

# Strategies for Maximizing Supply Chain Resilience: Learning From the Past to Prepare for the Future

By

Christopher B. Pickett

B.S. Industrial & Systems Engineering  
Virginia Polytechnic Institute and State University, 1998

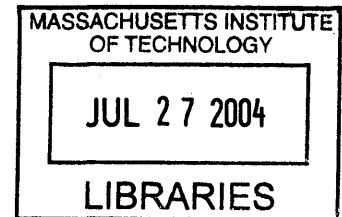
[ESD]

Submitted to the Department of Civil and Environmental Engineering  
in Partial Fulfillment of the Requirements for the Degree of

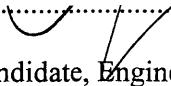
Master of Engineering in Logistics  
at the  
Massachusetts Institute of Technology

June 2003


©2003 Massachusetts Institute of Technology  
All rights reserved.




Signature of Author.....

  
Christopher B. Pickett  
M.E. Logistics Candidate, Engineering Systems Division  
May 9<sup>th</sup> 2003

Certified by.....

  
Yossi Sheffi  
Professor of Civil and Environmental Engineering  
Professor of Engineering Systems  
Thesis Supervisor

Accepted by.....

  
Yossi Sheffi  
Professor of Civil and Environmental Engineering  
Professor of Engineering Systems  
Co-Director of MIT Center for Transportation and Logistics

ARCHIVES

---

# **Strategies for Maximizing Supply Chain Resilience: Learning From the Past to Prepare for the Future**

By

Christopher B. Pickett

Submitted to the Department of Civil and Environmental Engineering  
On May 9<sup>th</sup>, 2003 in Partial Fulfillment of the Requirements  
For the Degree of Master of Engineering in Logistics

## **Abstract**

The terrorist attacks undertaken by Osama bin Laden's al Qaeda organization on the morning of September 11, 2001 ushered in a new era of indiscriminate global terrorism characterized by an unprecedented focus on security, risk management, and business continuity. The probability of future attacks, coupled with government response to the threat, has introduced myriad new challenges that virtually every manufacturer, distributor, and retailer engaged in global commerce must now face. This thesis will explore and analyze the impact that the "new" terrorist threat has, and will continue to have, on the supply chains of those manufacturers, distributors, and retailers by studying relevant historical disruptions; in essence, looking to the past to glean important insights as to how enterprises can best prepare for the future.

Throughout history, numerous disruptive events have occurred that bear comparison to a potential terrorist attack. These events include earthquakes, hurricanes, floods, industrial accidents, and labor strikes, as well as other terrorist attacks. By studying such events in detail and understanding the impact that they had on the supply chains of companies that were affected, important lessons can be learned regarding how best to prepare for, and react to, future disruptions. This thesis project ultimately seeks to collect, analyze, and synthesize historical data with the goal of presenting insights and conclusions that can be applied by businesses in the current operating environment to best prepare their supply chains for future disruptions, whether natural or man-made.

All research results are organized and presented in terms of the nature of the specific supply chain disruption (key supplier down, transportation capability disrupted, etc.), as opposed to the nature, location, or other defining characteristics of the disaster itself. Conclusions consist of a discussion of the unifying themes and the relevant lessons learned. The thesis then goes on to recommend ten prescriptive measures that organizations can take in today's business environment to strengthen their supply chains, minimize their exposure to future disruptions, and maximize their operational resilience.

Thesis Advisor: Yossi Sheffi  
Professor of Civil and Environmental Engineering  
Professor of Engineering Systems

---

## Acknowledgments

I would first like to acknowledge my thesis advisor, Dr. Yossi Sheffi, for his guidance, knowledge, and support throughout this process. I would also like to thank the rest of the core MIT Supply Chain Response to Terrorism team: Jim Rice, Jonathan Fleck, Deena Disraelly, and Don Lowtan, for all of their help over the last six months. I have learned a great deal from each of them and am grateful to have had the opportunity to work with such an outstanding team on such an interesting and relevant area of research. And of course, there is my partner in crime throughout this endeavor, Reshma Lensing. I would especially like to thank Reshma for her knowledge, advice, and most importantly, her friendship, over the course of this project.

I would also like to take this opportunity to acknowledge my mother, Debbie Pickett, my father, Bruce Pickett, my brother Stephen, and my sister Becky. Their unwavering confidence and constant encouragement kept me kept me moving in a positive direction regardless of how bad things may have seemed at the time.

Finally, I would like to thank my MLog '03 peers, my MIT professors and classmates, and my various ex-colleagues and friends who helped clarify my thinking and provided a constant source of insight and inspiration.

---

## Table of Contents

Abstract .....	2
Acknowledgments .....	3
List of Tables & Figures.....	6
<b>CHAPTER 1: INTRODUCTION.....</b>	<b>7</b>
1.1 September 11, 2001: A New Age of Global Terrorism.....	7
1.2 The Threat: How did we get here? .....	7
1.3 The MIT SCRT Research Initiative .....	8
1.4 Importance of the Research.....	9
1.5 Research Goals.....	9
1.6 Scope.....	10
1.6.1 Scope of Past Disruptive Events .....	10
1.6.2 Scope of Case Studies.....	11
<b>CHAPTER 2: METHODOLOGY.....</b>	<b>14</b>
2.1 Data Sources and Research Methods .....	14
2.2 Thesis Framework/Structure .....	14
<b>CHAPTER 3: LITERATURE REVIEW.....</b>	<b>15</b>
3.1 Summary Overview of Relevant Published Research.....	15
<b>CHAPTER 4: SURVEY OF PAST DISRUPTIONS .....</b>	<b>18</b>
4.1 Overview .....	18
4.2 Earthquakes .....	18
4.2.1 Taiwan Earthquake – 09/21/99 – Chi-Chi, Taiwan .....	20
4.2.2 Kobe Earthquake – 01/17/95 – Kobe, Japan.....	23
4.3 Severe Weather .....	27
4.3.1 Hurricane Andrew – 08/16/92 – Southeastern USA, Bahamas, Bermuda.....	27
4.3.2 Hurricane Mitch – 10/22/98 – South & Central America .....	29
4.3.3 Quebec Ice Storm – 01/04/98 – Northern U.S. and Canada .....	31
4.4 Floods.....	33
4.4.1 1993 Mississippi River Flood – Summer 1993 – Midwestern U.S.....	33
4.4.2 Central European Floods – Summer 2002 – Germany, Czech Republic, Austria .....	36
4.4.3 Seven Building Flood. – 01/06/02 – London, England .....	39
4.5 Fires.....	40
4.5.1 Philips Plant Fire – 03/17/00 – Albuquerque, NM .....	40
4.5.2 Avon Injected Rubber & Plastics Plant Fire – 04/02/99 – Albion, NY .....	42
4.5.3 Toyota P-Valve Supplier Plant Fire – 02/01/97 – Kariya, Japan.....	43
4.6 Port Explosions/Disruptions.....	46
4.6.1 Halifax Port Explosion – 12/06/17 – Nova Scotia, Canada.....	47
4.6.2 Texas City Disaster – 04/16/47 – Texas City, TX.....	49
4.7 Terrorist Attacks.....	52
4.7.1 1993 World Trade Center Bombing – 02/26/93 – New York City, NY .....	54
4.7.2 Oklahoma City Bombing – 04/19/95 – Oklahoma City, OK.....	55
4.7.3 9/11 Terrorist Attacks – 09/11/01 – NYC, DC, PA.....	57
4.8 Labor Strikes .....	60
4.8.1 1997 UPS Strike – 08/04/97 – Atlanta, GA.....	60
4.8.2 1998 General Motors Strike – 06/05/98 – Flint, MI .....	61
4.8.3 West Coast Port Lockout – 09/29/02 – Western U.S.....	62
4.9 Financial Distress .....	63
4.9.1 Land Rover/UPF-Thompson Case – 12/15/01 – UK .....	64

