"Supply Chain Response to the Unexpected: Resilience and Security"

ISCM Research Project Update
WebEx Session

James B. Rice, Jr.
April 8, 2003

MIT Research Project – SC Response

- Prof. Yossi Sheffi initiated project to study terrorism and supply chains
  - How can companies respond to make their supply chains more secure
  - How can companies respond to make their supply chains more resilient
- Multi-Phase Project
  - Current Activities – situation scan to focus next phase, report March 2003
    - Literature review on how different groups have responded
      - Government
      - Risk management and insurance industry
      - Industry and corporations
    - Studying past disasters/disruptions to identify useful learnings
    - Collect specific data via interviews with shippers.
    - Applying real options to determine value of different responses

Today's Plan

- Review some highlights of observations to-date
  - Note that the work is in progress
  - Our data set represents experiences of shippers primarily
  - Data is anecdotal
  - Your feedback and input is welcome
- How the various segments have responded
  - Government
    - New Initiatives, Interdependencies and Public-Private Partnerships
  - Risk management and insurance industry
    - Failure Modes, Network Risk
  - Corporate Response
  - Learning from Past Disruptions
  - Emerging Progressive Practices
  - Watchouts

Network Resilience & Security

Resilience & Security

- Insights from understanding how different organizations respond to disruption (e.g. terrorist attacks, natural disasters, unexpected capacity loss)
- How the various segments have responded
  - Government
    - New Initiatives, Interdependencies and Public-Private Partnerships
  - Risk management and insurance industry
    - Failure Modes, Network Risk
  - Corporate Response
  - Learning from Past Disruptions
  - Emerging Progressive Practices
  - Watchouts

Responses

Government Response
(as it relates to commerce and the supply chain)

Government Actions Since September 11

- Legislation
  - Over 100 new laws passed since 9/11/2001
  - Primarily address Recovery and Symptoms
- Budget
  - $40 B designated since 9/11 for recovery & homeland security
  - $2B+ primarily designated for recovery
    - Federal Emergency Management Agency ($2 B, NY/DC)
    - Department of Health and Human Services ($126 MM)
    - Small Business Administration ($100 MM)
- Department of Homeland Security
  - $36 B 2004 budget, 200k employees, 22 Fed organizations
- Federal Agency Actions
  - Many new initiatives – Public-Private Partnerships

Initiatives Currently in Place

- Customs (Department of the Treasury):
  - Customs-Trade Partnership Against Terrorism (C-TPAT):
    - Certified companies assume responsibility for cargo security and are granted “fast lanes” at Customs.
  - Container Security Initiative (CSI):
    - Identify and pre-screen high-risk containers before they arrive in the U.S., exploiting the latest technologies.
  - Automated Commercial Environment (ACE):
    - Information technology system to process goods and merchandise imported in the U.S.
  - Business Anti-Smuggling Coalition (BASC):
    - A business-led, U.S. Customs-supported alliance created to combat narcotic smuggling via commercial trade.
  - Carrier, Land Border Carrier and Super Carrier Initiatives:
    - Anti-drug smuggling training to air, sea and land commercial transportation companies.
  - The Treasury Advisory Committee on the Commercial Operations of the US Customs Service (COAC):
    - Representatives of the trade industry at large, including importers, ports, customhouse brokers, trade attorneys and carriers.

Initiatives Currently in Place

- Department of Transportation:
  - Marine Transportation System National Advisory Council (MTSNAC):
    - 30 senior-level representatives from transportation-related organizations.
  - National Infrastructure Security Committee (NISC):
    - Officials from the DoT and US Customs.
- Joint initiative of the Customs and the Coast Guard (DoT):
  - Operation Safe Commerce:
    - Tracking goods from the source to the destination in the U.S.
- Homeland Security
  - Homeland Security Advisory Council:
    - A group of 21 leaders from business, academia and state and local government that advise the Bush administration.
  - National Infrastructure Protection Center (NIPC):
    - Representatives from U.S. federal, state, and local Government agencies, and the private sector housed at FBI HQ, focused on protecting IT infrastructure.
- DoC – Technology Administration
  - National Institute for Standards and Technology (NIST)
    - Computer Security Division (CSD)

