stop of production, with major consequences on the whole business. This is particularly true for companies operating on a lean supply/just in time base[47], since the absence of inventory limits the time the firm has to respond before a disruption has direct affect on customers. The possible causes of disruption could be many: a natural disaster that affects the area where the supplier is located, a fire in the supplier facility, a terrorist attack, or even the supplier going bankrupt.

   A notable example of a disruption in supply is the Philips Electronics radio frequency chips shortage that resulted from a 10-minute fire spawned by a lightning strike and which eliminated over a month's supply of RFCs. Two customers, Nokia and Ericsson both depended heavily (sole source) on Philips for these chips in their cellular phone products, but only Nokia responded quickly to replace the supply. Ericsson responded late and by their own estimates lost over $400MM in revenue, and ultimately they got out of the cellular phone production business.

   Other examples of disruptions in supply include the notable 1999 Taiwan earthquake that disrupted supply of high-tech components, the 2001 unexpected bankruptcy filing of key chassis supplier Thompson to Land Rover, and the 1998 Hurricane Mitch which disrupted the supply of bananas to Dole and Chiquita.[48]

2. **Disruption in transportation**: Supply chains rely on the continuity of raw materials, parts and component flows, and a disruption in the transportation services could severely affect the continuity of operations. In particular, firms that rely on international shipments in general are more exposed to this danger, as the reactions to the September 11 attacks (closed airspace, border slowdowns) and the October 2002 West Coast lockout (delays in flows through West Coast ports) illustrated for firms dependent on inbound materials. Firms interviewed largely shared more concern for

[47] Company 1 is a good example of lean operation that relies strongly on continuity of supply
[48] "Strategies for Maximizing Supply Chain Resilience: Learning From the Past to Prepare for the Future" MIT Thesis by Christopher Pickett, June, 2003

inbound flows and less concern for outbound flows. One explanation is that a disruption in transportation for inbound materials will more likely result in additional disruption in supply, whereas a disruption in outbound material/product flow is less likely to have an affect on internal operations. Additionally, it is generally true that there are multiple choices for outbound flows (including various modes, routes, intermediaries, channels, distribution centers, points of sale, etc.) therefore providing for multiple choices in the case of disruption in one mode.

The interchangeability afforded by the different transportation alternatives provides no comfort however, when the disruption is a systemic disruption such as closure of airspace and border slowdowns ordered after the September 11 attacks. In this case these constrained all international inbound shipments and firms companies could not arrange alternative cross-border emergency shipments for some period of time. Ford Motor Company was forced to shut down five of its U.S. plants, and the production of the fourth quarter dropped 13 percent below the plan.[49]

3. **Freight breaches**: Another failure mode is the case where the integrity and security of the freight being shipped is adulterated. Traditionally the concern has focused on preventing theft[50] or product tampering, but today companies are broadening the scope, considering the possibility of terrorists manipulating goods while in transfer. This could include, for example, the introduction of weapons or people into containers, or the adulteration of products for criminal purposes. This form of vulnerability is considered a priority for two distinct groups of companies: on one side there are freight carriers, who are responsible for the safety and integrity of the goods transported; on the other side there are those industries, such as food and pharmaceuticals, whose products are particularly sensitive to the risk of tampering[51]. While the perception of the threat appears increased for freight carriers compared to the past, the food and pharmaceutical industries have always been concerned with these problems, due also to past events of product adulteration (e.g. the Tylenol case), and thanks to the already very strict regulations and control.

4. **Disruption in production facilities (internal):** Asset-based manufacturing firms often incorporate both high-value assets and most of their value-added activities in their facilities. For these firms the highest vulnerability often resides in their assets, as these represent the source of the firm's ability to generate revenue that may not be easily or inexpensively replaced. This is particularly true for firms with very specific and valuable assets, such as proprietary technologies and one-of-a-kind plants[52].

   A recent example a disruption in production can be found in the disruption that Procter & Gamble suffered when a tornado tore the roof off a manufacturing facility and downed trees blocked vehicle entry and exit to the plant as well. Six weeks of finished goods inventory of potato and corn chips provided a buffer, but the firm expected the disruption to reduce monthly revenues by 1%, and elected to use the

[49] Martha and Subbakrishna, 2002.
[50] This is particularly true for high tech companies but also CPG companies have similar concerns
[51] This is the case of companies 6, 3 and 15 in our sample.
[52] The best example is company 2, but also 8 has a similar concern, given the high value of its equipment.

only other manufacturing facility located overseas as a source for supply.[53]

5. **Disruption in communication/information flow:** The widespread adoption of e-commerce and a variety of Internet technologies have resulted in many more electronic communications and transactions. Hence, information systems and the information itself play a critical role for all business operations and for supply chains in particular, but in some cases they become the most important asset and consequently the highest vulnerability. This is particularly true for non-asset based companies that rely on outsourcing manufacturing[54] where the value-add is through coordination among a complex network of suppliers, contractors, carriers and customers.

   Disruptions of information systems recently have often been associated with one of two different types of cyber attacks. Cyber attacks can either be attacks on the data in the system or on the system itself (often resulting in denial of service for web based service systems). In both cases, the attack serves as a disruption to communication that can cascade into other disruptions in the business operation and supply chain when the service or product is dependent on real time system operation to perform. As an example, the recent SQL Slammer virus (January 2003) was a denial of service attack that shut down Bank of America's Automated Teller Machines because the tellers depended on information system availability to access account information and funds.[55]

6. **Disruption in Human Resource Capacity:** Several firms cited the (temporary or permanent) loss of human resources, either with specialized skills or a large number of personnel, as both a risk and failure mode for consideration. Such a loss could be the result of terrorist activity using chemical or biological agents, union activity (strikes), or natural disasters and viruses. The latter has gained even greater visibility with a 2003 SARS outbreak in Eastern Asia that idled some high tech contract manufacturers.[56]

Assessing the risk of a terrorist attack or even of a disruption entails considering a broad range of possibilities. Assessing the impact of these various disruptions entails a much more manageable process by focusing on these limited number of 'failure modes' to guide subsequent management action.

### 4.3.2 Modeling Risk of Terrorism Methodology

It is important to note that modeling the risk of terrorism for any entity – a person, a company, or even a government – is not considered possible using traditional (e.g. insurance industry) methods that are probabilistic, deterministic, or actuarial-based.[57] This is due to both the lack of historical data and the nature of human beings who may or may not act rationally (i.e. are willing to engage in self-destructive behavior). Additionally, because

[53] "Closing of Pringles Plant will hurt P&G sales" Cincinnati Post, May 9, 2003
[54] E.g. Companies 7 and 16 as companies that outsource manufacturing, or 11 as an EMS.
[55] "Historical Events and Supply Chain Disruption: Chemical, Biological, Radiological and Cyber Events" Reshma Lensing, MIT Thesis June 2003
[56] Severe Acute Respiratory Syndrome (SARS) became a worldwide issue in March of 2003. It is a natural and deadly virus. Motorola is one company that idled a production facility as a direct result of SARS.
[57] Numerous risk experts in articles, reports, and talks have articulated this challenge.

terrorists may modify their plans depending on the preventative actions taken by firms, the risk may not change although the targets might, further complicating the challenge of assessing the risks.[58] In addition to the various methods described in this report, other methods have been used.

One method that has been used is the theory of quantitative risk assessment (QRA) that seeks to answer three questions:[59]

- What can go wrong?
- What is the likelihood of that happening?
- What are the consequences if it does happen?

Finally, the Council of Logistics Management (CLM) white paper "Securing the Supply Chain"[60] included a comprehensive disaster classification profile with four dimensions:

- Primary cause: an intentional illegal act, an accident or a natural disaster.
- Agent responsible for disruption: biological, chemical, explosions, tampering, failures, extreme temperatures, tremors, water and wind.
- Magnitude of impact: severity, duration, scope, detect ability and frequency.
- Supply chain resource impacted: human, product, private physical infrastructure, public physical infrastructure, information, or financial.

## 4.4 Quantifying the Impact: Making the Business Case

A fundamental reason for risk assessment is to provide management with some data-based (ideally) input that could be used in business planning and decision-making. Hence, risk assessment will be most useful for the firm when the assessment quantifies the risk in ways that business leaders can understand. This amounts to translating the risk that a firm is exposed to into a financial assessment and specific business impact – basically making the business case for taking specific actions.

The lack of a clear business case is a barrier to the implementation of new supply chain security initiatives. Some respondents indicated that when people within the organization realize the magnitude of the threat and compare the costs with the potential losses, security would no longer be seen as a cost, but as a cost saving. Additionally, there is growing evidence that there are collateral benefits that accrue to the firm that has a more secure and resilient supply chain.

While the majority of assessment methods entailed qualitative methods, those firms that made quantitative assessments suggested they found greater success gaining support for investment requests (i.e. they made a successful business case). The importance of making the assessment quantitative was emphasized in the previously noted quote suggesting the need to tie risk and investments to reduce risk to business performance.

[58] This point was articulated by Prof. Yossi Sheffi in "Supply chain management under the threat of international terrorism", *International Journal of Logistics Management*, Vol. 12, No. 2, 2002 pp. 1-11.
[59] "Perspectives on the Use of Risk Assessment to Address Terrorism" by Dr. John Garrick.
[60] "Securing the Supply Chain" by Helferich and Cook, 2002

### 4.4.1 Cost or Collateral Benefit?

Securing the supply network and making it resilient will entail some measure of investment as part of a 'response.' For some firms, the costs are largely the expenses required to gain and maintain C-TPAT certification, whereas for other firms, the costs include the expenses and capital that may result from redesigning the supply network. These could include costs from modifications in supply arrangements (e.g. additional resources allocated to supplier qualification and management) and capital for technology investments. Many of the companies interviewed perceive these costs as a constraint to the further adoption of supply chain security initiatives.

The respondents demonstrated a range of opinions on these new costs: some perceived these as part of the cost of doing business, while others attempt to quantify and then balance costs and benefits. Only a portion of the interviewed companies performed cost/benefit analysis, and some of them only in a qualitative way. One problem is that most companies perceive the costs as clear and relevant, while the benefits as intangible and uncertain.

One respondent noted that the benefits are often in the form of avoiding losses, saying "nobody gets credit for solving problems that did not happen."[61] The benefits are difficult to measure if the avoided costs are not incurred. This reflects a challenge to the business to identify and value real savings from avoidance. Thankfully, this problem has been addressed in some measure by previous cost avoidance efforts such as lean production, total quality management, and customer service improvements.[62]

Additionally, many of the new costs are potentially related to other investments that will provide 'collateral' benefits, as suggested by this list:

- Investments in technology to provide real time awareness of business operations with visibility will benefit the firm with
  - Better process knowledge which will enable the firm to focus efforts on key improvement areas[63]
  - RFID (radio frequency identification) can help improve security by tracking and monitoring cargo movements, but also enhance shipment visibility which could then be used to reduce inventory investments and potentially increase service levels.
  - Improved control of the supply network
  - Less theft and IP loss
  - Ability to reduce inventory investments and other investments intended to provide a buffer against the uncertainty without visibility
  - Ability to make the supply network more efficient by exposing inefficiency (e.g. transportation linkages that require multiple handoffs could be changed for fewer handoffs and directed to have less time in waiting or exposed on the road where freight is most vulnerable)
- Investments in building organizational capabilities and awareness will benefit the firm with

[61] Company 17 voiced this opinion. This problem has also been recently addressed by researchers using system dynamics methods. See "Nobody Ever Gets Credit for Fixing Problems that Never Happened" MIT Research Paper, J. Sterman & N. Repenning, July 2001

[62] The article by Lee and Wolfe proposed applying total quality improvements to the security domain. Lee, H.L., Wolfe, M. (2003), "Supply Chain Security Without Tears", *Supply Chain Management Review*, January - February.