---

---

<b>CHAPTER 5: VULNERABILITIES OF THE MODERN SUPPLY CHAIN.....</b>	<b>67</b>
5.1 Survey of the Modern Supply Chain.....	67
5.2 Supply Chain Failure Modes.....	68
5.2.1 Physical Infrastructure Disruption (Non-IT).....	69
5.2.1.1 Oklahoma Federal Employee Credit Union – 04/16/95 – Terrorist Attack.....	69
5.2.1.2 New York Board of Trade – 09/11/01 – Terrorist Attack.....	72
5.2.2 IT/Communication Disruption.....	75
5.2.2.1 ING Canada Property & Casualty – 01/15/98 – Quebec Ice Storm.....	75
5.2.2.2 Merrill Lynch – 09/11/01 – Terrorist Attack.....	78
5.2.2.3 Sidley Austin Brown & Wood LLP – 09/11/01 – Terrorist Attack.....	80
5.2.3 Supply Disruption.....	82
5.2.3.1 Dole Vs. Chiquita – 10/22/98 – Hurricane Mitch.....	82
5.2.3.2 Dell Vs. Apple – 09/21/99 – Taiwan Earthquake.....	83
5.2.4 Manufacturing Disruption.....	84
5.2.4.1 Unilever – 10/28/98 – Hurricane Mitch.....	85
5.2.4.2 Compaq Computer – General Best Practices.....	85
5.2.5 Transportation/Distribution Disruption.....	86
5.2.5.1 Rocket USA Inc. – 08/04/97 – 1997 UPS Strike.....	86
5.2.5.2 Continental Teves – 09/11/01 – Terrorist Attack.....	87
5.2.5.3 Ford vs. Daimler-Chrysler – 09/11/01 – Terrorist Attack.....	88
5.2.5.4 Toyota/GM NUMMI Plant – 09/29/02 – Port Lockout.....	89
5.2.5.5 Dow Corning Corp. – 03/20/03 – 2003 U.S.–Iraq War.....	91
5.2.6 Demand Disruption.....	92
5.2.6.1 GHSP – 09/11/01 – Terrorist Attack.....	92
5.2.6.2 Cantor Fitzgerald – 09/11/01 – Terrorist Attack.....	93
<b>CHAPTER 6: SUPPLY CHAIN RESILIENCE STRATEGIES.....</b>	<b>97</b>
6.1 General Observations and Conclusions.....	97
6.2 Lessons Learned: 10 Steps to a More Resilient Supply Chain.....	98
6.3 Summary of Lessons Learned.....	109
6.4 Opportunities for Further Study.....	111
6.5 General Conclusions.....	112
<b>REFERENCES.....</b>	<b>113</b>
<b>APPENDIX ITEMS.....</b>	<b>121</b>
Figure 37.0 – Severe Weather Fatalities & Damage Costs: 1940 - 2001.....	121
Figure 38.0 – Significant Weather Events: 2001.....	122
Figure 39.0 – Seismicity of the United States: 1977 - 1997.....	123
Figure 40.0 – Seismicity of Europe: 1975 - 1995.....	124
Figure 41.0 – Seismicity of the Pacific Rim: 1975 - 1995.....	124
Figure 42.0 – Total International Terrorist Attacks: 1981 - 2001.....	125
Figure 43.0 – Total Terrorist Attacks by Region: 1996 - 2001.....	125
Figure 44.0 – HydroQuebec Electrical Grid at Peak Ice Storm Conditions.....	126

---

---

## List of Tables & Figures

Table 1.0 – Scope of Disruptive Events.....	10
Table 2.0 – Scope of Relevant Business Cases.....	11
Table 3.0 – Common Failure Modes.....	14
Figure 1.0 – The Efficiency vs. Resiliency Tradeoff.....	9
Figure 2.0 – Significant Worldwide Earthquakes: 2150 B.C. - A.D. 1994 .....	19
Figure 3.0 – U.S. Seismic Hazard Map.....	20
Figure 4.0 – 1999 Taiwan Earthquake .....	22
Figure 5.0 – Kyoto University team crossing collapsed bridge northeast of Fengyuen .....	23
Figure 6.0 – Kobe Earthquake Data.....	26
Figure 7.0 – Kobe Recovery Statistics.....	26
Figure 8.0 – Large Section of Hanshin Expressway Topples Over .....	26
Figure 9.0 – Remains of a furniture warehouse west of Whispering Pines, FL.....	28
Figure 10.0 – Hurricane Mitch Crop Damage, Honduras .....	30
Figure 11.0 – Mitch Caused Massive Road Damage, Honduras .....	30
Figure 12.0 – Area Affected by Quebec Ice Storm.....	32
Figure 13.0 – Tower Damage, Quebec Ice Storm.....	32
Figure 14.0 – 1993 Mississippi River Flood Region .....	35
Figure 15.0 – Pre-Flood St. Louis, MO.....	35
Figure 16.0 – Post-Flood St. Louis, MO.....	35
Figure 17.0 – Major Rivers and Cities Affected by 2002 Central European Floods .....	38
Figure 18.0 – Flood Damage in Prague, 2002 .....	38
Figure 19.0 – Halifax Explosion Blast Radius (S.S. Imo in Inset) .....	48
Figure 20.0 – Map of Galveston Bay and Texas City Harbor .....	51
Figure 21.0 – 150–ft Barge Washed Ashore by Tidal Wave, TX City Disaster.....	51
Figure 22.0 – Total Facilities Struck by International Attack, 2001.....	53
Figure 23.0 – Total Facilities Struck by International Attacks: 1996 - 2001.....	53
Figure 24.0 – Bomb Squad Investigators Look for Evidence after 1993 WTC Bombing.....	55
Figure 25.0 – Bomb Damage to Murrah Federal Building .....	56
Figure 26.0 – Terrorists Strike the World Trade Center, 9/11/01.....	59
Figure 27.0 – Footprint of WTC Damage, 9/11/01.....	59
Figure 28.0 – Modern Networked Supply Chain.....	67
Figure 29.0 – Potential Impact of Infrastructure Disruption.....	69
Figure 30.0 – Potential Impact of IT Disruption.....	75
Figure 31.0 – Potential Impact of Supply Disruption .....	82
Figure 32.0 – Potential Impact of Manufacturing Disruption.....	84
Figure 33.0 – Potential Impact of Transportation Disruption.....	86
Figure 34.0 – Potential Impact of Demand Disruption .....	92
Figure 35.0 – Recommended 3-Tier Cost Structure of Terror Insurance .....	108
Figure 36.0 – Milestones for Corporate Awareness of Supply Chain Vulnerabilities.....	109
Figure 37.0 – Severe Weather Fatalities & Damage Costs: 1940 - 2001.....	121
Figure 38.0 – Significant Weather Events: 2001 .....	122
Figure 39.0 – Seismicity of the United States: 1977 - 1997 .....	123
Figure 40.0 – Seismicity of Europe: 1975 - 1995 .....	124
Figure 41.0 – Seismicity of the Pacific Rim: 1975 - 1995.....	124
Figure 42.0 – Total International Terrorist Attacks: 1981 - 2001.....	125
Figure 43.0 – Total Terrorist Attacks by Region: 1996 - 2001.....	125
Figure 44.0 – HydroQuebec Electrical Grid at Peak Ice Storm Conditions .....	126

---

---

## **Chapter 1: Introduction**

### **1.1 September 11, 2001: A New Age of Global Terrorism**

On the morning of September 11, 2001, the world changed. A well-planned and highly organized strike – involving the simultaneous hijacking of four U.S. commercial airliners – was directed at multiple targets in New York City and Washington D.C. It was the worst international terrorist attack ever attempted on U.S. soil in modern history. And for all intents and purposes, it was very successful. Two of the planes struck and toppled the twin towers of New York City’s World Trade Center – one was flown into the Pentagon in Washington D.C. – and the third crashed, many believe prematurely, in a grassy field in rural Pennsylvania. The U.S. government’s response was immediate and far-reaching. Uncertain as to the likelihood of additional attacks that may have already been in progress, air traffic was grounded and security at border crossings was tightened to an unprecedented level. Until it could be determined that the skies and roads were safe, the airports remained closed and the borders remained clogged with trucks waiting to cross into the U.S. from Canada or Mexico to deliver their goods. For many businesses, the proverbial wheels of commerce were brought to a grinding halt. And for most of these companies, it was not the effects of the attack itself that disrupted their operations; it was the U.S. government’s response to the attack that did the most damage.