Initiatives Currently in Place

- Additional Industry Initiatives
  - Smart and Secure Tradelanes (SST):
    - A seaport operators driven initiative to deploy the Total Asset Visibility (TAV) network (pioneered by the DoD), in order to improve tracking and security of shipments.
  - Strategic Council on Security Technology (SCST)
  - Council of Security & Strategic Technology Organizations (COSTO)
  - Technology Asset Protection Association (TAPA)
  - Business Executives for National Security (BENS)
  - National Petrochemicals & Refiners Association (NPRA)
  - American Chemistry Council (ACC)
  - National Industrial Transportation League (NITL)
  - …

Government Response – New Initiatives

- New legislation, spending, and initiatives
  - Involving government and industry to improve security
- New interdependencies becoming evident
  - Business dependent on the government
    - Fast flow through customs for cargo movements
    - Technology infrastructure investments & secure infrastructure
  - Government dependent on business
    - Assessing vulnerability of the extended supply network
      - It's a 'joint effort' to secure the supply chain, we need business to know the vulnerabilities of their supply sources*
    - Local implementation of security measures (C-TPAT, FAST)
    - Maintaining economic engine
  - Business dependent on business
    - Coordinating flows, securing the supply network

* Admiral Vivien Crea, U.S. Coast Guard, Dec. 5, 2002
MIT Symposium "Supply Chain Response to Terrorism: Planning for the Unexpected"

New Initiatives – New Opportunities

- Public-Private Partnerships
  - Many new initiatives started by the government
  - Still need to fully integrate industry and government
    - 'Voluntary' programs present conflicts for supply chain parties
  - Still need to fully integrate industry and industry!
    - Shipper – Carrier disconnect
  - Still need to develop emergency response systems coordination between industry and government
  - New systems being developed, with new questions about….
    - Coordination – How will new systems be coordinated?
    - Ownership – Who will own the new systems?
    - Control – Who will control the new systems? Decision-making?
  - These are opportunities to 'partner' for system improvement in unprecedented ways

Risk Management and Insurance Industry Response

Risk Management Community Response

- September 11 changed insurance economics
  - $56B est. losses from WTC exacerbated existing problem
    - Unsatisfactory return on capital for insurers before 9-11-01, much of the loss will be paid out of the industry capital account
  - Result
    - Coverage eliminated on many policies after 1-1-02 renewal date
    - Deductibles and premiums raised on other policies (e.g. Contingent Business Interruption Insurance) for less coverage
    - Insurers depending largely on actuarial data to assess terrorism risk
      - No data, no coverage
      - It could take three to five years for the private insurance industry to develop the means to cover terrorism**
    - Many firms resorting to more self-insurance
    - US Government seen as the insurer of last resort
      - "The only viable re-insurer for truly large-scale terrorism is the U.S. Government"*

* Source: Warren Buffett, Berkshire Hathaway
** Source: Swiss Re

Risk Management Response

- The risk as we know it….
  - Historically, terrorist groups that attack the U.S. target business
    - Since 1968 when the government first started tracking terrorism, 80 percent of attacks on U.S. interests have been on businesses *
  - Commonly-held opinions in the industry
    - Terrorism risk not insurable because it cannot be quantified
    - Losses from 9-11-01 ultimately resulted in reduction in coverage offered and increase in cost of coverage – most firms self-insure….
  - Limited tool sets available to assess risk of terrorism…
  - So how can the firm assess the risk to supply chains?