[63] Company 18 determined it had 48 hours to respond to a disruption which allowed the firm to plan for less expensive 2-day service rather than the more costly next day service in responding to disruption.

- Better collaboration beyond the initiatives of the last decade (e.g. VMI, CMI, EDR, QR, JIT, JIT II, CPD, CPFR, etc.) to facilitate practical and effective implementation and coordination between firms in the supply network
- Awareness of and experimentation with new supply chain design alternatives (alternative shipping methods, alternative suppliers) that may provide new capabilities that the firm may leverage for advantage
- Increased flexibility to accommodate traditional variation in demand and capacity, made known and developed via joint emergency planning and testing
- New ability to recognize other risks that could affect firm operations (e.g. one may argue that officials in Toronto sensed SARS rapidly largely due to being aware of and sensitive to bioterrorism attacks, even though SARS is not recognized as bioterrorism)

- Investments in building resilience into improving supply chain operations may benefit the firm with
  - Ability to operate with fewer resources and assets as the existing ones become multi-purpose via added flexibility
  - Ability to accommodate wider ranges of demand fluctuation with a dedicated flexible workforce
  - Ability to produce broader array of products, extending the ability of the firm to serve wider markets as desired

With additional study, it is likely that this list would expand and evolve with meaningful and practical examples of collateral benefits deriving from security and resilience investments. It is possible that additional study may reveal that, like Phil Crosby's assertion about quality in the 1980's, security and resilience are free.[64]

### 4.4.2 Who pays and who decides 'standards of care'?

The costs of security and resilience have not been fully identified and defined to date. Moreover, the whole economics of security and resilience is still unclear, calling for advances in this field to aid practitioners and policy planners as well. Given all these uncertainties, this makes it difficult to clearly identify 'who pays.'

Carriers' costs are more clear and therefore are easier to separate out since they are step functions (e.g. new technology costs, more shipments, longer time in transit for shipments so shipment cost is higher), whereas suppliers' costs are more integrated into the firm and incremental (slightly more inventory, additional time and effort required to assess suppliers, monitor their performance, develop additional sources as necessary).

System-wide cost estimates were not available via the interviews, but there are some technologies and investments that should be made in the system rather than by the individual firm in order for the investment to be productive. For these system-wide costs, it would be difficult for the individual firm to drive implementation across the industry (unless the firm is large enough and powerful enough to mandate standards), and therefore it may be necessary for an industry response rather than just a corporate response.

Overall, the respondents generally agreed that additional supply chain costs resulting from the threat of terrorism would be passed through to end consumers, although this is not

[64] "Quality is free" Phil Crosby. Lee and Wolfe in "Supply Chain Security without Tears," from Supply Chain Management Review Jan-Feb 2003 recognize and note similarities between security improvement and quality improvement.

currently the case. For the present time, these additional costs are a point of contention between shippers and carriers. There are some efforts in the carrier community to charge for additional 'security' services, although these increases have not been universally accepted or adopted.

While the U.S. federal government is investing in infrastructure, no company believes that government will bear all supply chain security costs.

Standards of care

In some cases, the issue extends beyond the additional costs to the 'standards of care' that may define routes, driver requirements, handling procedures, security processes, and technology requirements deemed necessary to secure shipments. Various shippers and carriers groups have developed their own respective 'standards of care,' a positive indicator that these groups are taking security seriously. These efforts will likely serve to improve security in the long term once all the parties come to a common understanding on 'standards of care,' but at the present time, this is another point of contention between shippers and carriers as these standards haven't been reconciled or coordinated.

These efforts have yet to involve all the relevant parties from the network (shippers, carriers, agents, terminal operators, relevant government agencies such as the U.S. Coast Guard and U.S. Customs), and therefore room for improvement exists to improve system security and resilience. These efforts should be coordinated lest there begin a proliferation of different 'standards of care,' or possibly unfavorable terms and conditions 'forced' on the other party in the name of security or resilience. Rather, the shippers and carriers will benefit by collectively working to use their respective expertise and skills to develop higher levels of security for the entire network.

There are some efforts in the carrier community to charge for additional 'security' services, although these increases have not been universally accepted or adopted. While the U.S. federal government is investing in infrastructure, no company believes that government will bear all supply chain security costs.

### 4.4.3 Examples of Quantifying the Impact to Make the Business Case

Some of the notable examples of quantifying the impact are listed below. These illustrate various ways in which some of the firms quantified the risk in ways that business leaders could understand:

- One firm calculated a rough estimate of $50-100MM cost impact for each day of disruption in their supply network[65]
- Another firm identified 72 hours as the time from the disruption to the point at which the disruption directly affected the customer[66]
- Less quantified but still compelling for the business was one firm's assessment that certain disruptions will lead the firm to "lose the franchise" or miss a critical promotion point ("back to school")[67]

[65] Company 19
[66] Company 18
[67] Company 15

- One firm identified that a disruption to the production of a few products in the firm's broad product line would risk financial insolvency, precipitating a cash-flow crisis in the near-term[68]

## 4.5 Other Possible Risk Assessment Approaches

In summary, as mentioned, risk assessment is not yet a consolidated or truly scientific practice among firms, and the issues associated with terrorism-related risk remain unclear for many of the firms. There is a need for a deeper understanding of the nature of the risk and for the investigation of the most suitable methodology to assess company exposure.

It may be worthwhile to consider assessing the risk from a few different perspectives. Depending on the specific situation, the preparation and the response may be significantly different. Two possible dimensions of risk classification that have not been explored in great detail here include the following:

- Risk of impact from a direct attack Vs. Risk of impact from an indirect impact
- Risk of immediate Vs. Risk of delayed impact
- Risk of temporary impact Vs. Risk of permanent impact

These may by useful ways to analyze the risks that call for additional work and study.

A white paper chartered by the Council of Logistics Management on "Securing the Supply Chain"[69] prepared a comprehensive disaster classification profile with four dimensions that outline multiple potential ways to consider and assess the vulnerability of the supply chain. The four dimensions are:

- the primary cause (an intentional illegal act, an accident or a natural disaster),
- the agent responsible for disruption (biological, chemical, explosions, tampering and failures, extreme temperatures, tremors, water and wind),
- the magnitude of impact (severity, duration, geographical scope, detestability and frequency), and
- the supply chain resource impacted (human, product, private physical infrastructure, public physical infrastructure, information, financial).

However, our observations indicate that the sources of the disruption are less important for the supply chain than the effects, thus suggesting that further work is needed to reduce these multiple dimensions and narrow the multiple ways of assessing the risk to a manageable set of most critical factors to consider.

# 5 Corporate Response

While the initial investigation was focused on 'how to respond to global terrorism,' the findings and observations led to studying 'how to respond to supply chain **disruption**.' This broadens the scope of the research, but also allows one to identify the synergies between the response to the threat of terrorism and the response to a wide number of other supply chain disruption threats. This evolution also surfaced several aspects of response which we note as

[68] Company 18
[69] "Securing the Supply Chain" by Helferich and Cook, 2002

supply network security (and preventing major disruptions), and supply network resilience (and responding to major disruptions).

## 5.1 Network – and not Firm Level – Security and Resilience

Both resilience and security have become more clearly network problems rather than firm-level problems. While the firm cannot abdicate responsibility to create a secure and resilient operation, it is important to recognize the firm's dependence on the network for higher levels of security and resilience. The supply network is only as secure and resilient as the least secure and resilient party in the network. This is evident in the sad example of Pan Am flight 103 that crashed over Lockerbie, Scotland. The bomb that made its way into the plane did so not through a failure in Pan Am security, but through a failure in Malta Airlines' security that allowed the bag into the system. Pam Am failed to recognize the weakness of the system, and the result was tragic.[70]

## 5.2 Resilience ? Security

Equally important in assessing corporate response has been discriminating between security and resilience, noting that these are indeed different characteristics. One can think of supply network security in terms of maintaining the integrity of the product, in contrast to resilience which is "the ability to react to unexpected disruption and restore normal supply network operations." These are certainly different characteristics that will require different action plans to create and maintain. This distinction becomes important for the firm when making choices about making system improvements.

While security and resilience are unique characteristics, we have already noted that there are collateral benefits possible, which provides additional leverage to some investments. It is also possible that investments to improve security or resilience may adversely affect the other characteristic. As an example, one may choose to change from single source supply to multiple sources of supply for all purchased materials. While this could enable continuity of supply (resilience) if one supplier fails or is disrupted, it also increases the difficulty to secure the supply network with many additional suppliers. Hence there are tradeoffs that the firm should recognize when making design choices – in this case, resilience may be increased at the expense of greater security challenges and cost to secure.

One common aspect in designing for security and for resilience is the idea of creating a layered backup system that entails a series of security and resilience measures. Such a design does not require perfect implementation of each measure, and hence the system could be secure and resilient even though one of the layers may have been defeated.

> "The concept of a layered (security) system, in which multiple (security) features are connected and provide backup for one another, has a particular advantage. Perfect execution by each element in the system is not crucial, because other elements can compensate for human, technological, or other shortcomings, and, correspondingly, enhancements to one element can boost the performance of the system as a whole.

[70] Larder, Jr., George, "2 Libyans Indicted in Pan Am Blast" Washington Post, November 15, 1991, pg. A01

> Such systems, long used to secure communications and information systems, cannot be breached by defeating a single layer. Because the terrorist can find it difficult to calculate the odds of defeating multiple layers, some randomly interleaved, such a system can deter as well as impede terrorist acts." [71]

Ultimately, the firm ought to consider making design choices to improve both security and resilience. Recognizing that these are different characteristics will enable the firm to make more thoughtful choices about investing in the desired capability.

## 5.3 Supply network security

Supply network security has two primary aspects: physical and digital.

### 5.3.1 Physical security

Today, almost every firm is paying more attention to physical security of facilities and workplace safety than they were prior to September 11, 2001. This includes stricter compliance with existing policies and standard operating procedures, particularly access control. Examples include requiring employees to wear badges, monitoring all who enter facilities, hiring additional guards, enhancing security systems and performing more extensive background checks on potential employees. There appears to be greater emphasis on background checks with good reason. [72]

Even among the most security-conscious companies, effective screenings need to extend beyond the hiring process to include ongoing tracking and assessment of each employee and third party provider with security access. This requires careful record keeping for the firm to track potential threats from anyone with enough knowledge and access intent on defeating the security system. While this may seem extreme, such a procedure may have prevented a previously trusted third party from releasing nearly one million liters of raw sewage into local rivers from a wastewater plant in Australia. The offender was a contractor who installed the wastewater control system, and who was subsequently turned down for a position at the wastewater plant. In retribution, he used his knowledge of the system to penetrate the plant and release the sewage. [73]

For some firms, extensive background checks and monitoring personnel access are nothing new, especially for those firms that work closely with the military or that currently deal with hazmat materials. At other firms, increased physical security is a reaction to the general sense of higher exposure to danger. In certain companies the emphasis on physical security is due to past experience of breaches: one company had intruders enter a facility with guns [74]

[71] "Making the Nation Safer – The Role of Science and Technology in Countering Terrorism" Committee on Science and Technology for Countering Terrorism of the National Research Council, The National Academies Press 2002, p. 214

[72] E.g. Company 8; some suggest the most significant risk for firms exist because of 'the enemy within' – that is the employee who has access to the firm, its data and operations. This would call for more extensive background checks on new hires as well as recurring background checks on existing employees.

[73] See "Historical Events and Supply Chain Disruption: Chemical, Biological, Radiological and Cyber Events" MIT MLog thesis by Reshma Lensing, June 2003, pg. 46.

[74] Company 11 suffered a multi-million dollar loss in 1990 8 people with machine guns broke into a facility and stole materials and products

and steal products worth several million dollars, while others experienced the anthrax attacks of fall 2001.[75] Each of these different incidents led the firms to pay greater attention to physical security.