### **1.2 The Threat: How did we get here?**

Terrorist attacks, natural disasters, political upheaval, and industrial accidents are nothing new – most as old as commerce itself. But events like the Year 2000 (Y2K) computer upgrade frenzy, the 9/11 terrorist attacks, and even the West Coast port lock-out in the summer of 2002 have brought the risks to the forefront of global consciousness. It is not that disruptive events are necessarily occurring with any greater frequency or magnitude, but that enterprises now find themselves increasingly vulnerable to their effects. For the past two decades, there have been two major trends at work that have led to this new reality: Just-in-Time (JIT) manufacturing and rapid globalization.

The trend towards lean JIT manufacturing practices, adopted from the Japanese in the 1980s, has resulted in the evolution of very efficient, but very fragile supply networks. One of the goals of JIT is to minimize the level of raw materials, work-in-process (WIP), and finished goods inventory levels throughout the chain, which reduces the level of capital investment required,

---

---

freeing up that cash to more profitably allocate elsewhere. This means that firms will often carry only a day or two, much less in some industries, of inventory at various manufacturing locations. When parts deliveries are made as planned, the system functions beautifully. When the flow of goods is disrupted however, there is little, if anything, to prevent a major system interruption. Even minor delays can have a significant impact on downstream operations. And as enterprises regress towards leaner and leaner inventory levels, network supply chains are only left more and more vulnerable.

The increasingly global nature of business, combined with a prevailing trend towards outsourcing many activities once considered critical to ongoing operations, has also aggravated the situation. To take advantage of geographic cost advantages – proximity to markets, proximity to raw material sources, and low labor costs for example – enterprises have extended their supply networks on an unprecedented scale. For example, many companies have chosen to locate their manufacturing operations, whether internal or outsourced to a third-party, in China and along the Pacific Rim to exploit the relatively low cost of labor. While certainly offering significant savings in direct labor costs, this also exposes a company to new risks. Any number of potential supply chain disruptions can directly impact that company's ability to get their products to market in a timely and cost-efficient manner. And the greater the complexity (i.e. the number of nodes) and geographic dispersion (i.e. the distance spanned) of the supply network, the more vulnerable it tends to be to disruption. Figure 1.0 on the following page illustrates this *efficiency vs. resiliency tradeoff* that, often unnoticed until recently, has underpinned these trends over the last twenty years.

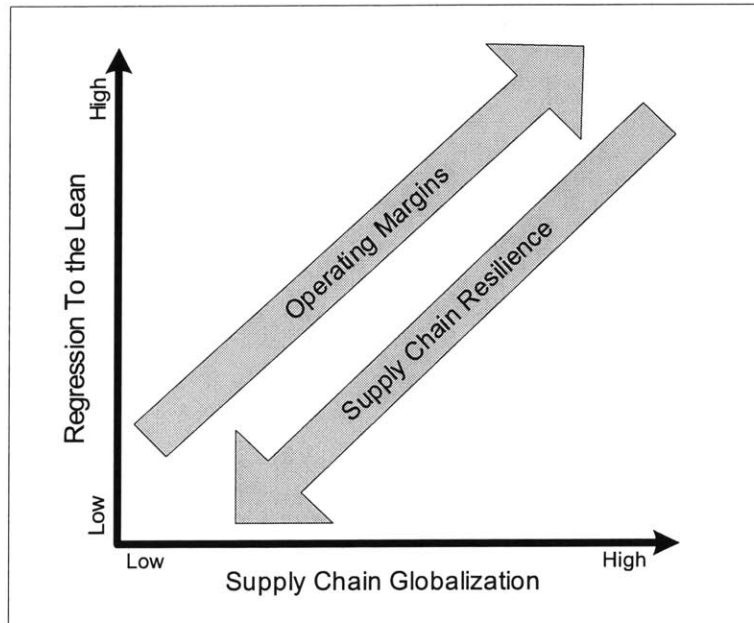
### **1.3 The MIT SCRT Research Initiative**

In response to the new era of indiscriminate global terrorism ushered in on the morning of September 11, 2001, a research project was initiated by the MIT Center for Transportation and Logistics to examine the new challenges facing virtually every manufacturer, distributor, and retailer that participates in global commerce. The Supply Chain Response to Terrorism (SCRT) research project was chartered to explore and analyze the impact that the “new” terrorist threat has, and will continue to have, on the extended supply chains of those manufacturers, distributors, and retailers.



---

**Figure 1.0 – The Efficiency vs. Resiliency Tradeoff**



#### **1.4 Importance of the Research**

Throughout history, numerous disruptive events have occurred that bear comparison to a potential terrorist attack. These events include previous terrorist attacks, natural disasters, industrial accidents, cyber attacks, and labor strikes. By studying such events in detail and understanding the impact that they had on the supply chains of companies that were affected, important lessons can be learned regarding how best to prepare for, and react to, future disruptions. This thesis will contribute to the SCRT initiative by looking to the past to glean important insights as to how enterprises can best prepare for the future.

#### **1.5 Research Goals**

The core research question(s) that this thesis seeks to address are:

- What, specifically, was the impact of the disruption to the supply chain or business operations of the affected enterprises?
- How did they react and/or recover (or not)?
- What insights can be gleaned from their experiences to help current enterprises prepare for future disruptions?

---

This thesis project ultimately seeks to collect, analyze, and synthesize historical data with the goal of presenting insights and conclusions that can be applied by businesses in the current operating environment to best prepare their supply chains for future disruptions, whether natural or man-made.

## **1.6 Scope**

The focus of this thesis is on past events that had a significant disabling affect on one or more supply chain nodes or functions of a given company or industry. For the purposes of this study, all events are of either a physical, financial, or labor-related nature and were selected with the goal of providing a broad base of data from which to compare and contrast their respective impact on affected supply chains. For, as this thesis will show, although the root causes of the disruptions may vary, the effects on the supply chains that they interrupt often do not. This means that a single general resiliency strategy can be implemented to minimize a supply chain's exposure to a wide range of potential disruptions. Please note that a similar 2003 MLog thesis project, titled *Historical Events and Supply Chain Disruption: Chemical, Biological, Radiological and Cyber Events* by Reshma P. Lensing, was conducted in parallel and focuses on disruptions of a cyber/digital, chemical, biological, or radiological nature.

### **1.6.1 Scope of Past Disruptive Events**

The events that were studied as a part of this thesis can be grouped into the following categories: earthquakes, severe weather, floods, fires, port explosions, terrorist attacks, labor strikes, and financial distress. Table 1.0, shown on the following page, provides an outline of the disruptive events that are discussed in further detail in Chapter 4.