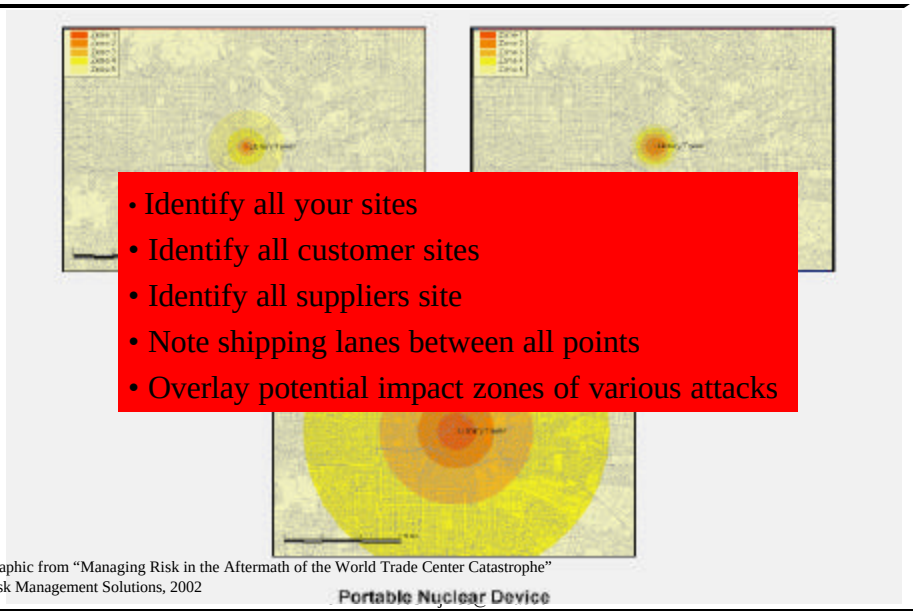
*Ambassador L. Paul Bremer, Chairman of the Crisis Consulting Practice at Marsh, Washington, D.C.

Terrorism Risk As We Now Know It

- Historically, terrorist groups that attack the U.S. target business
  - Since 1968 when the government first started tracking terrorism, 80 percent of attacks on U.S. interests have been on businesses *
- Commonly-held opinions in the industry
  - Terrorism risk not insurable because it cannot be quantified
  - Losses from 9-11-01 ultimately resulted in reduction in coverage offered and increase in cost of coverage – most firms self-insure….
- Limited tool sets available to assess risk of terrorism…
- So how can the firm assess the risk to supply chains?

*Ambassador L. Paul Bremer, Chairman of the Crisis Consulting Practice at Marsh, Washington, D.C.

One Approach: Map Attack Impact vs. SC



Graphic from "Managing Risk in the Aftermath of the World Trade Center Catastrophe"
Risk Management Solutions, 2002

Aggregate Risk to focus on Disruption

- Risk of Terrorist attacks is hard to predict
  - But the impact is not hard to predict – disruption
- According to the firms we interviewed….
  - The real risk of disruption cannot be seen by looking at terrorism risk alone
  - Currently, risk assessed by class of disruption
    - Terrorism, facility, personnel, theft, natural disaster
  - Separate assessment of each class leads to the conclusion that the risk is low for each class
  - Conduct an assessment of aggregate of disruption
    - Uncover a more holistic representation of the pattern of disruption

Failure Modes

- There are unlimited sources of disruption
- But there are a finite number of **failure modes**
  - Disruption in supply
  - Disruption in transportation
  - Freight breaches
  - Disruptions at facilities
  - Disruptions in communications

The Supply Chain as an Element of a Network

The Risk of Disruption

- September 11 did not change the threat or the risks
  - The risk of disruption just became more apparent
    - Personally, at home and at our place of work
    - At the borders, gateways
  - Some supply chains felt the disruption
    - Not so much from the attacks but from the response
      - Closed airspace, tighter border controls
      - Delayed supplies, shipments to customers
    - Many supply chains were minimally impacted
  - Apprehensive of the next disruption and wondering….
    - How should our supply chains prepare to respond?
    - Now 18 mos. later, do we understand the risk for our supply chains?

Risk of Disruption: Function of the Network

- Risk of disruption to the firm:
  - Is a function of the network of companies in the supply chain
  - Each party is dependent on the others in the network
    - Pan Am 103 – dependent on Malta Airlines for secure baggage
    - Chrysler – fuel sending unit dependent on sub-tier ink supplier, leaves drivers stranded with false fuel gauge readings
    - Disruption via sub-suppliers – a 10 min. fire in a Philips Electr. plant in New Mexico delayed RFCs (radio frequency chips) several weeks
      - Nokia detected erratic supply, responded first and fast to replace supply
      - Ericsson did not detect, $400 MM lost revenue, got out of the business
  - It's not possible to:
    - Control the entire supply network (exc. vertically integrated in one site)
    - Check every part from every direct and indirect (sub) supplier
- Firms need to assess the risk of disruption they are exposed to in their supply network

State-of-the-Art Risk Assessment

- Firms interviewed indicated no standard approaches or tools for assessing risk in the supply chain
  - Traditionally a qualitative assessment
    - Leaders appear to apply more quantitative methods
  - Quantitative assessments required … and motivating
    - $50-100 MM cost per day of disruption
    - "Lose the franchise"
    - Miss critical promotion window (e.g. 'back to school')
    - Risk financial insolvency without revenue stream of key products
    - Identify time until a disruption affects the customer
  - "Ultimately, you need to tie risk to business performance"
- Focus on failure modes and pattern of disruption there
- Recognize that the risk to the SC is a function of the network

Being dependent on others….