As noted previously, the respondents' general opinion is that company facilities are an unlikely target for terrorists, while freight is perceived as more vulnerable because it could serve both as a vehicle for introducing weapons or as a weapon itself. This has lead to greater emphasis on increasing freight security, supported with particular emphasis by the U.S Government. However, the interviewed firms, being largely shippers, have not made significant efforts in this direction. There is a high reliance on their logistics providers to ensure that freight is safe and secure.

### 5.3.2 Digital security

As noted previously, there are two types of attacks that have plagued digital security: attacks on the information system, and attacks on the information itself. Every day new cyber attacks on systems and data are perpetrated, ranging from Internet viruses to frauds, from intrusions into systems to data and identity thefts.[76] For example, Viruses such as Melissa, Code Red and the SQL Slammer have been global problems, and not only is the scope of such attacks broadening, but also the effects are becoming worse.[77] An October 2002 attack on Internet global servers was hardly noticed by individual users, but it was not far from bringing down the entire Internet.[78]

Corporate responses to date rely primarily on basic tools such as antivirus software, firewalls, passwords and similar measures. Companies are starting to realize that hardware and software are not enough if the people are not educated on the risk of cyber attacks, and specific training is now in place in many firms. Advanced solutions have been adopted so far only by a few companies, generally those who have higher concerns for data security, such as those working with the military or those in financial institutions.

Another issue is related to information exchange with suppliers, partners and customers in the supply chain: modern platforms allow a closer connection of the information systems and have become a fundamental tool, but they could also create new vulnerabilities. In fact, some companies now audit supply chain partners to check the security of their partner's IT/IS systems and procedures.[79]

Finally, digital security improvements will not depend solely on technology, as recent disruptions illustrate that management practices led to the failure of some information systems. The SQL Slammer virus of January 2003 actually was a virus that attacked an old problem that had a broadly available solution (a software patch) 6 months prior to the attack.

[75] Two companies noted their parent firm received anthrax alarms in one of its facilities and the corporation which led to a company-wide response.
[76] The number of reported cyber attacks[76] is increasing at a dramatic rate: from 252 in 1990 to 2,412 in 1995 to 21,756 in 2000 and 82,094 in 2002.
[77] See Thesis by Reshma P. Lensing, MIT MLog June 2003
[78] Ibid.
[79] Carnegie Mellon University's Computer Emergency Response Team's Coordination Center www.cert.org/nav/index.html

While the technology was available to prevent the disruption, the management practices failed to ensure broad implementation of known solutions.[80]

### 5.3.3 Summary security measures

The data from respondents suggested a spectrum of security measures were being utilized by firms. The table below summarizes supply chain security measures at the low and high end of responses (see section 6, 'Classifications' for expanded classification of the responses).

*Supply Chain Security Measures*

| | Basic Responses | Advanced Responses |
|---|---|---|
| Physical security | ?? Access control, badges.<br>?? Gates, guards, camera systems. | ?? Extensive background checks.<br>?? Vulnerability testing by outside experts. |
| Information security | ?? Hardware: firewalls, dedicated networks, etc.<br>?? Software: intrusion detection, antiviruses, passwords, etc. | ?? Audits of partners' IS security.<br>?? Education and training for IS security. |
| Freight security | ?? Inspections.<br>?? U.S. government initiatives (e.g. C-TPAT, Container Security Initiative, Operation Safe Commerce).<br>?? Cargo seals. | ?? Documented "standards of care," use of certified third parties, defined and vetted chain of custody.<br>?? Industry initiatives to establish standards of care with among shippers and carriers<br>?? GPS, RFID, e-seals, biometrics, smartcards, sensors, etc. |

We don't necessarily conclude that every company should adopt the advanced responses. Those that have done so among our survey sample are organizations highly exposed to risk, but other companies with less exposure could be sufficiently protected by the basic measures.

## 5.4 Supply chain resilience

In material science, resilience is the physical property of a material that can return to its original shape or position after a deformation that does not exceed its elastic limit. In organizations, resilience can be defined as 'the ability to bend and bounce back from hardship.'[81] Today, this word is widely used for companies, referring to the ability to react to an unexpected disruption, such as the one caused by a terrorist attack or a natural disaster, and restore normal operations. Adapting this definition to the supply network environment, we define resilience to be

"the ability to react to unexpected disruption and restore normal supply network operations."

In many cases, resilient companies are those that have actively engaged in business continuity planning.

[80] Ibid. Lensing Thesis
[81] Coutu D.L. (2002), "How Resilience Works", *Harvard Business Review* , May.

Response and its impact on strategy and competitive advantage

Respondents were asked whether their firm had changed its strategy as a function of the new awareness of heightened threat and vulnerability. While many companies perceive the threat as very serious, only one of the firms suggested it had changed its strategy, in terms of value proposition to the market. It is the case of an IT company[82] that provides both products and services, which did make changes to its strategy to compete on the basis of its ability to offer the most secure and resilient services. This is not surprising, given the above-mentioned awareness of the IT community of the risks they are facing in terms of both security and resilience. Two other firms were considering expanding their product offering by adding supply chain security and resilience services externally, given the expertise that the firms had developed internally.[83]

Considering the entire supply chain, strategic design choices can make continuity more achievable when major disruptions do occur. These strategic supply chain design choices depend on a variety of factors: industry, business model, company culture, customer requirements, government regulation, supplier capabilities, or geography. The situation scan highlighted how many different supply chain choices can be made in order to ensure continuity of operations. Some of these decisions were made after a major disruption affected the supply chain (e.g. a natural disaster), and proved helpful in the aftermath of September 11.

There is some potential for a firm to use its resilience as an advantage if it can respond more favorably to disruption than its competitors – this effectively entails being ready to take advantage of opportunities to serve your competitors' customers if the competitor fails to meet the customers' needs. However, if the disruption is system-wide (i.e. the disruption affects all competitors equally), the potential to gain advantage is likely to be limited (but not always).[84]

### 5.4.1 Achieving Resilience through Flexibility and Redundancy

Analyzing the various alternatives that firms have utilized to create resilience, we observe there are two principle methods to create resilience in the supply network. One entails achieving resilience through flexibility, and the other entails achieving resilience through redundancy. Each has different cost and service characteristics that are important considerations when designing for resilience.

Flexibility

Flexibility entails **creating capabilities** in the firm's organization to respond by using existing capacity that can be redirected or reallocated. Flexibility comes from investments in infrastructure and capabilities long before the flexibility is needed. These would include:

- Investing in and developing a multi-skilled workforce
- Implementing production scheduling systems that can adjust rapidly
- Designing facilities that can accommodate multiple products and rapid changeovers (e.g. single-minute exchange of dies)

[82] Company 13

[83] Company 2 noted that the firm has developed an interface between their systems and standard facial recognition devices. They plan to sell it also, they are entering the industry of security devices.

[84] One company (8) contracted for emergency transportation services from a dedicated mode if other modes and services are not available for a 48-hour period.

- Creating flexible supply contracts for time-specific supplier capacity increases (e.g. a commitment to increase supply by 25% with a 1-week notice).
- Designing products so that suppliers can be changed without affecting the product – i.e. enabling transparent supplier changes often accomplished by using commodity components, standardizing parts supply across multiple product lines
- Developing distribution channels and operations that permit the use of multiple transportation modes (i.e. designing products and shipping systems that can use air, ocean and land-based shipping modes).

By using flexibility, there would be no unused capacity and limited fixed costs, largely only variable costs when flexibility is used. (The fixed costs include the cost of maintaining an alternative supplier, the cost of having an alternative transportation mode available, and the cost of being able to shift production to an alternative site, for examples).

While flexibility is an efficient choice because there is no excess capacity that goes unused, it does require the firm to make choices about reallocating capacity (material, machine, human resources), basically making tradeoffs on which products would take priority in the event that one product or facility were disrupted. A compromise would likely be required somewhere in the system.

Redundancy

In contrast, redundancy entails **maintaining capacity** in the firm to respond, largely through investments in capital and capacity prior to the point of need. An important distinction is that the additional capacity may or may not be used – it is this additional capacity that would be used to replace the capacity loss of a disruption. Examples would include:

- Inventory
- Additional production lines or facilities in excess of capacity requirements
- Qualifying and maintaining multiple suppliers when there is a cost to qualify and maintain
- Committed contracts for material supply (paying for capacity whether used or not)
- Maintaining a dedicated transportation fleet

Unused capacity means fixed extra costs, which in turn means reduced efficiency. Despite the lower efficiency, redundancy would not require the firm to make the same kind of tradeoffs that flexibility would require.

The firm will likely choose a mixture of these alternatives, depending on various business- and industry-specific factors, and taking into consideration the different cost and service characteristics of flexibility and redundancy.

### 5.4.2 Business Continuity Planning

Broadly speaking, business continuity entails development of plans to be prepared to restore operations after an unexpected, major disruption occurs. This incorporates a variety of choices for the firm including the degree or level of resilience the firm desires, the use of flexibility and/or redundancy, alternative backup solutions, etc. The IT community has been dealing with service continuity for years, and the knowledge developed in this field is rich for reapplication to other domains such as the supply network. This requires some effort, as the

supply network community may not fully appreciate the need for business continuity as the IT community generally recognizes.[85]

The majority of the continuity plans developed today concern internal operations: the loss of a manufacturing facility, the evacuation of a building, or the restoration of operations and information systems. As already mentioned, however, resilience is not just IT disaster recovery or internal operations recovery but full, supply chain-wide business continuity planning and recovery.

Some of the more progressive firms have developed not only detailed plans for business continuity, but have also taken action to set up emergency control centers that are 'opened' once a disruption is detected. The emergency control centers provide a defined working environment, hierarchy, decision-making process and operating procedures for responding to disruptions. Effectively, this permits alternative ways to manage operations and coordinate communications in the event of a major disruption. A few firms have dedicated locations for these purposes, and for one firm with military customers, the emergency control center is an underground bunker.[86] At another firm, there are emergency coordination centers at each facility and two corporate centers,[87] the former to manage local disruptions and the latter to coordinate communication and manage corporate-wide problems (there are two corporate centers in case one of them is disabled).

For the progressive firms, they seem to recognize a value in planning for disruption. At one firm this is taken to extreme, where they expect that disruptions will occur each day and therefore contingency planning as most think of it doesn't apply, this is the normal business planning process for the firm. Explained by Rob Carter of FedEx:

> "Contingency planning is a bit of a misnomer since these events are really the norm, rather than the exception."[88]

For some firms, business continuity plans existed prior to the September 11 attacks, and now there is even higher awareness of their importance. One example of this higher awareness is at Morgan Stanley, which immediately evacuated its headquarters in the WTC on September 11, losing "only" 7 of its 2,700 employees. The firm continued conducting business in its three pre-arranged recovery-sites, and this was possible because the firm took significant action after the first WTC attack in 1993 to plan and train for subsequent attacks.[89]

As already mentioned, the vulnerability of the supply chain is not primarily related to the facilities, but to the flows of goods and information. The respondents illustrated a broad range of continuity planning being used across the supply network, although not consistently. Several firms have developed continuity plans to address disruptions in supply, some times involving their suppliers in the process, but more often working autonomously.

On the contrary, only a few of the interviewed firms have developed continuity plans to address problems in serving customers. One partial explanation that has been provided is that

[85] Company 17 has tried to learn from the IT community, but their experience indicated a need to show the rest of the organization that the issue was broader.
[86] Company 8
[87] Company 2
[88] Ibid, J. Rice conversation with Rob Carter, EVP, CIO FedEx April 15, 2003
[89] Coutu D.L. (2002), "How Resilience Works", *Harvard Business Review* , May.

the transportation of products to customers is seen as a commodity service: there are multiple modes available and multiple carriers for each mode. Consequently, it appears that companies are comfortable with the ability to deliver products, once they have been able to produce them.

