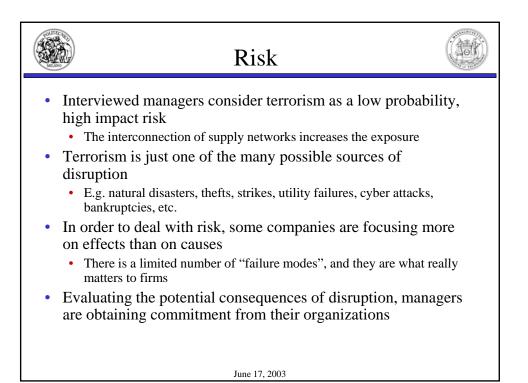


June 17, 2003



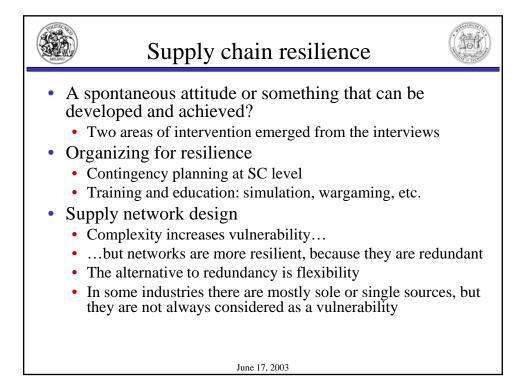


Research methodology and sample								
• Methodology								
• 20 semi-structured, explorative interviews								
• 3 case studies								
• Sample								
-	 Medium to large US based companies, generally operating world-wide 							
	 Heterogeneous sample in terms of industry, size and stage of the supply chain 							
 Respondents were either SC managers responsible for security or security managers responsible for the SC 								
	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				
June 17, 2003								



	Failure Modes
Failure Mode	Description
Disruption in supply	Delay or unavailability of materials from suppliers, leading to a shortage of inputs that could paralyze the activity of the company.
Disruption in Transportation	Delay or unavailability of the transportation infrastructure, leading to the impossibility to move goods, either inbound and outbound.
Disruption at Facilities	Delay or unavailability of plants, warehouses and office buildings, hampering the ability to continue operations.
Freight breaches	Violation of the integrity of cargoes and products, leading to the loss or adulteration of goods (can be due either to theft or tampering with criminal purpose, e.g. smuggling weapons inside containers).
Disruption in communications	Delay or unavailability of the information and communication infrastructure, either within or outside the company, leading to the inability to coordinate operations and execute transactions.
Disruption in demand	Delay or disruption downstream can lead to the loss of demand, temporarily or permanently, thus affecting all the companies upstream.
	June 17, 2003

Supply chain security						
	Advanced Initiatives					
rol, badges, ds, camera	• Test of security by an external					
firewalls, yorks, etc. intrusion antiviruses,	• Education and training for IS security					
nt initiatives	 Procedures, audits and certification Industry initiatives GPS, RFID, e-seals, biometrics, smartcards, security sensors, etc. 					
	June 17, 2					



Different paths towards the same goal

Company 1	Company 2	Company 11					
 Consolidated relationships with flexible SME suppliers, personal contacts Many sole and single sources Capacity audits of suppliers Agreements with a supplier to shift production to his site Demand Flow Technology Flexible workforce and temporary employees Duplication of IS and training to restore operations Direct management of transportation in case of emergency Suffered from Icestorm that hampered transportation 	 Strategy of exact plant replication in different countries Multiple sources for every part Creation of an industry association Emergency Operations Centers in every plant coordinated from the HQ Extensive simulations and drills Company culture stressing the attention to details Physical protection of facilities Suffered from thefts and various SC disruptions Staff from FBI, MI5, MI6, Mossad, Irish Garda, Hong Kong police, etc. 	 Flexibility written into contracts (+25% 1 week, +100% 4 weeks) Multiple sources wherever is possible Agreements with equipment providers to restore assembly lines in 4 weeks Unique IS across the world, also in acquired facilities Collaboration with logistics providers to ensure continuity of transportation Suffered from major theft Military personnel 					
June 17, 2003							