- Questions for your business: Can you…
  - Secure the supply chain?
  - Survive future attacks and other disruptions?
  - Respond and restore the supply chain to normal operations?

Corporate Response

Lit. Review of SC Responses after 9/11

- Various approaches were reported in use….
  - Bringing suppliers closer to the factory:
    - Ford building a supplier park (Chicago) to concentrate a tier 1, 2 suppliers
  - Alternative transportation modes as backup:
    - Chrysler used expedited truck service to backup air freight for parts from Virginia to Mexico immediately after 9-11-01
    - Continental Teves shifted to ocean transport and added 1+ weeks of inventory in lieu of air transport
    - Pfizer built strong relationships with carriers to be able to arrange fast ground transport in case the air system is shut down.
- Decentralized distribution:
  - Abbott Labs is expanding and decentralizing its distribution of some products
- Automation in material handling:
  - H-P is increasing automation to increase both efficiency and security
- Electronic seals and sensors on cargo:
  - Dell using smart seals on containers to indicate tampering en route
  - Wal-Mart adopted temperature monitors on trailers to ensure meat safety.

Corporate Response

- Firms participating:
  - 20 companies from across industry, primarily shippers with relationships with MIT
  - Industry segments represented include automotive OEMs and tier 1, high tech component manufacturers, aerospace, consumer products, contract manufacturers, medical devices
- Firms interviewed responded in four general classes
  - Basic
  - Reactive
  - Proactive
  - Advanced
- Classification is a function of
  - Breadth of response,
  - Intensity and type of initiatives taken to create a secure and resilient supply chain
- A path towards a higher level of response?

Firms Interviewed

- Avaya
- Bose
- Boston Scientific
- CH Robinson
- Cummins
- GE Aircraft Engines
- General Motors
- Gillette
- Hasbro
- Helix
- Intel
- Jabil
- Lucent
- Masterfoods
- P&G
- Reebok
- Shaws
- Taro
- Texas Instruments
- Welch's

Corporate Response Classifications

- Four classes of response – each level exceeds prior
  - Basic Response – Companies engage in broad security & preparedness activities (but not fully related to terrorism)
    - Physical security focus, limited internal contingency planning
  - Reactive Response – Companies firms show greater awareness of security vulnerabilities
    - Supply contingency plan, limited training
  - Proactive Response – Companies adopt newer security practices beyond industry norms, govt, customer reqts
    - Structured risk assessment, distribution contingency plan
  - Advanced Response – Companies lead new and progressive supply chain and security initiatives
    - Emergency Operating Centers, formal security strategy, cost-benefit analysis, contingency planning with customers-suppliers, flexibility contracts, learning from past disruptions

Corporate Response: Level 1 – Basic

- Level 1 – Basic Response
  - Companies may engage in broad security and preparedness activities (but not fully related to terrorism)
  - Some companies may have strengthened such programs and initiatives after 9/11. Basic responses include:
    - **Physical security measures**: Access control, badges, guards, camera systems.
    - **Standard risk assessment**: Consideration of risks such as fire, flood, vandalism, utility disruptions.
    - **Basic cyber security**: Anti-virus software, firewalls, passwords.
    - **Internal contingency plan**: How to recover within one's own operations.
    - **Freight protection**: Employee background checks, cargo seals, tracking technologies, sensors.

Corporate Response: Level 2 – Reactive

- Level 2 – Reactive Response
  - Exceeding Level 1 response, Reactive companies express greater awareness of security vulnerabilities.
  - Have typically altered or added supply chain and security initiatives since 9/11. Reactive responses include:
    - **Larger security, risk, or business continuity organizations**: This may have occurred either through reallocation of human or capital resources.
    - **C-TPAT compliance**: This may have occurred through either internal leadership or government pressure, but most importers have acted on this.
    - **Supply contingency plan**: Consequences of 9/11 and the threat of a new disruption in supply lead to the development of dedicated contingency plans.
    - **Limited training**: Select employees (not all) receive training or education on Level 1 and 2 initiatives.