### 5.4.3 Responses to Create Resilience by Failure Mode

Firms sought to create resilience through a variety of responses, which have been organized by failure mode. As the following list of responses illustrate, there are multiple choices available for the firm to create resilience in operations and information systems. The optimal choice for one firm may not be the optimal for other firms, as the choices reflect varying business needs, situations, and appetites for risk.

Appendix 7 – "Comparison Cases: Many Paths to the Same Destination" – provides several examples of how three respondents designed their respective supply networks in very different ways to accomplish similar objectives. As stated in the executive summary, the net effect is that these firms have created resilient and secure supply networks by using the same principles applied to their respective business situations, resulting in many different supply network designs.

There are advantages and disadvantages associated with each potential response, and these should be considered when designing the network. For reference, there is a table at the end of this section that presents a matrix of the responses showing advantages and disadvantages for each response.

**Resilience to disruption in supply**

When faced with a disruption in supply, respondent firms indicated they used second sources, sole sources, progressive management of supplier resilience, supplier capacity agreements, inventory policies, and product design modifications to create a resilient supply network.

Multiple/secondary sources: Some firms have elected to use multiple sources for direct materials as a method to improve resilience by facilitating supply continuity.[90] Obviously, multiple sources give the firms alternatives for supply, which protects the firm from losing all of its supply in the event of a disruption at the supplier. It does not guarantee full continuity of supply however, because the reduced or 'lost' supply from the disrupted supplier will need to be 'made up' by the other suppliers. This suggests that it may be prudent to also make arrangements for supplier flexibility agreements (see below) that would entail contracting with suppliers to increase supply by a certain amount within a specific time period.

This approach may not protect the firm against a disruption that affects a specific region if all of the suppliers are located in or near that region. For example, a terrorist attack could destroy the transportation infrastructure (highways, railroads, airports) in a specific location. If all of the suppliers were located in the general area such that they were all somewhat dependent on the same highways and railways, then the firm would still be at risk of complete supply loss due to one disruption. Therefore, the firm may benefit from considering the locations of the different suppliers (as well as considering the different production locations for suppliers that have multiple sites). Some firms have elected to maintain a

[90] Companies 2, 12 and 15

domestic source of supply in cases where the primary source is an overseas supplier and therefore protecting against international supply constraints.

In some situations, it isn't economically feasible to maintain multiple active sources because the cost to coordinate multiple suppliers is high compared to the perceived benefits of having multiple sources. In these situations, some firms identified secondary sources and made preliminary agreements for supply to enable the rapid shift of supply in case of need. This process will generally include evaluation and certification of the supplier, but not all firms can afford alternative sources of supply when the qualification and maintenance process requires large investments.

Single/sole sources: Several firms decided to utilize sole source supplier relationships in selected situations as a method to improve resilience by leveraging committed relationships with those 'known' suppliers. There were two distinct motivations for adopting this approach.

One motivation was driven by efficiency. Similar to aforementioned supply situations where the economics are driven by coordination costs, there are some supply situations where it isn't economically feasible to maintain multiple sources because the cost to qualify and maintain the suppliers is prohibitively high compared to the perceived benefits of having multiple sources. This occurs in industries where suppliers' parts[91] require significant application testing before being approved for use, such as medical instruments or aerospace products where part failure can result in risk to human life. It is simply less costly to maintain a single source of supply.

A second motivation was driven by effectiveness – that is to say that the firms believed that a sole source relationship would be more effective because of shared destiny and higher commitment from the supplier. The firms developed collaborative relationships that resulted in better coordination, alignment and awareness of their shared need for resilience and security.

In the cases where the firms sole sourced, the firm required that the supplier actively engaged and worked together to improve their collective resilience (and security). This entailed including the supplier in business continuity planning, requiring that the supplier develop and maintain a comprehensive business continuity plan. The firm supported this with regular site visits to the supplier to visually inspect and assess the supplier's capability to respond to potential disruption, along with processes that maintained an open and continuing dialogue regarding capacity, security and resilience of the supplier's operations.

Interestingly, the firms using sole sources of supply did not express concern about their vulnerability. The common explanation was that focusing on a single source of supply allowed them to become intimately familiar with the supplier's capabilities to respond to disruption.[92] Focusing on one supplier and developing that supplier's capability to respond actually increased the firm's confidence level in supplier resilience, and hence their own resilience.

[91] Company 8
[92] In particular companies 1 and 8

Focusing on a single supply source also provided an added benefit of allowing the firm to leverage all of its purchasing volume and all of its efforts to increase resilience, therefore developing a clear 'we're in this together' relationship with the supplier that serves to align the organizations.

Multiple Sources vs. Sole Source: Neither one of these approaches is always better than the other. As noted, some firms have decided that the costs and efforts to qualify, approve, and maintain multiple suppliers do not justify the benefits if there is a low likelihood of disruption. In other cases, sole sources suppliers are chosen in the product design stage to provide proprietary knowledge or technology.

The net pertinent result is that by their nature, additional sources may provide only single location risk mitigation, and may actually be less resilient and secure than a sole source that has greater capacity to respond to disruption. This should be determined on a case-by-case basis, keeping in mind these tradeoffs.

Supplier flexibility agreements: Flexibility agreements with suppliers – contractual arrangements for volume increases from suppliers – can provide resilience in supply where there are multiple suppliers. These have been used to supplement various supply arrangements with one or more suppliers. As an example, one firm has contractual agreements with all of its suppliers to provide supply capacity increase of up to 25% in one week's time, and 100% in 4 week's time.[93]

An alternative to formal contracts for additional capacity is arranging for this flexibility informally. One firm used informal agreements; basically open communications, mutual trust and careful assessment of the supplier's capacity to ensure supplier resilience.[94] In particular, the firm used 'quarterly capacity reports' via site visits to the supplier facilities to assess the supplier's capability to support the firm in case of a disruption. This also contributed to 'socializing' the suppliers to see resilience as important criteria for serving the firm.

Supplier capacity flexibility can also come via use of multiple sources, provided the firm can substitute suppliers if one supplier is not able to deliver.

Inventory policies: Some firms relied on inventory policies, replenishment rules, and safety stock as means to mitigate risks and ensure continuity of operations. Some firms, reposition inventory to fewer stocking locations and 'pooled risks' that reduce required inventory levels and hence the need for inventory and resupply.

Some firms evaluate inventory position for each component and adjust desired inventory levels as conditions change, determining a priori the number of days of supply desired in case of disruption.[95] Additionally, repositioning inventory to fewer stocking locations and 'pooling risks' can reduce inventory needs and hence the reliance on suppliers for resupply.

Effectively, this calls for the firm to identify a target disruption service level – the level of service that the firm desires to deliver when there is a supply network disruption. These

[93] Company 11
[94] Company 1
[95] Company 8 is covered for 5 days

service levels may vary by several factors, potentially by customer, product, or nature of disruption.

Product Design: Some firms consider modifying the product in design and components in order to make it possible to use standard, commodity components. This benefits the firm by reducing part costs and complexity, at the same time broadening the natural base of supply. This can be cost prohibitive to modify product designs for existing products.

**Resilience to disruption in transportation**

Firms indicated the use of multiple transportation modes, spot markets for transportation supply, collaboration with logistics providers, multiple distribution channels and direct shipments from contractors to create a supply network resilient to a disruption in transportation.

Multiple/secondary transportation modes: Firms currently using different modes for transportation expressed less concern with the disruption of transportation mode, exhibiting confidence in their resilience. Firms currently relying on the one mode however did not share this confidence, expressing greater concern about not having relationships with other providers.

In response, some firms reached out to other freight carriers to establish a foundation of a relationship, setting up agreements for capacity in case of disruption as well as actually using the alternative mode in order to have access in case of need. As an example from the literature, Chrysler used expedited truck service to move parts that were usually shipped by air[96] after September 11. Also, Continental Teves shifted from shipping products into the US via air to shipping via ocean carrier (interestingly, this required additional inventory to offset the longer transportation time). It remains to be seen whether carriers will be able to handle additional service requests from 'new' customers when there is a disruption of a certain mode. One may anticipate that the carriers may put a higher priority to serve the existing customer base.

Spot market: Instead of developing agreements or relationships in advance, some firms expect they will depend on spot markets for transportation capacity in the case of a disruption. These firms generally consider freight movement a commodity service, and accept the likelihood of paying a premium for transportation via a spot market. This assumes there will be adequate capacity in the case of a disruption, or that transportation providers would take capacity away from existing relationships and commitments in order to temporarily serve the more lucrative spot markets in cases of disruption. It would be useful to check these assumptions with carriers and some data analysis.

Collaboration with logistics providers: As suggested, in the event of a significant disruption to a transportation mode, capacity may become the constraint for firms. In this case, it may be useful to have a relationship with third parties or major providers in order to ensure continuity even during disruptions.[97]

[96] Martha, J., Subbakrishna, S. (2002), "Targeting a just-in-case Supply Chain for the Inevitable Next Disaster", *Supply Chain Management Review*, September/October, pp. 18-23.
[97] E.g. Avaya with UPS and Fed-Ex.

Additionally, firms can establish contracts for supply with third parties for disruption conditions. One particularly advanced example where one firm set up a contract to have dedicated 747s available within 48 hours in case of delay or unavailability of regular airfreight.[98]

Multiple distribution centers: Firms with multiple distribution centers in their downstream networks use them to provide flexibility in distribution, freely shifting among the distribution centers to move the product in case of disruption at one distribution center. This may entail higher transportation costs, potentially extended lead times and sometimes even product reconfiguration (e.g. packaging).

Direct shipments from contractors: Some of the firms outsource manufacturing to third party contractors and could have the contractors ship products directly to the end customers if going through the company warehouse is not possible.[99]

**Resilience to disruption in production facilities**

Firms indicated the use of multiple sites, agreements with suppliers, and agreements with equipment providers to create a resilient supply network in cases of production facility disruption.

Multiple sites: Firms with multiple plants, in case of disruption at one facility, can shift production to other sites. This is not always easy, as it requires that the facilities have the technical capabilities (equipment, personnel, processes) to produce many different products rather than a small set of products as many 'focused factories' produce today. In order to facilitate the shift of operations from one site to another, one of the interviewed companies adopts the same information system across all its facilities all over the world, even when they are acquired from other companies.[100] One other firm uses the same production layout and best practices for all plants located around the world.[101]

Agreements with suppliers: Firms with a single production plant, or a single plant for each product family, can consider shifting production to their suppliers' facilities in case of disruption. One firm has explicit agreements with a supplier for this possibility, since their production operations rely on similar processes and the firms have an existing collaborative relationship.[102] This not only made for a comprehensive solution in case of disruption to the facility, but it also communicated to the customer that maintaining service to the customer was important and warranted taking action to protect against disruption.

Agreements with equipment providers: For disruption at one facility, often the critical resource is the production machinery rather than the building itself. One of the firms, which uses highly automated assembly lines, has a contractual agreement with the manufacturer of the automated assembly line for a new line within 48 hours in case of need.[103]

[98] Company 8
[99] Company 7
[100] Company 11
[101] McDonald, Chris, "The Evolution of Intel's Copy EXACTLY! Technology Transfer Method," Intel Technology Journal, 4th Quarter 1998
[102] Company 1
[103] Company 11

Recently, some firms have explored using 'procurement options' to that give firms the option to order and quickly receive a long-lead-time machine in exchange for some cost determined by the supplier.[104]

Inventory policies: As is the case for response to disruption in supply, some firms also utilize modified inventory policies to mitigate risks and provide resilience. This comes at a significant cost, and has been sparingly used to date. When exercised, it entails the same processes of relocating inventory to pool risks and re-evaluating inventory positions to aid in providing a selected disruption service level.

Back up production facilities:– Some firms included identifying back up production facilities that could be available for use in the event of a disruption. More aggressively, firms could make contracts for this back up capacity as well as building the additional back up capacity (redundant capacity) at a different location as one firm[105] did to protect itself from potential disruption.