---

**Table 1.0 – Scope of Disruptive Events**

<b>Event</b>	<b>Nature of Disruption</b>	<b>Date</b>
Kobe Earthquake	Earthquake	01/16/95
Taiwan Earthquake	Earthquake	09/22/99
Hurricane Andrew	Severe Weather	08/16/92
Quebec Ice Storm	Severe Weather	01/18/98
Hurricane Mitch	Severe Weather	10/22/98
1993 Mississippi Flood	Flood	Summer/93
Seven Building Flood	Flood	01/06/02
Central European Floods	Flood	Summer/02
Toyota P-Valve Supplier Plant Fire	Fire	02/01/97
Avon Rubber & Plastics Plant Fire	Fire	04/02/99
Philips Plant Fire	Fire	03/17/00
Mont Blanc Port Explosion	Port Explosion	12/06/17
Texas City Disaster	Port Explosion	04/16/47
1993 WTC Bombing	Terrorist Attack	02/26/93
Oklahoma City Bombing	Terrorist Attack	04/16/95
9/11 Terrorist Attacks	Terrorist Attack	09/11/01
1997 UPS Strike	Labor Strike	08/04/97
1998 General Motors Strike	Labor Strike	06/05/98
West Coast Port Lockout	Labor Strike/Lockout	09/29/02
UPF-Thompson Bankruptcy	Financial Distress	12/15/01

### **1.6.2 Scope of Case Studies**

In addition to the disruptive events outlined in Table 1.0 on the previous page, several cases where actual companies were faced with supply chain resiliency challenges were also included within the research scope of this thesis. All cases identified in Table 2.0, shown on the following page, pertain to one or more company's specific response to one of the past disruptions listed in Table 1.0 and discussed in Chapter 4. All cases are discussed in detail in Chapter 5.

**Table 2.0 – Scope of Case Studies**

Case	Event	SC Disruption
Oklahoma FECU	Oklahoma City Bombing	Non-IT Infrastructure
New York Board of Trade	9/11 Terrorist Attacks	Non-IT Infrastructure
Seven Asset Management	Seven Building Flood	IT Infrastructure
ING Canada Property & Casualty	Quebec Ice Storm	IT Infrastructure
Merrill Lynch	9/11 Terrorist Attacks	IT Infrastructure
Sidley Austen Brown, & Wood	9/11 Terrorist Attacks	IT Infrastructure
Dole Vs. Chiquita	Hurricane Mitch	Supply Base
Dell Vs. Apple	Taiwan Earthquake	Supply Base
Nokia Vs. Ericsson	Philips Plant Fire	Supply Base
Land Rover	UPF-Thompson Bankruptcy	Supply Base
Toyota Motor Corp.	P-Valve Supplier Plant Fire	Supply Base
Unilever	Hurricane Mitch	Manufacturing
Compaq	n/a	Manufacturing
Avon Rubber & Plastics	Avon Plant Fire	Manufacturing
Rocket USA Inc.	1997 UPS Strike	Transportation
Continental Teves	9/11 Terrorist Attacks	Transportation
Ford Vs. Daimler-Chrysler	9/11 Terrorist Attacks	Transportation
Toyota/GM NUMMI Shutdown	West Coast Port Lockout	Transportation
Dow Corning Corp.	2003 U.S.-Iraq War	Transportation
GHSP	9/11 Terrorist Attacks	Demand Disruption
Cantor Fitzgerald	9/11 Terrorist Attacks	Demand Disruption

As each of the disruptive events (Table 1.0) was studied, additional research focused on those companies that were impacted, either directly or indirectly, as follows:

**Direct Impact:**

A firm’s own physical assets were disabled or destroyed:

- Manufacturing capability
- Distribution capability (Warehouses, Distribution Centers, Private Fleets, etc.)
- Other assets or employees (Sales office, etc.)

**Indirect Impact:**

Assets of supply chain partners or were disabled or destroyed:

- Suppliers
- Contract Manufacturers
- Transportation/Distribution Service Providers
- Re-Sellers or Retail Outlets
- Major Customers

---

Transportation capability impacted:

- Caused by the event itself (roads destroyed, ports closed, etc.)
- Caused by response to event (border closings, etc.)

Affected companies were studied further to explore:

- How, specifically, were their supply chains or general business operations affected?
- What was the short-term and long-term impact of the disruption?
- How prepared were they?
- How did they react and recover (or not)?
- What lessons can be learned from their experiences?

---

## Chapter 2: Methodology

### 2.1 Data Sources and Research Methods

The data collection and analysis methodology employed for this project consisted primarily of library and internet-based research, and was supplemented with brief interviews and/or additional research methods as was deemed both useful and feasible.

### 2.2 Thesis Framework/Structure

A primary theme of this thesis is that it is important to focus not necessarily on the nature of a disruption, but on how business operations are likely to be impacted. Thus, organizations should focus on the failure modes, not the failures themselves. Firms cannot foresee every potential threat, let alone the probability of it occurring at each point in a complex and rapidly expanding supply network. It simply isn't feasible, nor would it be practical. For example, before September 11<sup>th</sup>, 2001, a company could not realistically have been expected to plan for a plane hitting its building. Luckily, firms should not have to. As this study will show, a wide variety of disruptions tend to have very similar effects on a company's supply chain. Therefore, the examples and cases discussed in Chapter 5 are organized and presented by the nature of their impact on the supply chain, or by the ways in which a supply chain can generally break or fail. These are referred to as a supply chain's failure modes. The failure modes identified and used in this study are listed below in Table 3.0 below and are described in further detail in Chapter 5.

**Table 3.0 – Common Failure Modes**

<b>Failure Mode</b>	<b>Description</b>
Non-IT Physical Infrastructure	Loss of non-IT related assets like staff, office locations, etc
IT Assets/Infrastructure	Data loss, communication links so supply chain partners, etc
Key Supplier	Ability to source a key component, etc.
Manufacturing Capability	Ability to produce goods and/or services for sale
Distribution/Transportation Capability	Ability to move raw materials or finished goods throughout the supply chain
Key Customer	Loss of one or more key customers

---

## Chapter 3: Literature Review

### 3.1 Summary Overview of Relevant Published Research

The focus of this thesis is on historical events that had a significant disabling affect on one or more supply chain nodes or functions of a given company or industry. For the purposes of this study, all events are of either a physical, financial, or labor-related nature and were selected with the goal of providing a broad base of data from which to compare and contrast their respective impact on affected supply chains. So with this focus solely on past events, it is important to note that all data was collected from previously published works. A vast majority of data came from publications that were written with one of the following two purposes:

1. To explore the subject of general supply chain resiliency or security, or
2. To review a specific disruptive event and/or its effect on a specific company

While the numerous publications written with the purpose of reviewing a specific event (2) were certainly useful in understanding their particular topics, the real value to the subject of supply chain resiliency was realized only when analyzing them in the context of other events. By evaluating the aggregate body of disruption data, several important insights and unifying themes were identified, which are detailed in Chapter 6.

In contrast, the publications written to explore the subject of general supply chain resiliency (1), while far fewer in number, were extremely important in guiding the research for this thesis and providing a basis from which to extend the current body of knowledge. While only three publications fell into this category, all were invaluable to the author and are summarized below.

- Sheffi, Y. (2001). Supply Chain Management under the Threat of International Terrorism, International Journal of Logistics Management, v. 12, no. 2.