Corporate Response: Level 3 – Proactive

- Level 3 – Proactive Response
  - Exceeding Level 2, Proactive companies adopt newer SC & security practices beyond industry norms, government, supplier, customer requirements. Responses include:
    - **Director or Chief of Security**: The existence of executive level positions with resources and responsibility for ensuring security.
    - **Ex-federal or ex-military personnel**: Leadership with military, law enforcement, or intelligence agency experience.
    - **Structured risk assessment**: Comprehensive and systematic approaches to analyze and understand their exposure to risk.
    - **Advanced cyber security**: Intrusion detection systems, relocation of IS in secure buildings, physical separation of the internal network from the Internet, auditing of partners' practices.
    - **Distribution contingency plan:** Developed alternative transportation plans in collaboration with logistics providers
    - **Participation in industry supply chain and security groups:** Strengthening industry via common policies, standards.

Corporate Response: Level 4 – Advanced

- Level 4 – Advanced Response
  - Exceeding Level 3, Advanced companies often lead new and progressive supply chain and security initiatives.
  - Often these efforts predate 9-11-01. Responses include:
    - **Customer-supplier collaboration**: Flexible contracts, shared contingency plans, alternative sources.
    - **Learning from past disruptions**: Building on past experiences to make their organizations stronger.
    - **Formal security strategy**: Developed and implementing a comprehensive, documented strategy, which is the base of all the initiatives put in place to increase security and resilience.
    - **Supply chain drills and mock exercises**: Perform training or exercises that include simulations of supply chain disruption.
    - **Emergency operating control center**: A facility to manage and coordinate the response to unexpected disruptions.
    - **Cost/benefit analysis**: Efforts to quantitatively understand the actual or expected costs and benefits of different alternatives.

Corporate Responses

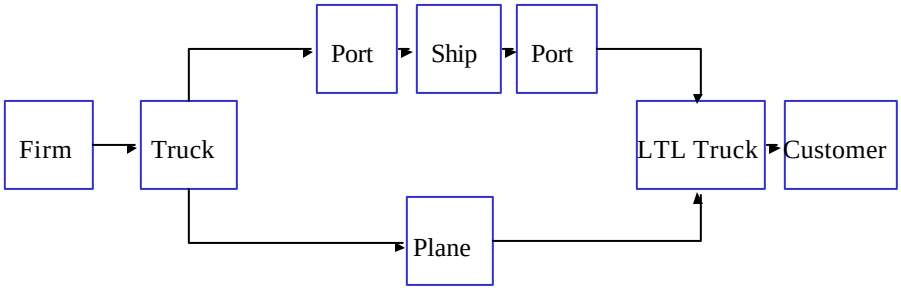
- Corporate responses being utilized
  - **Business Continuity Planning**
  - Supply Network Design
  - Learning from Past Disruptions
  - Emerging Progressive Practices

Business Continuity Planning

- Business continuity planning is …
  - Developing plans to regain or maintain continuous business operations when faced with a disruption
  - Requires a methodical process
  - Several approaches to surface the vulnerabilities
    - Map your supply network vulnerabilities and know your supply network
    - "Staple yourself to a shipment"*
    - Plan to 'fail smartly'**

* Reference to article titled "Staple yourself to an order" Harvard Business Review, July 1, 1992, B. Shapiro, V. Rangan, J. Sviokla
** "Fail smartly " was introduced in the article "Homeland Insecurity" by Charles Mann, The Atlantic, September 2002