**Resilience to disruption in communication**

Firms indicated using parallel operating or mirrored operating systems, contracts with emergency information system providers and data backups to create a resilient supply network in the event of a disruption in information flows and communication.

Today it is important to take action to ensure the continuity of information and communication systems since they are obviously critical to maintaining operations and coordinating the supply chain. Hardware and software providers offer more dedicated products and services to facilitate this, and many of the firms interviewed confirmed having backup solutions in place, largely because the IT community and providers have been leaders in emergency response and preparedness. To supplement continuity plans, some firms actively test their information systems by using third party audits,[106] emergency shutdown drills, and third-party hackers to test the vulnerability of the system to break in and access. [107] A few examples illustrate the limitations of existing solutions.

One firm's IT continuity plan planned to restore the information systems within 3 days of a disruption. While the plan was comprehensive, it fell short of the business need to have the information systems restored in 8 hours to avoid shutting down production,[108] and this went undiscovered until a minor disruption exposed the mismatch. This example also illustrates how the information systems and communication continuity plans need to be checked versus the business need, and hence should be integrated and coordinated with the business operation continuity plan in order to be business effective.

Another firm found its IT system backup generally effective except that some of the emergency operating center procedures required that the information system be operating in order to access the needed information (there was no plan to maintain a hard copy for use when the system was down).[109] Fortunately for the firm, this problem was discovered in a

[104] Johnson, Blake E. "Optimizing Tool Availability and Lead Time With Procurement Options" ISSM 2003
[105] Company 18
[106] Company 1
[107] Companies 2, 8, 17
[108] Company 17
[109] Company 2

recent routine emergency shutdown drill and spared the firm from learning through a real disruption rather than a drill experience.

As it is in making operations resilient, there is a range of choices for the firm to make when planning information system continuity. This could range from basic data back-ups to mirrored systems, with the choice depending on the business situation, need, the firm's appetite for risk, as well as the desired disruption service level.

**Resilience to disruption in human resource**

Firms actively used cross-training, temporary employees, and modified production processes to create a supply network resilient in the event of a disruption in human resource capacity.

Some firms cross-trained employees to perform multiple tasks, adding to the flexibility of the firm but also inherently providing some resilience in the event of a disruption that affects personnel. One firm modified its production processes using the demand flow technology approach, breaking the work into 20-minute tasks that can be learned in a short period of time. This made it possible for lesser skilled employees to perform the process.[110] The same firm uses this approach to respond to demand fluctuations that are typical in the high tech industry in which they compete.

In addition to these policies, using knowledge management systems have been productive for firms suffering loss of human resources. Cantor Fitzgerald lost its much of its critical customer contact and relationship information when it sadly suffered the loss of hundreds of its traders in the collapse of the WTC towers. The firm however was able to reclaim much of its business operations because it had started to archive this information in a database, backing up the information that was traditionally kept by the individual traders. They were in the midst of implementing an automated process that utilized this data and depended less on traders and more on the system when the September 11 attacks occurred.

[110] Company 1

*Table Supply Chain Resilience Reponses by Failure Mode*

| Resilience to Disruption in…. | **Action** | **Advantages** | **Disadvantages** |
|---|---|---|---|
| Supply | Use multiple and/or local sources in different locales. [111] | Spreads risk across two firms, two locations; local source protects against international supply constraints. | Higher cost to qualify supplier, lower volume leverage, no assurance additional supplier is more resilient. |
| | Use single source. | Known supplier, high supplier commitment, leveraged volume. | Vulnerable to disruption unless supplier has multiple flexible sites, backup plans. |
| | Contract for supplier flexibility. | Contract obligates supplier in advance. | Potentially higher cost per unit, may entail fixed costs for "take or pay" committed volume. [112] |
| | Modify inventory levels. | "Right" parts inventory and risk pooling may reduce inventory costs. | Requires periodic analysis by item as conditions change. |
| | Modify product to use standard parts. | Reduces part and inventory cost, complexity. | Costly to modify existing materials standards. |
| Transportation | Prepare for, use multiple modes and carriers. | Pre-disruption relationship ensures support in crisis. | May need to commit volume to the alternate modes to get access in a disruption. |
| | Use spot market for capacity. | Efficient transaction with no upfront or lasting commitment. | Unknown carrier means added risk, potential for exceptional high pricing. |
| | Use logistics providers to source transportation. | Providers may have greater leverage and access. | Requires commitment (volume, cost) and relationship with logistics provider |
| Production Facilities | Use multiple sites, each making multiple products. | Enables shifting production around locations. | Requires standardization in production operations, additional capital for additional facilities. [113] |
| | Modify inventory levels and policies. | "Right" FGI levels and risk pooling may reduce inventory costs. | Requires periodic analysis, potential redesign of supply network. |
| | Modify product to use standard processes. | Leverages common capabilities for lower cost, easier backup available. | Costly to modify product and production processes. |
| | Contract backup production facilities | Committed back up assured, potential to co-locate at supplier or customer | Not dependable without contingency contract for the facilities in disruption. [114] |
| Communications | Use range of media. [115] | Communication in nearly any event. | Must maintain range of old and new technology. |
| | Back up data. | Protects against data loss. | Still requires physical system in event of system loss. |
| | Contract backup system. | Provides for near-term availability. | Potential delay in response to massive disruption. |
| | Set up and operate parallel or mirrored IT system. | Affords immediate system availability. | Requires cost to build, operate, and maintain separate system in protected environment |
| Human resources | Cross-trained workers. | Shift employees to best use as needed | Must cross-train, modify work system. |
| | Modify production process for unskilled labor. | Allows rapid increase or decrease in capacity. | Requires simplification of production process (not always feasible). |
| | Back up knowledge. | Best practices captured and documented. | Requires significant investment to capture and maintain knowledge in useful form. |

[111] 'Dual supply' and 'dual response' described respectively by Sheffi, Y. (2001) and Billington, Johnson and Triantis "A Real Options Perspective on Supply Chain Management in High Technology" *Journal of Applied Corporate Finance*, Summer 2002

[112] Byrnes, J. and Shapiro, R. "Intercompany Operating Ties" Harvard Business School Working Paper 92-058, 1991

[113] Eg. Intel's Copy Exact policy ensures all semiconductor fabrication plants are exact replicas.

[114] One automotive supplier succeeded in restarting operations in two days after a fire destroyed a factory by utilizing local facilities that had similar production capacity.

[115] One firm maintains ham radios to provide communication between all facilities in case of a complete information system disruption

### 5.4.4 Systems that fail smartly

Businesses around the world have benefited from new technologies and organizational systems that have enabled higher levels of system performance and capabilities. The recent attacks have exposed how these performance improvements have come at the expense of higher levels of dependency on technologies and on other firms. The result is that current technologies and organizational systems create more problems when they fail compared to old technologies and systems.[116] Given that resilience is an important capability that firms ought to build into their system, then how their systems fail is an important aspect that affects the firm's resilience.

Effectively, one approach to improving supply chain resilience is to design the supply chain to 'fail smartly' – that is, to fail in ways that are recoverable and not crippling. We should note that while this is an interesting idea, it is not necessarily any different than developing and improving continuity plans for disruption (see section 5.4.2 on Business Continuity Planning). It differs in the sense that it focuses on expecting disruption or failure, and therefore planning how the system should fail to enable a resilient response. It suggests there is merit in anticipating disruptions rather than thinking that one can prevent them.

There are several instances where supply chains did 'fail smartly.' The Cantor Fitzgerald case mentioned above is an example of how the firm designed its system to 'fail smartly' by using a knowledge management system (in this case it was a type of customer requirements management, or CRM system) to protect against human resource vulnerability.

In another example, a Dutch automotive supplier experienced a fire in its production facility that eliminated the firm's information system as well as its ability to produce its products. Fortunately, the firm had designed a production process that could use readily available manufacturing capacity nearby, and the firm was able to restart operations in two days.

Thinking these and other disruptions through in a continuity planning process, one can identify the risks of the response of existing systems and processes. Taking action to eliminate the evident risks effectively results in 'failing smartly.'

### 5.4.5 Designing to 'fail smartly'

Whether this is called 'failing smartly' or business continuity planning, it appears that there are several common requirements.

To fail smart, one must capture necessary information about the products, processes (manufacturing, proprietary processes that make the product unique), materials, suppliers, and customers, and retain this in an accessible environment. Unlike physical equipment and materials, redundancy of information is less expensive (the cost to copy a file is negligible although the cost to capture the information initially is not). Designing a supply chain that can be recreated with external resources (effectively designing a modular supply chain of standardized processing elements) is desirable, although not necessarily easily attained in some cases. Finally, knowledge and awareness of the availability of the resources necessary to recreate the supply chain will enable the firm to utilize the captured knowledge and exercise a modular design to create a resilient supply chain that will fail smartly.

[116] "Fail smartly" was introduced in the article "Homeland Insecurity" by Charles Mann, The Atlantic, September 2002

Depending on the specifics of the supply chain itself, this may not be realistic, but the principles may be useful as part of a business continuity planning process.

### 5.4.6 Supply network vs. integrated supply chain

Supply network design explicitly emerged as an issue – specifically what the role if for supply chain structure in providing security and resilience. On one hand, one may design an integrated supply chain with few (possibly just one) actors at each stage that are closely linked to customers and suppliers, perhaps even geographically close one to the other. One can argue that this should be more secure because it is easier to protect a few locations and short movements of goods, but, such a design would be not be very resilient: if disrupted, it would be more difficult to continue operations.

On the other hand, one may design a supply network with multiple actors at each stage of the supply chain, geographically dispersed, multiple transportation modes. This configuration is more vulnerable, since it is difficult to protect so many nodes and connections and since the network relies heavily on the communication and transportation infrastructures. A network is, by definition, more resilient because the nodes can be substituted; connections are redundant in ways that allow flows to reach their destination through an alternative sequence of nodes and connections (like TCP-IP does for the Internet).

This appears to be a promising field of investigation for subsequent study, and for the present it may be useful to recognize the tradeoffs when making design choices.

## 5.5 Responding through organization and training

While the aforementioned practices and actions are potential responses that firms can use to create a resilient supply network, firms may also consider using a concurrent effort to build an organization designed for resilience and security. Several different actions surfaced in the interviews and studies that presented this potential of creating resilience via the organization.

The following practices represent growing anecdotal evidence that the organization may be an underestimated key success factor for creating security and resilience in responding to terrorism and disruption. This warrants additional focused study to better understand this phenomenon and its impact on the firm.

### 5.5.1 Creating a Security ('Socializing Security') and Resilience Culture

Taken together, the actions in response to terrorism and disruption at some firms amount to the creation of a security and/or resilience culture. A recent conference held at MIT [117] surfaced the importance of socializing security in the organization, as well as with the other firms in the supply network, by effectively incorporating security and resilience in the daily decision-making and operating process. The following notes how some firms are 'socializing security' in their organizations and in their supply network.

[117] "Freight Lane Security in the Supply Chain" April 29, 2003, sponsored by the Center for Transportation and Logistics

### 5.5.2 Use of Organizational Design Factors in Response

Structure

Several firms improved security and supply chain performance by structurally bringing the security organization and logistics (or supply chain) organizations together in the same organization. One firm accomplished this informally by creating a project team that had both security and logistics leaders participating. The team was charged with executing a 'sting' operation intended to catch an organized theft ring that had been hijacking freight en route, and their collective action found success where the independent logistics and the security initiatives in the past did not.[118] Another firm actually put five security experts from the global security team onto the Global Logistics team, making the connection structured and long-term rather than just for the length of a project.[119]

Companies with comprehensive business continuity plans in place have generally also developed an organizational plan for whenever there is a disruption. As an example, these plans include a predetermined organization structure, hierarchy, with specific roles and responsibilities defined and procedures to be followed.[120]

Overall, efforts intended to integrate the security and logistics operations appear to be nascent and another respective element of integration to achieve network improvements in security.