Dr. Sheffi's paper was the catalyst for MIT's Supply Chain Response to Terrorism (SCRT) research initiative and for this thesis project specifically, which his is also the faculty advisor for. The paper looks at the dual corporate challenges of preparing to deal with the aftermath of terrorist attacks and operating under a new steady state of heightened security. The first challenge relates to setting certain operational redundancies. The second implies less reliable lead times and less certain demand scenarios. Dr. Sheffi's paper also discusses ways by which

---

---

companies should organize to meet those challenges efficiently and goes on to suggest a new public-private partnership. Specifically, the paper identifies and explores the following tradeoffs:

- Efficiency Vs. Redundancy
  - Collaboration Vs. Secrecy
  - Centralization Vs. Dispersion
  - Lowest Bidder Vs. Known Supplier
  - Security Vs. Privacy
- 
- Martha, J. & Vratimos, E. (2002). Creating a Just-in-Case Supply Chain for the Inevitable Next Disaster. Viewpoint Magazine, no. 2. Marsh & McLennan Companies, Inc.
  - Martha, J. & Subbkrishna, S. (2002, September 1). Targeting a Just-in-Case Strategy for The Next Inevitable Disaster. Supply Chain Management Review.

The Martha & Vratimos and Martha & Subbkrishna papers address the subject of supply chain resiliency from a more disruption-agnostic perspective, much as this thesis does. Both draw attention to the notion that natural disasters, wars, and political upheavals occur regularly around the globe, but only recently was supply chain risk brought to the forefront of corporate consciousness. Only when the September 11<sup>th</sup> terrorist attacks on the World Trade Center and the Pentagon caused widespread transportation delays, resulting in costly inventory shortages and plant shutdowns for many U.S. manufacturers and goods shortages for many retailers, did firms finally begin to understand the vulnerabilities of the modern networked supply chain. The papers also go on to identify the trend towards lean Just-in-Time manufacturing and logistics practices as a contributing factor to the resiliency issue.

Additionally, both papers briefly discuss various real-world examples of companies that were faced with major supply chain disruptions. In fact, several of the case studies included in this thesis are based on cases identified in this paper. These include, among others:

- Dell Vs. Apple
- Dole Vs. Chiquita
- Continental-Teves
- Daimler-Chrysler Vs. Ford



- 
- Helferich, O. & Cook, R. (2002). Securing the Supply Chain. Council of Logistics Management Research Report.

This report, sponsored by the Council of Logistics Management, was also triggered by the events of September 11<sup>th</sup> and encompasses the general issues of preparedness and response and goes on to provide a classification of major events that are likely to disrupt supply chain performance. Dr. Helferich and Dr. Cook introduce a resiliency analysis framework that can be summarized as:

Planning → Mitigation → Detection → Response → Recovery

As the authors explain, the process begins with preparing the enterprise and the supply chain for the unforeseen event-disaster through development of formal “planning”. Preparedness includes defining actions to reduce the impact of a disaster, referred to as “mitigation”. The next stage in the preparedness process is “Detection”, which is necessary given that some disasters such as release of biological agents are not easily identified until medical symptoms appear. “Response” involves preparing for the actions that will be taken by enterprise employees, the general community, the emergency first responders, and emergency relief. The final stage involves executing a strategy to resume normal business and community functions called “recovery”.

The overall objective of the paper is to develop a planning framework and provide the supplemental tools that will assist the supply chain continuity management team through each stage of the disaster management process.

- Lensing, R. (2003). Historical Events and Supply Chain Disruption: Chemical, Biological, Radiological and Cyber Events. (Masters Thesis, Massachusetts Institute of Technology, 2003).

An additional source of information that was used to help shape the direction of the research was another 2003 MLog thesis project, undertaken by Reshma P. Lensing, that focuses on disruptions of a cyber/digital, chemical, biological, and/or radiological nature. The Lensing paper and this thesis were developed in parallel and are designed to provide a comprehensive view of supply chain resiliency under a broad array of potentially disruptive conditions.

---

## **Chapter 4: Survey of Past Disruptions**

### **4.1 Overview**

The disruptive events that were studied as a part of this thesis can be grouped into the following categories: earthquakes, severe weather, floods, fires, port explosions, terrorist attacks, labor strikes, and financial distress. All vary significantly by frequency, magnitude, and scope, but in many cases, tend to affect the supply chains of affected companies in very similar ways. For example, it will not matter much to a large auto manufacturer whether the flow of components from a key supplier was disrupted by an earthquake, a plant fire, or a government-imposed border closing. What matters is that the flow of those components was compromised and now that auto manufacturer must respond to minimize the impact of the disruption on their operations. They must be resilient regardless of the root cause.

### **4.2 Earthquakes**

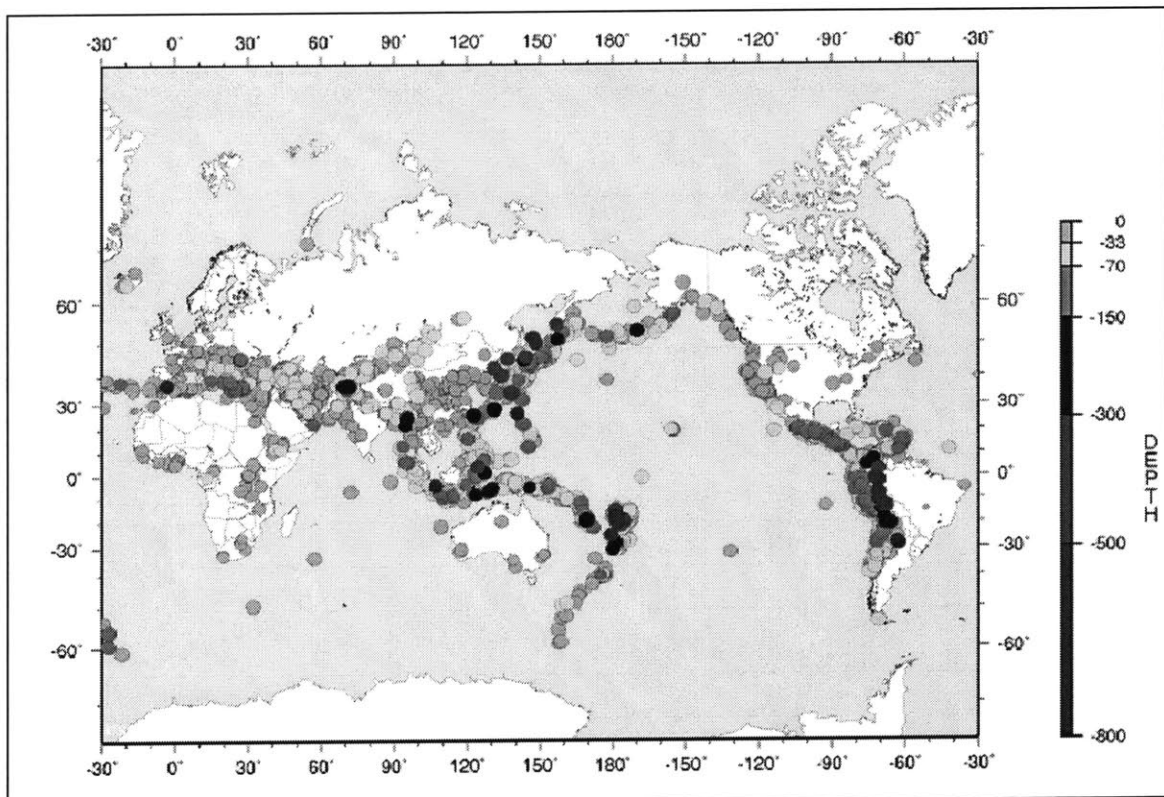
The destructive power of an earthquake can be awesome. In just seconds, it can topple buildings, collapse bridges, and destroy roads. And while a company's general exposure to earthquake risk can be predicted to some degree by the proximity of supply chain nodes to known fault lines or areas of geological instability, the factors that influence earthquake frequency and magnitude are still a relative mystery. There is no early warning system. And given the relative infrequent nature of major quakes, there are often many benefits from locating a supply chain node in a seismically active region that justify the risk. The Pacific Rim, for example, is a known earthquake hot-spot yet low costs of labor and other factors have attracted billions of investment dollars used to build manufacturing capacity in the region. But while the risk of an earthquake is not normally sufficient in and of itself to direct investment decisions, a prudent company should be aware of its general exposure and have a plan in place should disaster strike.