"Staple Yourself to a Shipment"*

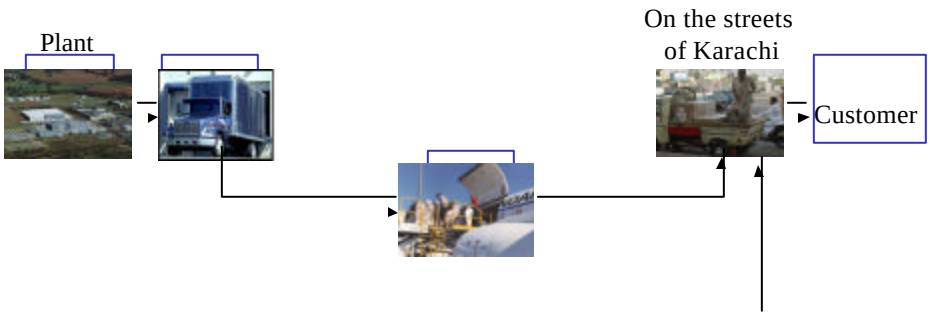


- Map your supply network … in detail
- Ask "What could go wrong?" at each point and link
- Identify how the firm could/would respond

* Reference to article titled "Staple yourself to an order" Harvard Business Review, July 1, 1992, B. Shapiro, V. Rangan, J. Sviokla

An Example: A Shipment to Karachi

A rush shipment of >$1mm in high tech materials from Boston to Karachi (circa 1996)



The firm discovered how their product maneuvered through to the streets of Karachi

All you need is one weak link: One reason to develop freight security standards

Business Continuity Planning: 'Fail Smartly'*

- Fail Smartly
  - Designing your supply network so that it is possible to restore operations post-disruption
  - An interesting way to think about business continuity planning but not truly different
- Premise
  - There will be disruptions
    - Terrorist attacks – direct and indirect, natural disasters
    - Supplier and/or customer business failure
  - Therefore plan for failure in a way that business operations can restart quickly

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

"Fail Smartly"* Examples

- Some misses
  - Medical device mfrs: Hospitals couldn't receive emergency shipments
    - 'Fail smartly' – Blast and Burn formulary, flexible receiving
  - Ericsson response to New Mexico fire
    - 'Fail smartly' – having orgz'l capability to sense disruption & take action
- Some 'fail smartly' cases, plans
  - Auto part supplier: Fire burned facilities, all data
    - Products could be made in alternate facilities, suppliers provided material info ("Send us what you sent last week"), back up in 2 days
  - Cantor Fitzgerald: Lost nearly all traders and their personal relationships
    - Failed smart by having most of traders' customer info captured, recaptured 50% of trades despite losing nearly all traders, back in the business
  - High tech equipment manufacturer
    - Plans in place for supplier to take on customer's production in emergency
  - Morgan Stanley
    - Had redundant IT system, back up 9-12-02 (learned from prior WTC attack)

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

Corporate Responses

- Corporate responses being utilized
  - Business Continuity Planning
  - **Designing for Resilience & Security**
  - Learning from Past Disruptions
  - Emerging Progressive Practices

Designing for Resilience and Security

- Resilience
  - "the ability to bend and bounce back from hardship"*
  - For supply networks: "the ability to react to unexpected disruption and restore normal supply network operations"
- Resilience ? Security
  - A secure supply chain is not necessarily a resilient supply chain
  - Design supply network for suitable levels of both security and resilience
- Organization design for resilience
  - Education important to identify resilience importance
    - Internal employees
    - Suppliers
  - Training critical for effective response

* "How Resilience Works" Harvard Business Review, May, 2002, Coutu, D.L.

Dimensions of Resilience

- Resilience: two types
  - Information system resilience at different levels
    - IT: From data backups to mirrored systems
  - Operations, supply network resilience at different levels
    - Operations: From restoring local, internal operations to restoring extended, external supply network operations
- Achieve resilience through different methods
  - Flexibility: responding through actions that entail prior investments in infrastructure and capabilities
    - Multi-skilled workforce, flexible production scheduling systems
  - Redundancy: responding through actions that entail prior investments in capital and capacity that may not be used
    - Inventory, additional production lines
  - What is the right mix for your supply network?

Supply Network Design: Resilience

- Flexibility
  - Ability to shift supply to a second source
  - Flexible contracts for upside demand
  - Multi-skilled workforce
  - Facility designed for multiple products and rapid changeovers
  - Design for resilience and security
  - Contract for additional transportation (option price)
- Redundancy
  - Inventory
  - Multiple suppliers (cost to qualify and maintain)
  - Committed contracts for supply
  - Additional converting/production capacity
  - Multiple sites
  - Dedicated transportation fleet
- What is the right mix for your supply network?