Leadership

The data collected highlighted that today almost all firms have a Chief Security Officer, or a Director of Security, or a similar senior role for security leadership in place. Some of these parties were in these positions prior to September 11, but several have been either 1) recently appointed, or 2) recently elevated in their organization structure or hierarchy. In general, the number of staff reporting to these leaders has grown. In some firms this role covers both supply chain security and business continuity, while in others the security officer takes care essentially of physical security, while operations officers are responsible for the supply chain continuity.

Skills

The majority of the firms have hired people with a background in federal law enforcement agencies or in the military, including agencies like the FBI, the CIA, the NSA, the U.S. Customs and the Military Police. U.S.-based global firms have enlisted security experts from non-U.S. law enforcement agencies including the Israeli Mossad, Irish Garda, British MI5 and MI6, and the Hong Kong Police.[121]

The general impression is that firms are looking for a new kind of expertise that they do not have internally, and consequently they look for it where it is more likely to be found. However, this expertise needs to be merged with a deep knowledge of the business and the supply chain, and hence, there is a need to integrate security operations with logistics and supply chain operations.

[118] Examples provided by Gillette and H-P representatives at the aforementioned event on April 29, 2003
[119] Example provided by Pfizer representative at the aforementioned event on April 29, 2003Pfizer
[120] Companies 2, 8
[121] Company 2

### 5.5.3 Educating and Training the Organization for Security and Resilience

The most frequently noted organizational actions taken by the firms in response are the education and training of the organization for security and resilience.

Educating on Security and Resilience

Specifically, firms educated their organizations (as well as suppliers and customers in some cases) about the risks and principles of operational (facility, freight) and information system security and resilience. At companies with comprehensive business continuity plans in place, these sessions are used to communicate roles, responsibilities, and procedures in case of major disruption.[122] Firms used external coursework, learning via industry organizations or initiatives, or in-house courses to achieve this.

Training on Emergency Response – Supply Chain Drills

Firms also train the organizations on executing the specific defined emergency response plans. This is largely accomplished through in-house efforts and included emergency response or supply chain 'fire drills,' simulations, and exercises that explicitly test the organization's capability to execute the emergency response plan.

Drills and tabletop simulation entail mock exercises that address different kinds of disruption, considering not only the facilities, but also disruption throughout the supply chain, sometimes involving even suppliers, other partners and local authorities.[123] The rationale for the drilling is that only a properly trained and educated organization can react to a major supply chain disruption. Additional benefits include:

1) stress testing of business continuity plans,
2) identifying improvements to make,
3) highlighting hidden vulnerabilities or externalities, and
4) implicitly building security and resilience as a second nature response (one method to socialize security and resilience).

## 5.6 A False Sense of Security and Confidence

Many of the practices adopted by firms have provided higher levels of supply chain security and greater supply chain resilience. Some question remains, however, regarding the real value and benefit of much of the activity.

Just as the obvious presence of the TSA at airport metal detectors has increased our awareness but not necessarily our safety, the visible activities of firms fortifying their physical properties and securing second supply sources may not actually improve the overall system security or resilience significantly. It is possible that some of the actions taken by companies intended to make the supply chain more secure and more resilient may be serving the opposite purpose. Specifically, rather than building a resilient and secure supply chain, some of the practices are cultivating a harmful false sense of security and confidence. To avoid this, practitioners need to identify suitable practices for their environment and situation that improve system security and not just visible physical security.

[122] Companies 2, 8
[123] Copmanies 2 and 17 are the most advanced examples encountered so far.

Several practices potentially contribute to the creation of a 'false sense of security and confidence' in the security and resilience capabilities of the firm. These include the use of second sources of supply, utilizing C-TPAT as the firm's response, and focusing on physical security of facilities.

### 5.6.1 Sole Source vs. Second Sources of Supply: Impact on Security, Resilience

One of the more common practices for companies to adopt after unexpected disruption to has been seeking second sources of supply for materials where there is only one supplier. While this makes sense on the surface to spread the risk of loss of supply by having a second source, a deeper analysis reveals that it may actually reduce the security and resilience of the supply chain.

While adding a second supplier can reduce the risk of disruption that is localized around a single source with a single site, it may increase the risk of security breach or inability to respond if the second supplier does not have a secure or resilient supply chain itself. Having two suppliers that are not secure and not resilient only makes the supply chain more vulnerable (now there are two possible targets instead of one), and it makes coordination of supply twice as difficult. Any efforts made to improve the security or resilience of multiple suppliers' operations requires at far more effort than working with one firm.

The effect of adding a second supplier is different for security and for resilience. Adding a second supplier to increase security appears to have negative impact, since by adding a supplier there is more supply chain to secure. On the other hand, adding a supplier to increase resilience could increase resilience if each supplier had the ability to offset capacity loss or delay by the other supplier. This would mean each supplier would have some ability to increase capacity up to 50% in a defined period of time (assuming a 50-50 split of volume between suppliers). While capacity increases of this order of magnitude are not out of the question in some industries, this often entails a significant effort. Spreading the effort across two firms may reduce the ability to deliver results. Given the required work, it may lead one to consider focusing resilience improvement efforts on one supplier in order to focus the effort, leverage the volume and invest in the relationship.

Certainly having two suppliers makes it more unlikely to lose 100% of supply, thus allowing to continue production at least partially even when the surviving supplier is not flexible. This "loss mitigation" should be compared with the additional efforts required and the potential related consequences.

The net pertinent result is that by their nature, second sources may provide only single location risk mitigation, and may actually be less resilient and secure than a sole source that has greater capacity to respond to disruption. This should be determined on a case-by-case basis, keeping in mind these tradeoffs.

### 5.6.2 C-TPAT as the foundation for Corporate Response

C-TPAT is serving an important and surprising role for firms by actually providing a base standard for corporate response to improve the security of the supply chain. Since there isn't a standard in place or being promoted broadly, the C-TPAT requirements are serving that purpose. The good news is that this is indeed adding some measure of security to the firm,

especially for those firms that become C-TPAT certified and earn preferential treatment in port passages.

The adoption of C-TPAT however, may contribute to creating a 'false sense of security' in participating firms for two reasons. C-TPAT is an initiative to increase security, not resilience, and therefore the firm adopting C-TPAT as its base response neglects to consider the resilience of its supply chain.

Secondly, C-TPAT does not guarantee a high level of security because the impact of C-TPAT compliance depends a great deal on the diligence of the firm implementing C-TPAT. Importing firms signing C-TPAT agreements must carry out several assessments[124] and pass an audit conducted by Customs. All of these practices build some rigor into the process initially, but the maintenance of the firms' performance and its relationships with suppliers is up to the diligence of the firm. While many are well-intentioned to 'do the right thing' to make for a secure supply chain, it would be easy to disagree about what constitutes 'the right thing,' and maintaining the rigor associated with the initial C-TPAT application will likely come under pressure as daily business operations appear more pressing than conducting audits and assessing capabilities. Ultimately, the security efforts may decline as a result. As it is with adopting a second supplier, merely becoming C-TPAT compliant may lead the firm into feeling as though there is a higher level of security that what actually exists.

### 5.6.3 Focus on physical security versus network security or business continuity

Many firms have added new measures of physical security to their business operations. These are often very visible to external parties and often entail some new levels of security for personnel in the form of ID badges, perimeter control, and access control for employees, contractors, and non-employees alike. While these may serve the useful purpose of limiting access to specific facilities, this is only one of several vulnerabilities that need to be considered and addressed when securing a supply network. Hence, the added physical security measures and visible modification may lead the firm to think that it is now 'secure' and protected, but this does not reflect the security of the firm's extended supply chain in the inbounds from suppliers and the outbound shipments to customers.

Additionally, physical security of the premises does not protect against one of the more significant vulnerabilities, that of the employee. The firm will still need to protect against the 'enemy within' by checking the backgrounds of existing employees and managing specific access to facilities as needed, and by protecting the extended supply chain by assessing the real security and resilience of its suppliers and downstream supply chain parties.

[124] From the C-TPAT Fact Sheet located at http://www.customs.gov/xp/cgov/import/commercial_enforcement/ctpat/fact_sheet.xml
firms applying for C-TPAT must "conduct a comprehensive self-assessment of supply chain security, submit a supply chain security profile questionnaire to Customs, develop and implement a program to enhance security throughout the supply chain, communicateC-TPAT guidelines to other companies in the supply chain and work toward building the guidelines into relationships with these companies"

# 6 Classification

Four different levels of response surfaced on a preliminary analysis of the anecdotal data from the 20 firms interviewed. This may be useful for rudimentary self-assessment as this may reflect a potential progression to higher levels of security and resilience, although the data is not robust enough to make these assertions without reservation. Additional data and analysis are required, and the analysis would likely need to consider various firm-specific factors including suppliers, customers, products, geography, technology, culture, past experiences, industry standards, and regulation by government may also be important factors.

**LEVEL 1 - Basic Initiatives.** Firms in this group may engage in many security and preparedness activities that have large diffusion (but are not generally related to terrorism). Some of these firms may have strengthened such programs and initiatives after September 11. Basic initiatives include:

- **Physical security measures**: Access control, badges, guards, camera systems.
- **Personnel security:** criminal, credit and background checks on potential employees
- **Standard risk assessment**: Consideration of risks such as fire, flood, vandalism, utility disruptions.
- **Basic cyber security**: Anti-virus software, firewalls, passwords.
- **Continuity plan**: for internal purposes and small-scale incidents, How to recover within one's own operations.
- **Freight protection**: Employee background checks, cargo seals, tracking technologies, sensors.

**LEVEL 2 - Reactive Initiatives.** Firms in this group meet or exceed the practices described as Level 1, and they express greater awareness of security vulnerabilities. These firms have typically altered or added supply chain and security initiatives since September 11. Reactive initiatives include:

- **Larger security, risk, or business continuity organizations**: Firm increases commitment either through reallocation of human or capital resources.
- **C-TPAT compliance**: Firm filed an application for compliance, perhaps as a result of internal leadership or government pressure.
- **Analysis of supply base**: understanding supplier capabilities in the event of disruption.
- **Supply continuity plan**: Consequences of September 11 and the threat of a new disruption in supply lead to the development of dedicated continuity plans.
- **Limited training**: Select employees (not all) receive training or education what our research group has termed Level 1 and Level 2 initiatives.

**LEVEL 3 – Proactive Initiatives.** Firms in this group meet or exceed the practices described as Level 2, and participate in or adopt newer supply chain and security practices beyond industry norms, government regulation, and supplier or customer requirements. Proactive initiatives include:

- **Director or Chief of Security**: The creation or existence of executive level positions with resources and responsibility for ensuring security.
- **Ex-federal or ex-military personnel**: A number of firms have actively sought or retained employees with prior government, military, law enforcement, or intelligence agency experiences.
- **Structured risk assessment**: Firms using formal and comprehensive approaches to analyze and understand their exposure to risk.
- **Advanced cyber security**: Firms using intrusion detection systems, relocation of IS in secure buildings, physical separation of the internal network from the Internet, auditing of partners' practices.
- **Business continuity plan:** Firms develop plans to address primary failure modes, including supply, transportation, freight, facilities, and communication, often developed in collaboration with logistic providers.
- **Participation in industry supply chain and security groups:** Firms are aware of and provide input on the development of industry-wide common policies, standards; support or advocate government actions.

