
Corporate Response to Terrorism: Creating Resilient and Secure Supply Chains

Global and Homeland Security: Science, Technology and the
Role of the University
MIT

James B. Rice, Jr.
May 2, 2003



© MIT 2003 jrice@mit.edu

Corporate Reponse

- How are firms' supply chains responding to terrorism?
 - Prof. Yossi Sheffi of MIT CTL initiated study to understand how different organizations respond to disruption (e.g. terrorist attacks, natural disasters, unexpected capacity loss)
- Preliminary insights from our study
 - Literature review
 - Detailed interviews with 20 firms associated with MIT
 - Considering corporate response in context of several factors
 - How the Government has responded
 - How the risk management and insurance industry has responded
 - How it may be possible to learn from past disruptions



© MIT 2003 jrice@mit.edu

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

© MIT 2003 jrice@mit.edu



Government Response – New Initiatives

- Monetary
 - \$75 B+ Homeland Defense spending since 9-11
- Regulatory
 - Aid Packages – SBA, FEMA, Aviation Industry
 - Reparative
 - Preventive and Preparatory
 - Department of Homeland Security
 - \$36 B 2004 budget, 200k employees, 22 Fed organizations
 - Over 100 new laws passed since 9/11/2001
- Federal Agency Actions
 - Many new initiatives – Public-Private Partnerships

© MIT 2003 jrice@mit.edu



Government Response – New Initiatives

- New legislation, spending, and initiatives
 - Involving government and industry to improve security
- New initiatives highlight new interdependencies
 - 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"

© MIT 2003 jrice@mit.edu



New Public-Private Partnerships

- New Interdependencies = a call for new Public-Private Partnerships with new needs and issues
 - Need to identify how to integrate industry and government
 - 'Voluntary' programs present conflicts for supply chain parties
 - Fundamental governance issues for the new systems
 - Coordination – How will new systems be coordinated?
 - Ownership – Who will own the new systems?
 - Control – Who will control the new systems? Decision-making?
 - Emergency response coordination between industry and government
 - Still need to fully integrate industry and industry!
 - Shipper – Carrier disconnect on securing the supply chain...
- New incentives for coordinating across the supply network in unprecedented ways
 - But it wont be easy

© MIT 2003 jrice@mit.edu



FAST vs. US-Mexico Border Agreement

- Similarities:
 - Fast lanes for rapid clearance of trans-border shipments
 - Enhanced supply chain security
 - Some means of expediting personnel transit
- Differences:
 - Potentially different technologies
 - Potentially different registration procedures
 - Potentially different identification requirements



© MIT 2003 jrice@mit.edu

Risk Management & Assessment

- Assessing risk problematic for firms
 - Actuarial method used by insurers not useful or timely
 - “No data, no coverage” so many firms resorting to self-insurance
 - For the firm, risk of terrorist attack is hard to assess
 - But the impact is not hard to assess and predict – **disruption**
 - Disruption will be one of a limited number of **failure modes**
 - Consider risk as an aggregate of various sources of disruption
 - Terrorism, fire, natural disaster, supplier failure, utility failure, employee strike, etc.
 - September 11 did not change the threat or the risks:
the risk of disruption just became more apparent
 - Personally, at home, at our place of work, at the borders, gateways



© MIT 2003 jrice@mit.edu

Risk of Disruption: Function of the Network

- The risk is a function of companies in supply network
 - 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 – Cell phone mgrs depend on RFCs
 - A 10 min. fire in a Philips Electronics plant in New Mexico delayed RFCs (radio frequency chips) several weeks
 - Nokia responded, Ericsson didn't and lost \$400M and the business
- But firms interviewed primarily use a qualitative, internal assessment, no standard approaches or tools
 - Quantitative assessments are needed... and motivating
 - \$50-100 MM cost per day of disruption
 - “Lose the franchise” by missing ‘back to school’ promotion
 - Risk financial insolvency without key product revenue stream

© MIT 2003 jrice@mit.edu



“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. Contingency planning is a bit of a misnomer since these events are really the norm, rather than the exception.”

Rob Carter, EVP & CIO, FedEx Corporation, 4-15-03

© MIT 2003 jrice@mit.edu



Corporate Response

- A variety of actions taken by firms in response:
 - Most advanced response: companies leading progressive supply chain and security initiatives across the network.
 - Emergency Operating Centers, formal security strategy, cost-benefit analysis, flexibility contracts, learning from past disruptions, extensive contingency planning (incl. with customers-suppliers)
 - Business continuity planning
 - Fail smartly, focused on failure modes
 - Building organization capacity to respond
 - Restructuring supply chain design for security & resilience
 - Bringing suppliers closer to the factory (Ford building a supplier park (Chicago) to concentrate a tier 1, 2 suppliers)
 - Alternative transportation modes (Continental Teves shifted to ocean transport, added 1+ wks inventory in lieu of air transport)
 - Technology Use
 - Ports adopting high-tech inspection equipment

© MIT 2003 jrice@mit.edu



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, flexibility contracts, learning from past disruptions, extensive contingency planning (incl. with customers-suppliers)

© MIT 2003 jrice@mit.edu



Business Continuity Planning: ‘Fail Smartly’*

- 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 supply network vulnerabilities, know supply network capacity
 - “Staple yourself to a shipment”**
 - Plan to ‘fail smartly’**
- Fail Smartly
 - Design the supply network to restore operations post-disruption without disruption to the customer
 - An interesting way to think about business continuity planning but not truly different

* Ref. to “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

© MIT 2003 jrice@ mit.edu



“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 in separate location, back up 9-12-02

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

© MIT 2003 jrice@ mit.edu



Designing for Resilience and Security

- Resilience
 - “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 designed for resilience
 - Human resource capabilities do make a difference, if not **the** difference
 - Ability to sense (e.g. Nokia)
 - Ability to respond (e.g. FedEx, but Bhopal gas leak illustrates org. failure)
 - Education and training important to build capacity internally and with suppliers/customers

* Adapted from “How Resilience Works” Harvard Business Review, May, 2002, Coutu, D.L.

© MIT 2003 jrice@mit.edu



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?

© MIT 2003 jrice@mit.edu



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?



© MIT 2003 jrice@mit.edu

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



© MIT 2003 jrice@mit.edu

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 be 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

© MIT 2003 jrice@mit.edu



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.

© MIT 2003 jrice@mit.edu



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



© MIT 2003 jrice@mit.edu

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



© MIT 2003 jrice@mit.edu

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

© MIT 2003 jrjce@mit.edu



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

© MIT 2003 jrjce@mit.edu



Questions?

Thank You



© MIT 2003 jrice@mit.edu