Corporate Responses

- Corporate responses being utilized
  - Business Continuity Planning
  - Supply Network Design
  - **Learning from Past Disruptions**
  - Emerging Progressive Practices

Learning From Past Disasters

- Impact of government response often greater than the disaster
  - Foot and Mouth Disease
  - Kobe Earthquake
  - 9-11-01 attacks
- Leaders learned from many non-terrorist attacks already
  - Quebec ice storm, tornados, Kobe earthquake, West Coast lock-out, anthrax scare, supplier bankruptcy, GM union strike
- Studying all disruptions emphasizes importance of
  - Business continuity planning (for **failure modes**)
  - Seeing company is dependent on network for security and resilience
  - Applying the learnings – but not all do….
    - Many Bhopal fatalities could've been avoided with basic evac training
    - Union Carbide experienced another potentially deadly gas leak after Bhopal because improvement actions from Bhopal were not applied
    - SQL Slammer virus attacked a problem that was 'fixed' 6 months prior

When Disaster Strikes

Crisis	Impact	Prepared Management	Unprepared management
Hurricane Mitch (Nov. 1998)	Floods destroyed banana plantations	Chiquita leveraged existing alternative sources	Dole took time to find alternatives and lost sales and
Taiwan Earthquake (Sep. 21 1999)	Component supplies to PC OEMs disrupted	Dell priced to steer customers to available components	Apple could not change config-faced backlogs and lost sales
Mad Cow & FMD (Spring 2001)	Shortage of hides for leather manufacturers	Gucci, Wilson – supply contracts; Naturalizer, Danier - inventories	Etienne-Agner suffered cost increases
9/11	Closed borders	Daimler-Chrysler Alt. modes based on contingency plans	Ford idled several plants

Source: Yossi Sheffi, SC Response Project 2002

Corporate Responses

- Corporate responses being utilized
  - Business Continuity Planning
  - Supply Network Design
  - Learning from Past Disruptions
  - **Emerging Progressive Practices**

Emerging Progressive Practices Adopted by Leaders

Progressive Practices (A)

- Collected from the range of interviews
  - Assessing the system vulnerabilities not just local or internal operations
  - On-site periodic assessment of supplier security
  - On-site periodic assessment of supplier ability to produce additional capacity
    - Quarterly Capacity Report Visits to Suppliers
  - Supply chain drills and mock exercises
  - Corporate Emergency Operations Center, EOCs
  - Flexibility contracts: 1 wk 25%, 4 wks 100%
  - Contract for airlift after 48 hours
  - Director of Security Role
    - Typically Federal law enforcement background
  - Recognizing and balancing tradeoffs of vulnerability/advantages of JIT
  - Informed assessment of dual-source, sole source (single-site) suppliers

Progressive Practices (B)

- Collected from the range of interviews
  - Connecting risk to business results in quantified measures
    - Financial, service impact
  - Structured risk assessment process related to business results
  - Shared contingency plans with suppliers and customers
  - Learning from past disruptions, building on the experiences
  - Variable-izing the costs to create resilience
  - Early detection systems
  - Consolidating the disruptions to see a holistic disruption profile
  - Supply network mapping through entire system critical
  - Organizational capability as critical skill set
    - Ability to respond, to recognize problem early on
    - Use of Demand Flow Technology for easy process adoption by low-skilled workers
  - Capturing business operations, customer, supplier knowledge in knowledge system accessible with backups
  - Coordinating with carriers for secure conveyance – identifying secure lanes, secure travel times, secure rest stops…..
  - Using dedicated and/or additional drivers on high risk lanes

Watchouts

- Responses have been active
  - Somewhat misguided in cases
  - Activity is good but….
- A False Sense of Security and Confidence
  - Depending on a second source of supply
    - Balance effort required for second source versus benefit
    - Will a second source of equal security and resilience increase your system security and resilience?
  - Dependence on C-TPAT as the sole security effort
    - Customs shares this concern…
  - Focus on local, internal security is good
    - But it does not address the security or resilience issues of the network
- Nearly all progressive practitioners had to experience pain first before responding…..
  - "It'll never happen to us"

Hurricane Andrew and Burger King

"Even the chief executive officer wasn't spared, Office of CEO of Burger King World Headquarters"*