To determine one's earthquake risk, geographic location is the primary driver. Companies that have operating assets near seismically active areas are much more vulnerable than companies that do not. And as the historical data summarized in Figure 3.0 on the following page shows, the active areas are fairly well delineated from the inactive areas. Figure 4.0 goes on to attribute a degree of earthquake risk to every region within the United States according to known seismic

activity. This map was developed with the assistance of the U.S. construction industry and the rating system was, in part, influenced by national U.S. building codes and the known vulnerabilities of structures built under those codes to specific types of earthquake activity. According the U.S. Geological Survey, similar maps have not yet been developed for areas outside the United States. However, for a summary of significant earthquake activity in the U.S., Europe, and the Pacific Rim from 1975 – 1995, please reference Figures 39.0 – 41.0 in the Appendix. All data was sourced from the U.S. Geological Survey (2003).

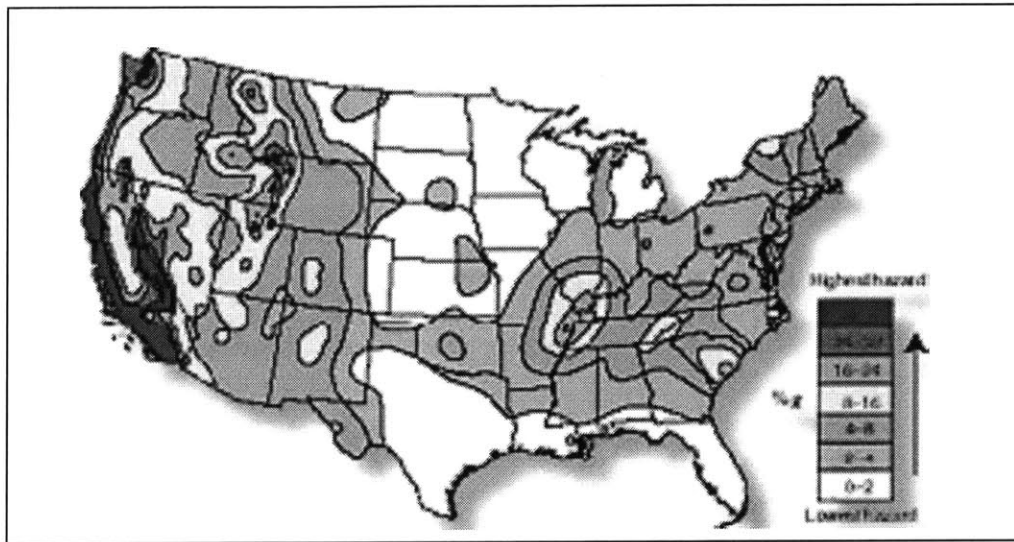
Once a company understands its likely exposure to earthquake risk, it can then incorporate that into its general supply chain resiliency strategy. And to better understand what the potential impact of such a disruption could be, the 1995 Kobe, Japan and 1999 Chi-Chi, Taiwan earthquakes were studied in detail as a part of this thesis and are profiled in the following pages.

**Figure 2.0 – Significant Worldwide Earthquakes: 2150 B.C. - A.D. 1994**



Source: USGS, <http://neic.usgs.gov/neis/eqlists/eqstats.html>

**Figure 3.0 – U.S. Seismic Hazard Map**



Source: USGS, <http://geohazards.cr.usgs.gov/eq/html/graphics.html>

#### **4.2.1 Taiwan Earthquake – 09/21/99 – Chi-Chi, Taiwan**

At 1:47 a.m. on September 21, 1999, an earthquake struck Taiwan with a destructive force that registered 7.6 on the Richter scale. Its epicenter was approximately 7 km northwest of Chi-Chi, a small town bordering a mountainous resort area, and located 155 km from the capital city of Taipei. The ground shook severely for 40 seconds and was felt throughout the entire island. In the subsequent days, several large aftershocks followed – four with a magnitude greater than 6.5. This, the Chi-Chi earthquake was the most devastating to hit Taiwan since a 7.1 quake struck the Hsinchu–Taichung region in 1953, killing over 3,500 people.

The earthquake toppled structures, including two tall buildings 150 km north in Taipei, and generated numerous landslides throughout the areas surrounding the epicenter. And to complicate the rescue and recovery efforts, numerous road sections (see Figure 5.0) were heavily damaged by the landslides and the shifting of the ground at major fault lines. When the dust settled, the death toll had exceeded 2,400 and over 10,700 people had been injured. Over 8,500 buildings were destroyed and another 6,200 were significantly damaged.

There was also a significant level of business disruption due to an island-wide power outage. An RMS Research note (2000) reported that while overall economic losses topped \$12B, a significant portion of the \$600M in insurance claims came from business interruption losses associated with the power outage. The Hsingchu Science Park, located 110km from the

---

epicenter, suffered some of the most significant damage. Hsingchu is the site of the Science Based Industrial Park, a major development where roughly 30 companies provide a significant percentage of the total global semiconductor manufacturing and silicon processing. The overwhelming problem caused by the earthquake was a loss of electrical power rather than any significant structural damage. As described in an EQE research report (1999), “almost all of the Science Park was down for several days, resulting in business interruption costs of about \$50M to \$100M per day. Earthquake damage to distant 345 kV transmission towers and a switching station made it impossible for the park to receive power from the usual steady supply from the south of Taiwan. Power was slowly restored to major users in the area by rationing residential and small commercial customers in other parts of the country, including Taipei. Some facilities were able to maintain emergency power with the use of generators, although with varying success. One wafer fabrication company sustained a large loss when the generators burned up after running continuously for 40 hours after the earthquake. And with loss of the standby power, this facility went completely black, and lost power to the fans that maintain the clean room environment” (EQE, 1999). The Dell vs. Apple case discussed in Chapter 5 describes how the two leading PC manufacturers were directly impacted by the disruption in the flow of critical components from these Taiwanese suppliers and how they each responded, both with varying levels of success.

It has been widely acknowledged in research reports – including both the RMS and EQE reports referenced here – that the significant business interruption to the high-tech industry could have been minimized with adequate seismic reinforcement of equipment and the proper execution of a recovery plan that would have more specifically addressed an island-wide failure of the power grid. In fact, the lack of redundancy in the power grid was a risk that had been identified well before the '99 quake. Construction of a back-up line in Hsingchu had begun several years earlier, but the project had been placed on hold until land acquisition problems could be resolved (EQE, 1999). But as unprepared as they were, the magnitude of the disruption could have been much, much worse. The only thing that saved the companies with plants located in Science Park, and the computer technology supply chains that depended on them, from more profound damage, was their distance from the epicenter. In that respect, the 1999 Chi-Chi earthquake should serve as a wake-up call not only for Hsingchu, but also for similar areas of concentrated manufacturing and/or development capacity. For, as EQE (1999) attests, “the building and equipment vulnerabilities at The Hsingchu Science Park are not much different from those in

---

---

other high-tech parks like Silicon Valley in California, where the earthquake threat is as great and is increasing over time” (EQE, 1999).

The port area of Taichung was also significantly affected, despite its distance from the epicenter and major fault lines. For reference, the map shown in Figure 4.0 below illustrates the quake’s scope of damage with the major fault lines shown as dark lines that crisscross the island. Liquefaction of the deep silty sand layers below the reclaimed land that Taichung was built on was severe and resulted in many wide sink holes, some up to 20 m wide. While the rebuilding efforts lasted over two years, the net disruption in Taiwan’s shipping capability was not significant. While the port’s capacity was constrained during the period of recovery, shipments were re-routed to other Taiwan ports that were not so severely damaged (EQE, 1999).