**LEVEL 4 – Advanced Initiatives.** Firms in this group meet or exceed the practices described as Level 3, and often lead new and progressive supply chain and security initiatives. Often these efforts have occurred for several years (i.e. before September 11) and have only been adopted by a limited number of companies. Advanced initiatives include:

- **Customer-supplier collaboration**: Firms develop flexible contracts, joint continuity plans with suppliers and customers, alternative sources.
- **Learning from past disruptions**: Firms build on past experiences to make their organizations stronger.
- **Formal security strategy**: Firms develop a comprehensive, documented strategy, which includes all initiatives to increase supply chain security and resilience.
- **Supply chain drills, simulations, and exercises**: Firms perform training or exercises that include simulations of supply chain disruption, stress testing security measures and business continuity plans for a variety of possible disruptions.
- **Emergency control center**: Firms implement a predetermined facility and set of procedures to manage and coordinate the response to unexpected disruptions.
- **Cost/benefit analysis**: Firms understanding (quantitatively when possible) the actual or expected costs and benefits of different alternatives.

# 7 References

In addition to the references sited in the report, these were useful references for the study.


- Coutu D.L. (2002), "How Resilience Works", *Harvard Business Review*, May.
- Forrester, J. (1961), *Industrial Dynamics*, MIT Press, Cambridge, MA.
- Lee, H.L., Wolfe, M. (2003), "Supply Chain Security Without Tears", *Supply Chain Management Review*, January-February.
- Lindroth, R., Norrman, A. (2001), "Supply Chain Risks and Risk Sharing Instruments – An Illustration from the Telecommunication Industry", *Proceedings of the Logistics Research Network 6th Annual Conference*, Edinburgh September, 13-14, pp. 297-307.
- Martha, J., Subbakrishna, S. (2002), "Targeting a just-in-case Supply Chain for the Inevitable Next Disaster", *Supply Chain Management Review*, September/October, pp. 18-23.
- Martha, J., Vratimos, E. (2002), "Creating a Just-in-Case Supply Chain for the Inevitable Next Disaster," MMC Viewpoint, Autumn 2002
- Sheffi, Y. (2001), "Supply Chain Management under the Threat of International Terrorism", *The International Journal of Logistics Management*, Vol. 12, No, 2, pp. 1-11.
- Shrader, R. W., McConnell, M. (2002), "Security and Strategy in the Age of Discontinuity: A Management Framework for the Post-9/11 World", *Strategy+Business*, www.strategy-business.com.
- Souter, G. (2000), "Risks from Supply Chain also demand attention", *Business Insurance*, Vol. 34, No. 20, pp. 28-28.
- Tsay, A.A., Nahmias, S., Agrawal, N. (1999), "Modeling Supply Chain Contracts: a Review", in Tayur, S., Ganeshan, R., Magazine, M., *Quantitative Models for Supply Chain Management*, Kluwer Academic Publisher, MA, pp. 299-336.
- Yin, R.K. (1984), *Case Study Research*, Sage Publications, Beverly Hills, CA.
- Zsidin, G. (2001), "Measuring Supply Chain Risk: an Example from Europe", *Practix, Best Practices in Supply Chain Management*, June, pp. 1-6.

# Appendix 1: Background Research and Literature Review

Within the supply chain management literature, a rich stream has dealt with the general issue of managing risk. Many authors have traditionally dealt with the uncertainty deriving from market volatility, ranging from the study of the amplification of fluctuations along the supply chain (the *bullwhip effect*, Forrester, 1961) to the development of solutions to manage this kind of risk (see e.g. Tsay et al., 1999 for a review of supply chain contracts).

However, market uncertainty is only one of the sources of risk for the supply chain. Zsidisin (2001) noted that another relevant source of risk lies within suppliers and the supply market. These supply risks can significantly affect the ability of an organization to achieve financial success. For example, the Taiwan earthquake of 1999 created serious financial loss for many high technology firms because supply was constrained which caused factory slowdowns and missed marke t opportunities.

In particular, a disruption in supply can affect companies a long way down the supply chain, showing how important it is, today, to consider not only the risk of a single company, but also of the many links in the supply network (Souter, 2000).

From a broader perspective, consequently, supply chain risks can derive from many different sources and impact different parts of the supply chain. Lindroth and Norrman (2001) suggest a framework for assessing and positioning supply chain risk issues, according to three dimensions: unit of analysis (from the single logistics activities to the whole supply network), type of risk (operational accidents, operational catastrophes and strategic uncertainties), and risk handling focus (risk analysis, risk assessment and risk management).

A limited number of authors, however, address directly the issue of terrorism-related risk. Sheffi (2001) introduces the problem and presents a variety of issues that are described in terms of three themes: how to deal with the aftermath of a terrorist attack, how to operate under heightened security and how companies should collaborate with the public sector to face the threat.

Martha and Subbakrishna (2002) show how the effect on the supply chain of a large scale terrorist attack can be very similar to those of a natural disaster or a major accident, providing examples of successful and unsuccessful management in recent ones, such as the outbreaks of Foot and Mouth Disease (also known as mad cow disease) in Europe in 2001 and the earthquake in Taiwan in 1999.

This last contribution provides a very useful insight: although terrorism is a new issue in supply chain management literature, the work done so far on other sources of risk can be valuable by illustrating how previous disruptions had been handled.

Companies however, besides identifying and assessing risk, also need suggestions on how to protect their own operations. In particular, firms are looking for ways of increasing the security of their supply chains without jeopardizing their effectiveness. Applying the lesson of the quality movement, Lee and Wolfe (2003) suggest that it is possible to achieve "supply chain security without tears," i.e. creating strategies that improve security while also strengthening productivity. In particular, the authors point out that a range of possible

measures exists, and they can be split into two main categories. On the one hand there are all the initiatives aimed at preventing security breaches (e.g. inspections, information protection, international standards, etc.), on the other hand there are the measures aimed at mitigating the consequences of a disruption and enabling a prompt reaction (namely: total supply network visibility, flexible sourcing, balanced inventory management, product and process redesign, and demand based management).

This last group of initiatives is aligned with an already existing, but increasingly relevant area of research, aimed at creating resilient organizations. In order to suggest a way to acquire preparedness to unexpected disruption, Coutu (2002) introduces the concept of organizational resilience, which can be defined as "the ability to bend and bounce back from hardship", adapting a concept developed by psychologists for people who survived to concentration camps.[125]

The threat of terrorism and other risks, consequently, is not affecting only the "physical" supply chain, but also the organizational dimension of companies, to the point of affecting the whole corporate strategy. Shrader and McConnell (2002) discuss how security should be incorporated into corporate strategy, starting from securing the company people, considering then the business and finally protecting the networks and the flows of goods and information. The goal is shifting security efforts from being a source of additional costs to become the source of new benefits, increasing efficiency and providing competitive advantages, in line with the previously mentioned contributions.

The limit of all these contributions is the scarce use of empirical evidence: some of them are purely theoretical and others are based on examples of reaction to past events, but none of them investigates the current corporate response. There is still no clear idea about the actual preparedness of companies to supply chain disruptions, also because it is not yet clear what could be done to increase security and resilience.

# Appendix 2: Project Description

## Methodology

The initial overarching objectives of the initial research effort included:

- To document both the current and expected impacts of terrorism on supply chains,
- To understand supply chain consequences of government actions in response to terrorism,
- To understand the actual risks for company supply chains in various industries,
- To identify opportunities for companies to improve their supply chains and business operations in light of disruptions such as terrorist attacks.

In order to achieve these goals, the research team studied several areas and used various methods as follows:

[125] For the purposes of the supply network, we define resilience as "the ability to react to unexpected disruption and restore normal supply network operations"

- Response of the risk management community and insurance industry:
  - Literature review, analysis, and synthesis of written material relevant to risk management and assessment.
  - Informal interviews with industry personnel and active participation in pertinent seminars and conferences.
  - Synthesis of the data and information into a set of observations and insights.
- Response of corporations:
  - Literature review, analysis, and synthesis of written material relevant to how corporations respond to terrorism and other similar disruptions.
  - Formal set of 20 interviews with industry leaders following a consistent interview format intended to capture corporate response data regarding risk assessment, continuity planning, use of technology and processes.
  - Synthesis of the data and information into a set of observations and insights.
- Response of government:
  - Literature review, analysis, and synthesis of written material relevant to government response, specifically impacting commerce, business operations, supply chains and/or the insurance industry.
  - Informal interviews with government personnel and active participation in pertinent seminars and conferences.
  - Synthesis of the data and information into a set of observations and insights.
- Response to prior disasters and catastrophes:
  - Literature review, analysis, and synthesis of written material relevant to past disasters such as earth quakes, bombings, plagues, hurricanes.
  - Synthesis of the data and information along with categorizations into a set of observations and insights that provide insight into learnings from the collective past disasters.

Corporate Response Interviews:

As a result of the initial literature reviews, the research team devised a survey with 25 questions to help further refine the scope and importance of the broad areas of investigation detailed above. This survey was administered either via phone or in-person to personnel from 20 large companies, primarily from the shipper community. These personnel were typically either Directors or Managers from Supply Chain or Security organizations. The industries represented include high tech, aerospace, automotive, food, pharmaceuticals, consumer goods, and logistics. Interviews were usually conducted by two researchers, recorded with participant permission, and lasted from 30 to 90 minutes, approximately 60 minutes on average.

## Industry Interview Participants & Study Detail

As noted, the "Supply Chain Response to Global Terrorism" project has studied the response to terrorist attacks from several different perspectives: the manufacturing and distribution industry response, the risk management and insurance industry response, and the U.S. Government response. Additionally, we studied how firms have responded to past disasters in the hopes of identifying useful analogies that we could learn from and enrich our work. [126]

[126] Additionally, the project is also developing the use of real options to assess the potential value of flexibility in supply chain design in responding to disruption. This research is being conducted by Prof. Richard de

The companies selected for the interviews are medium to large companies with operations in the U.S., and also subsidiaries or branches of the supply chain overseas. A semistructured interview was conducted with a sample comprised of 20 companies from different industries, operating at different stages of the supply chain. The sampling was based on an informal method combining self-selection and convenience criteria, i.e. those firms expressing an interest in the study and exploiting existing relationships. The respondents are listed in the Table below. Additional information about the study can be accessed at the project website, <http://web.mit.edu/scresponse>

*Table . The sample*

| N° | Industry | N° | Industry |
|---|---|---|---|
| 1 | High Tech Machinery | 11 | Electronic manufacturing services |
| 2 | Electronics components | 12 | Automotive |
| 3 | Food and beverages | 13 | Telecommunication equipment |
| 4 | Consumer packaged goods | 14 | Apparel |
| 5 | Electronics products | 15 | Food and beverages |
| 6 | Pharmaceuticals | 16 | Electronics products |
| 7 | Telecommunication equipment | 17 | Consumer packaged goods |
| 8 | Aerospace | 18 | Medical equipment |
| 9 | Retail | 19 | Automotive |
| 10 | Freight broker | 20 | Toys |

# Appendix 4: Limitations of data use

As suggested above, this report intends to inform the reader of the state of the work-to-date based on literature reviews and qualitative data collected from selected respondents. One of the sources of data was the series of interviews that were conducted (see above). This data was very useful in providing insight into some progressive companies. The data does not, however, provide enough of a foundation to make any assertions with statistical validity, and therefore, we use qualitative descriptors in reviewing the data received. Having said that, we do believe it is useful to consider the data in the context of the overall system, and offer some observations for practitioners to consider going forward.

Limitations of data use are as follows:

- Data reflects a primarily US-centric view.
- Data points are limited in number, making it impossible to conduct statistical analysis. This is a more realistic possible outcome from a subsequent survey.
- The intention of the preliminary work (including the literature review and situation scans) was to identify state-of-art practices of progressive companies attempting to make their supply networks more secure and more responsive.
- Many corporate and government responses related to supply chain management and terrorism are either ongoing (i.e. evolving) or undocumented for broad dissemination.

---

Neufville of MIT. For additional information about this subject matter, refer to http://ardent.mit.edu/real_options.

- Some industry or government personnel may not be willing or able to communicate how their organizations have responded to terrorism, which may limit the accuracy of the assessment of 'state-of-art' response.
- Different industries have different supply chain and security related issues, and therefore while a number of industries were queried, the response may not have captured a comprehensive assessment reflective of all industries.
- The data reflects responses of different dimensions: from various stages in the supply chain (manufacturing, distribution, retail), and from security and supply chain personnel. This makes for a more informed set of data but not one that has consistency among the data sources. Also, the data sources included a majority of shippers and a few carriers or agents, biasing the perspective towards supplier issues, practices and insights.