* Reference – http://www.photolib.noaa.gov/historic/nws/wea00531.htm

Key Issues with Responding

- A false sense of security & confidence?
  - Responses have been active, but not all are holistic or comprehensive
    - A 2nd source may not the same security/resilience, or maybe less
    - "We're C-TPAT compliant, that's our plan"
    - Focus on facility security does not improve network security/resilience
  - Most leaders had to experience pain first before responding…..
- Cost for security & resilience?
  - What are the costs and who pays?
  - Are resilience and security free? "Collateral benefits" exist…
- Firms still faced with making tradeoffs*
  - Efficiency vs. redundancy, collaboration vs. secrecy, centralization vs. decentralization, low-cost vs. known supplier, security vs. privacy
- The human factor appears to be underestimated
  - No technology can really increase security if people are not reliable.
  - Resilience lies within people
    - Driven by the culture & the education and training invested

* Yossi Sheffi, SC Response Project 2002

Insights and Issues to Date

- Challenges for industry
  - Design for Resilience and Security… mix of flexibility & redundancy
  - Including all the necessary parties – shippers, carriers, agents, terminals – to develop a system solution
    - Prescribed solutions don't always work for carriers
  - A Voice for Industry to decision makers in emergency response
- Are resilience and security free?
  - "Collateral benefits" exist, and can offset additional costs
- Risk assessment process not developed into a science yet
- The human factor is often underestimated.
  - Technology alone cannot increase security if people are not reliable.
  - Ability to respond lies within the people, culture of an organization, the amount of education and training invested
- Who pays?
  - Ultimately, the end customer will pay, but
  - In the meanwhile shippers and carriers are bearing the costs.
  - Industry associations are asking the government to share the burden.

Insights and Issues to Date

- Challenges for industry
  - Design for Resilience and Security… mix of flexibility & redundancy
  - Including all the necessary parties – shippers, carriers, agents, terminals – to develop a system solution
  - A Voice for Industry to decision makers in emergency response
- Are resilience and security free?
  - "Collateral benefits" exist, and can offset additional costs
- Risk assessment process not developed into a science yet
- Firms still faced with making tradeoffs*
  - Efficiency vs. Redundancy, Collaboration vs. Secrecy, Centralization vs. Decentralization, Low-cost supplier vs. Known supplier, Security vs. Privacy
- The human factor is often underestimated.
  - Technology alone cannot increase security if people are not reliable.
  - Ability to respond lies within the people, culture of an organization, the amount of education and training invested
- Who pays?
  - Ultimately, the end customer will pay, but
  - In the meanwhile shippers and carriers are bearing the costs.
  - Industry associations are asking the government to share the burden.

Summary

- Government Response has been active
  - Needs to be coordinated and integrated with industry, new interdependencies
- Risk Management
  - Risk of disruption across the entire supply should be aggregated for a comprehensive understanding of the real risk
  - Risk to the supply chain is a function of the network
- Corporate Response
  - Some progressive leaders pioneering business continuity planning for the supply chain and making the supply chain secure
  - Focus on creating resilience for different failure modes
  - Resilient supply chains are not always secure supply chains
  - Make choices about source of resiliency: flexibility-redundancy mix
  - Assess security and resilience intimately for your entire supply network

Research Project Reference

- Project Web Sites
  - Home Page
    - http://web.mit.edu/scresponse/
  - Research Description Page
    - http://web.mit.edu/scresponse/research/index.html
  - Download of Prof. Sheffi's Article
    - "Supply Chain Management Under the Threat of International Terrorism"
    - http://www.logisticssupplychain.org/articles/pdfs/Terrorism.pdf
- Research Team
  - Prof. Yossi Sheffi, Principal Investigator
  - Jim Rice, Director, CTL ISCM and APL programs
  - Jonathan Fleck, Coordinator, CTL Corporate Relations
  - Federico Caniato, Visiting PhD student (Politecnico di Milano)
  - Deena Disraelly, LT USN, Candidate for Master Degree 2003
  - Reshma Lensing, Candidate for Master Degree 2003
  - Donovan Lowtan, Candidate for Master Degree 2004
  - John Perry, PhD Candidate 2005
  - Chris Pickett, Candidate for Master Degree 2003
- Contact information
  - Jim Rice <jrice@mit.edu> or via phone 617.258.8584

Questions?

Thank You