# Appendix 5: Department of Homeland Security

As suggested previously, the most prominent action taken by the U.S. government recently has been the creation of the Department of Homeland Security (DHS), a cabinet-level organization with nearly 200,000 employees and a $36.2 billion budget for 2004. This was accomplished by bringing together 22 previously separate government organizations, thus representing the largest federal reorganization in fifty years.[127]

DHS has four primary directorates, each of which brings together these various organizations (with previous Department affiliation in parentheses):

The Border and Transportation Security directorate will bring the major border security and transportation operations under one roof, including:

- The U.S. Customs Service (Treasury)
- The Immigration and Naturalization Service (part) (Justice)
- The Federal Protective Service (GSA)
- The Transportation Security Administration (Transportation)
- Federal Law Enforcement Training Center (Treasury)
- Animal and Plant Health Inspection Service (part)(Agriculture)
- Office for Domestic Preparedness (Justice)

The Emergency Preparedness and Response directorate will oversee domestic disaster preparedness training and coordinate government disaster response. It will bring together:

- The Federal Emergency Management Agency (FEMA)
- Strategic National Stockpile and the National Disaster Medical System (HHS)
- Nuclear Incident Response Team (Energy)
- Domestic Emergency Support Teams (Justice)
- National Domestic Preparedness Office (FBI)

The Science and Technology directorate will seek to utilize all scientific and technological advantages when securing the homeland. The following assets will be part of this effort:

[127] Figures and quote from Department of Homeland Security web site: www.dhs.gov

- CBRN Countermeasures Programs (Energy)
- Environmental Measurements Laboratory (Energy)
- National BW Defense Analysis Center (Defense)
- Plum Island Animal Disease Center (Agriculture)

The Information Analysis and Infrastructure Protection directorate will analyze intelligence and information from other agencies (including the CIA, FBI, DIA and NSA) involving threats to homeland security and evaluate vulnerabilities in the nation's infrastructure. It will bring together:

- Critical Infrastructure Assurance Office (Commerce)
- Federal Computer Incident Response Center (GSA)
- National Communications System (Defense)
- National Infrastructure Protection Center (FBI)
- Energy Security and Assurance Program (Energy)

The Secret Service and the Coast Guard will also be located in the Department of Homeland Security, remaining intact and reporting directly to the Secretary. In addition, the INS adjudications and benefits programs will report directly to the Deputy Secretary as the Bureau of Citizenship and Immigration Services.

# Appendix 6: Trade-offs

Sheffi[128] pointed out a series of trade-offs that firms face when organizing for security and resilience. These tradeoffs are introduced here and are briefly discussed, although the comments are preliminary and not entirely developed. Despite that, we include them here for consideration and welcome input and feedback.

- **Repeatability vs. unpredictability**: Repeatability is one way to achieve efficiency, proficiency and reliability in operations, but it is also a way to introduce predictability, i.e. vulnerability. Introducing unpredictability means instead to frequently change truck routes, passwords, etc. Evidence so far shows that such actions have been put in place only when their cost is marginal or the risk is too high, as in the case of changing passwords, to avoid exposing the company to cyber attacks, whose cost would be unbearable. So far there is no particular evidence of cargo containing hazardous material taking longer routes to be less predictable, but if the risk becomes too high, probably it could happen. An interesting example is UPS, which sees the repeatability of the procedures followed by its personnel as a means to achieve both efficiency and the ability to react quickly to unexpected events.
- **The lowest bidder vs. the known supplier**: A few, well known and reliable suppliers can provide higher security than the lowest bidders, with whom the company has spot relationships, however this choice would probably determine higher costs in some cases. The same can apply for national suppliers vs. foreign suppliers. Evidence so far seems to support the shift towards major carriers and logistics providers with whom companies have strong relationships. Costs may be higher, but now also security costs should be taken into account, and often known carriers provides a lower total cost. This is true in particular for importers, due to the additional costs occurring at Customs for non C-TPAT

[128] Sheffi, Y. (2001), "Supply chain management under the threat of international terrorism", *International Journal of Logistics Management*, Vol. 12, No. 2, pp. 1-11.

carriers, but also for the choice between national and foreign suppliers. If the cost of imports becomes too high, U.S. companies could shift to national suppliers, but they could also decide to move operations completely abroad, in particular those selling globally.

?? **Centralization vs. dispersion**: Risk pooling and economies of scale often suggest centralizing inventories, people and assets, but security instead suggests dispersion. Generally speaking, there is no one single pattern regarding this trade off, but the choice depends on the magnitude of the different sources of risk. When the risk is essentially in the unreliability of deliveries from suppliers, which is inconsistent with a just in time approach, centralization (i.e. location of suppliers close to the customer) helps. When instead distribution is considered, if centralization increases the risk of disruption more than it reduces the forecasting risk, a certain degree of dispersion can be introduced.

?? **Managing risk vs. delivering value**: Managing risk implies additional costs that do not result in day-to-day value, consequently it is difficult to remain vigilant and continue investing in security in the long term, in particular when stakeholders ask for value and no disaster occurs. Today attention is still very high, but what will happen in the future is still to be seen and the economic downturn is pressing companies to cut costs and increase value. This is true, however, if risk mitigation measures are seen as pure costs. Initiatives that provide additional benefits, such as reduced theft, higher visibility, higher flexibility, etc. not only help reduce risk, but also deliver value.

?? **Collaboration vs. secrecy**: Collaboration between partners along the supply chain is likely to improve both efficacy and efficiency, but requires information sharing, which in turn can create additional vulnerability. Today there is still emphasis on inter-company collaboration, but with a new concern for information security, since also very secure internal information systems become vulnerable if partners with poor security are granted access to them. Some companies have realized that having firewalls and intrusion-detection software is not enough, and they are now auditing the information security practices of their partners before sharing information with them. More in general, when partners are considered really trustworthy, collaboration is seen not only as a way to improve performance, but also security and resilience.

?? **Redundancy vs. efficiency**: In a world that for decades has fought to reduce inventories and built just in time manufacturing systems, adding redundancy to reduce risk exposure is a very strong proposition. So far there is little evidence of compromises to create buffers, thus reducing efficiency. Everybody today claims for solutions that can increase security without creating redundancy, but increasing efficiency instead. Some examples include building higher visibility in the supply chain through the adoption of the latest technologies, but they are still in the development phase, and there is a need for common standards. In general, flexibility seems to be preferred to redundancy, but many companies still lament the lack of a clear business case.

?? **Government cooperation vs. direct shareholder value**: Private and private-public cooperation to increase security is today a reality, at least considering the number of initiatives currently in place. This does not mean, however, that shareholder pressure for short-term results has reduced, in fact the common denominator of all these initiatives is to increase security, but at the same time to reduce the related costs. Examples can be C-TPAT, which grants "faster lanes" at the Customs for members, and the lobbying efforts of industry associations, aimed at supporting security solutions whose costs are shared with the public sector.

# Appendix 7: Comparison Cases: Many Paths to the Same Destination

As one can infer from this report, there is no 'silver bullet' or single set of specific practices that all firms should adopt in order to make their supply network adequately secure and resilient. For one reason, the 'suitable' level of resilience and security may vary by firm, depending on the firm's situation and the level of security and resilience that the firm elects to pursue. Specifically, the situational factors include the importance of the firm's physical infrastructure, its intellectual property, the location of the firm in the supply chain, the size of the firm, its relationships with suppliers and customers, and the design of its supply network. How the firm assesses risks and the potential impacts of disruption are among several factors that guide the choice that the firm makes to pursue different levels of security and resilience.

In addition to choosing the level of security and resilience, each firm chooses how to attain those selected levels. It is apparent from the interviews with firms that it is possible to reach the same end point (in terms of supply chain security and supply chain resilience) by taking different paths. The experiences of three firms in the same extended supply chain illustrate this well, and they allowed the research team to investigate most of the above described findings, and to reflect on how the various tools available to manage risk, improve security and increase resilience can be combined.

All the three cases have an articulated and comprehensive approach to the problem, embedded in the company culture and definitely pre-existing to 9/11. All have suffered from some kind of disruption in the past and are used to a very volatile market, whose severe fluctuations are unpredictable, thus requiring high levels of flexibility. All of them operate in global supply chains and compete on global markets, although company 1 has a single manufacturing operations in the US, while the other two have plants all over the world.

Despite these similarities, many choices in terms of response to supply chain risk differ significantly, suggesting that there is not a single best way towards security and resilience, but instead different approaches can be equally valuable, if they are coherent with the company characteristics.

In particular, company 1 has many single and sole sources, while the other two have mainly multiple sources. Clearly multiple sourcing allows the firms to spread the risk of a disruption in supply, but company 1 also manages risk very carefully. They do it through a very close relationship with suppliers, who are very committed to ensure continuity of supply. If they consider a supplier too exposed to any kind of risk, they generally move to another one. They basically believe that a single, very flexible and committed supplier will provide higher security and resilience, compared to two rigid and insecure suppliers, who can be more easily affected and may not be able to backup for one another.

Another interesting difference is in the way supplier flexibility is achieved: company 11 requires it by contract, in very detailed way, while company 1 obtains it through informal agreements. They also perform regular capacity audits, in order to monitor the real ability of the suppliers to scale production.

In synthesis, we can conclude that every company undertakes a different series of initiatives, which are shown in the Table below, all aimed at the same goal of strengthening security and achieving resilience. The specific initiatives selected depend on the company characteristics,

such as size, location, type of operations, type of goods shipped, etc. For example, company 2 ships many high value, small sized products, which are highly exposed to theft, hence freight security is a priority. Company 1 is less concerned with freight security, while it is more concerned with its ability to ensure continuity of production, because it has a single plant worldwide.

*Table . Comparison of the case studies.*

| Company 1 | Company 2 | Company 11 |
|---|---|---|
| ?? Consolidated relationships with flexible SME suppliers, personal contacts<br>?? Many sole and single sources<br>?? Capacity audits of suppliers<br>?? Agreements with a supplier to shift production to his site<br>?? Demand Flow Technology<br>?? Flexible workforce and temporary employees<br>?? Duplication of IS and training to restore operations<br>?? Direct management of transportation in case of emergency<br>?? Suffered from ice storm that hampered transportation | ?? Strategy of exact plant replication in different countries<br>?? Multiple sources for every part<br>?? Creation of an industry association<br>?? Emergency Operations Centers in every plant coordinated from the HQ<br>?? Extensive simulations and drills<br>?? Company culture stressing the attention to details<br>?? Physical protection of facilities<br>?? Suffered from thefts and various SC disruptions<br>?? Staff from FBI, MI5, MI6, Mossad, Irish Garda, Hong Kong police, etc. | ?? Flexibility written into contracts (+25% 1 week, +100% 4 weeks)<br>?? Multiple sources wherever is possible<br>?? Agreements with equipment providers to restore assembly lines in 4 weeks<br>?? Unique IS across the world, also in acquired facilities<br>?? Collaboration with logistics providers to ensure continuity of transportation<br>?? Suffered from major theft<br>?? Military personnel |

Taken all together, this makes for cases where the organization recognizes the need for security and resilience, has systems in place to support adopting suitable levels of security and resilience, and achieves the desired goals without a mandate from the CEO. The leadership of the company did not have to identify security as the most important business driver, but the domain leaders were able to identify the economic risks and build organizational support for the necessary support to create secure and resilient supply chains. Resilience and security are viewed as necessary competencies to compete and to be successful.

The net result is that it is possible to get to the same result by going different paths, although there are commonalities that may serve as important determinants of success.[129]

[129] This is a research question that would need to be studied further.