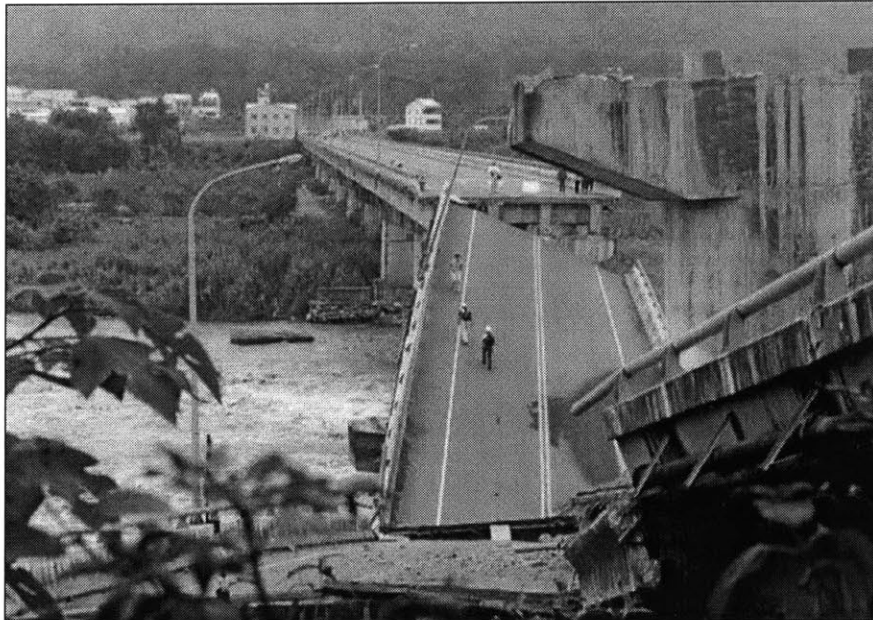
**Figure 4.0 – 1999 Taiwan Earthquake**



Source: ABCNEWS.com/ Magellan Geographix  
<[www.abcnews.com/sections/world/DailyNews/taiwan\\_quake990921.html](http://www.abcnews.com/sections/world/DailyNews/taiwan_quake990921.html)>

---

**Figure 5.0 – Kyoto University team crossing collapsed bridge northeast of Fengyuen**



Source: Chi-chi (Taiwan) Earthquake Information  
<http://www2.rcep.dpri.kyoto-u.ac.jp/~sato/taiwan/twpics/captions/tw003.html>

#### **4.2.2 Kobe Earthquake – 01/17/95 – Kobe, Japan**

At approximately 5:46 a.m. on January 17<sup>th</sup>, 1995, as most of its citizens slept, western Japan was rocked by the largest and most destructive earthquake to hit Japan since 1923. The “Hyogoken Nanbu” earthquake, which registered 7.2 on the richter scale, made its epicenter only 20km southwest of the port city of Kobe. The magnitude and proximity to such a densely populated region resulted in massive property damage and significant loss of life. The devastation was the worst in Kobe, where the quake toppled roadways, destroyed docks, severed communication, and ruptured natural gas lines which kept the city in flames well into the next day. When the dust settled, hardly a block in the industrial port city of 1.4 million people had a house or building intact. Many streets were rendered impassable with scattered mounds of rubble effectively blocking any all traffic. Over 5,250 people lost their lives while 30,000 were wounded, causing a critical strain on area hospitals. The same effect could be seen at makeshift shelters, which struggled to help the more than 400,000 citizens left homeless.

Kobe, Japan was the sixth largest port in the world and the gateway for 12% of Japan's exports. As Richard Arnold (2001) notes, “no earthquake had struck any major Japanese urban center with such destruction since the great Kanto earthquake of 1923 which killed 140,000 people in Tokyo and Yokohama” (Arnold, 2001). Japan is one of the most geologically unstable places on

---

Earth. The country has 40 active volcanoes that can produce up to 1,500 tremors in any given year, most of them considered minor. To combat the effect of this constant threat, the risk of earthquakes is considered heavily in architecture and civil defense planning. In fact, the majority of buildings that collapsed as a result of the Kobe quake were those with wooden walls that failed under the rocking of their heavy tile roofs. Most of the steel-framed buildings, built after 1981, were designed to bend without collapsing and suffered very little damage from the 20 seconds of severe shaking.

The worst effected area was in the Kobe's central region, a 5km by 20km area alongside the main docks and port area. This area was built on soft and easily moved rocks. The port itself was built on reclaimed ground similar to the port operations of the U.S.'s San Francisco bay. Here, the ground literally liquefied and acted like thick soup. This allowed buildings to topple sideways, resulting in many of the huge cranes in the harbor toppling over into the sea. All but 4 of the 239 shipping berths were damaged in the quake. To make matters worse, severe damage to roadways and rail systems confounded rescue and cleanup efforts in the days and months following the disaster. The worst damage was along the Hanshin Expressway, a major artery between Osaka and Kobe, which collapsed in five places and killed twelve motorists. An example of the damage can be seen in Figure 8.0 below. Other major roadways were damaged in 20 places. The Shinkansen, Japan's famous high-speed "bullet" trains, were slowed to a crawl when rails were damaged in 36 places. Local and commuter trains also sustained significant damage. Airports, on the other hand, were only slightly delayed. Kansai International Airport, built on Osaka Bay, was closed only temporarily on the day of the quake.

The massive failure of key infrastructure assets also played havoc on rescue and recovery efforts. As in most cities, water, gas, electricity, and sewage services were provided via a network of underground pipes and cables. When the ground began to shift, many of the rigid pipes could not flex and quickly fractured. As a result, approximately three quarters of the city's water supply compromised while natural gas lines leaked freely into the air and sewers discharged their contents into the streets. Although much of the city's electricity was routed through above-ground cables, they fared no better. Hundreds of Kobe's utility poles collapsed during the earthquake, cutting off electricity to homes, businesses police and fire stations, and even hospitals. As described at the Geography Resources for Teachers and Students Website (GRTS) (2003), "the collapse of the electricity and telephone systems made it almost impossible for



---

people to let the fire teams know where they were needed, whilst the broken water pipes and blocked roads made it hard for fire teams to reach and put out fires” (GRTS, 2003).

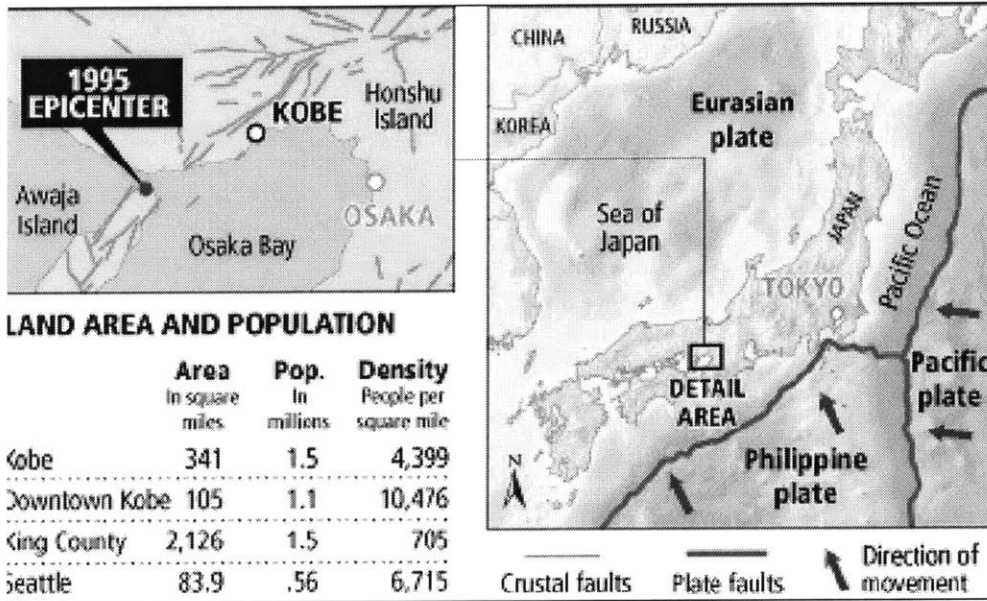
The impact to Kobe’s manufacturing base was also significant. Not immune from the complete failure of much of the city’s infrastructure, major electronics, steel, and heavy industry manufacturing plants were forced to close for several days. As the Kobe Earthquake Summary website (2003) attests, “many businesses were critically affected by severe employee absenteeism and disruption of infrastructural services such as phone lines, electricity, gas and water. Smaller firms also suffered heavy damage to building structures or contents. More than 40% of local knitted goods and over 90% of leather shoe manufacturing facilities were severely affected. One week after the quake, 190 companies were unable to obtain water for industrial consumption (Kobe Earthquake Summary website, 2003). The indirect effects of the disaster were also significant. For those firms fortunate enough to quickly recover manufacturing capacity, additional disruptions were the result of difficulty in obtaining direct materials and other supplies. Major business disruptions included:

- Toyota Motor Corp. cut production by 20,000 cars because of problems finding supplies,
- Hanshin Electric Railway suffered \$895M in damages to rail facilities, and
- Osaka Gas lost \$170M to pipe repairs and an estimated \$68M in lost revenues.

The massive damage to Kobe’s port operations made a serious dent in the port’s transport capacity – a reported 2.7 million containers shipped each year. Manufactured goods from Mitsubishi, Mazda, Toyota, and many other companies with facilities in the area had to be re-routed via truck and rail to secondary ports throughout Japan. It took over two years to restore Kobe’s port operations to pre-earthquake capacity.

Recovery efforts lasted several years and required over \$147B, making Kobe the most expensive disaster in recorded history. And this figure does not even factor in the indirect economic impact of the many business disruptions and lost manufacturing capacity. A summary of both the scope of impact and the timeline for restoring Kobe’s critical infrastructure are shown in Figures 6.0 and 7.0 below.

Figure 6.0 – Kobe Earthquake Data



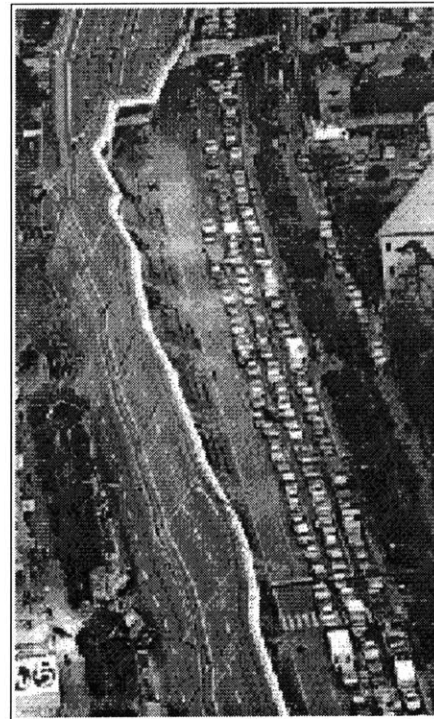
Source: Seattle Post-Intelligencer, 2002  
[http://seattlepi.nwsourc.com/local/60379\\_kobequake.shtml](http://seattlepi.nwsourc.com/local/60379_kobequake.shtml)

Figure 7.0 – Kobe Recovery Statistics



Source: Seattle Post-Intelligencer, 2002  
<http://seattlepi.nwsourc.com/local/60379>

Figure 8.0 – Large Section of Hanshin Expressway Topples Over



Source: J.P. Bardet, USC  
<http://www.seismo.unr.edu>

---

### 4.3 Severe Weather

Unlike earthquakes, severe weather occurs with no recognizably consistent pattern, at least not over the long-term. This means that the severe weather hot spots are not as clearly delineated from more tranquil areas. They can, however, be predicted with much greater short-term accuracy which allows for at least some degree of warning. In the context of this thesis, severe weather is a term that is meant to comprise destructive meteorological events like hurricanes, tornados, and winter storms. Their strike area, frequency, and magnitude, are all functions of rapidly changing weather variables that have yet to be completely understood. So while one cannot quite so easily determine whether or not they are vulnerable to severe weather by where they sit on a map, having a sound recovery strategy becomes all the more important. To illustrate this point, Figure 38.0 in the Appendix summarizes the significant weather events that occurred in the U.S. in 2001. Outside of the relative immunity of the western states to weather disruptions, there are no readily discernible patterns in terms of the type of event, the magnitude, or the frequency. It may be interesting to note that although the western states appear to have suffered far fewer weather events in 2001 than the eastern or middle states, the opposite pattern can be seen in U.S. seismic activity (Figure 39.0, Appendix). In terms of exposure, there is simply no place to hide.

To better understand what the potential impact of such a disruption could be, Hurricane Andrew (1992), Hurricane Mitch (1998), and the 1998 Quebec Ice Storm were studied in detail as a part of this thesis and are profiled in the following pages. For additional damage statistics as a result of severe weather events, please reference Figure 37.0 in the Appendix. It summarizes all U.S. fatalities and damage costs due to severe weather in the United States from 1940 - 2001.

#### 4.3.1 Hurricane Andrew – 08/16/92 – Southeastern USA, Bahamas, Bermuda

As described at the National Weather Service website (2003), Andrew started on August 14<sup>th</sup> as a tropical wave off the west coast of Africa. By August 16<sup>th</sup>, convection became more focused in a region of cyclonic cloud rotation and the wave transformed to a tropical depression. Between August 17<sup>th</sup> and August 20<sup>th</sup>, the system moved to about 925 km east-southeast of Bermuda. On the morning of August 22<sup>nd</sup>, Andrew reached hurricane. Andrew moved west for the next two days and passed over the Bahamas on August 23<sup>rd</sup> and 24<sup>th</sup>. After leaving the Bahamas, Andrew moved towards southeast Florida and made landfall near Homestead, Florida at 5:30 AM on August 24<sup>th</sup> as a Category 4 hurricane with winds of 232 km/hr (125 knots) and gusts of 278

---

---

km/hr (150 knots). Andrew crossed southern Florida in 4 hours. When it reached the Gulf of Mexico, it turned to the west-northwest crossing south-central Louisiana coast as a Category 2 hurricane. Andrew weakened rapidly shortly after landfall. The remnants of Andrew continued northward merging with another system over the mid-Atlantic U.S. states on August 28<sup>th</sup> (National Weather Service, 2003).

Andrew caused enormous damage in the Bahamas and Florida. Significant storm surge was created in both locations. In Florida, peak storm surge of 17 feet arrived when the tide was high. Andrew also dropped significant amounts of rain on southeast Florida, Louisiana, and Mississippi; Hammond, Louisiana reported 11.92 inches. 26 people died as a direct result of Hurricane Andrew while indirect loss of life raised the death toll to 65. Fortunately, there was ample warning, and good hurricane preparation and evacuation programs helped minimize this number.

Hurricane Andrew destroyed 25,524 homes and damaged 101,241 others. In Homestead, Florida, 99% of all mobile homes were destroyed. Damage in the United States was estimated to be roughly \$25B, making Andrew the most expensive natural disaster in U.S. history.

**Figure 9.0 – Remains of a furniture warehouse west of Whispering Pines, FL**



Source: National Weather Service  
<http://www.photolib.noaa.gov/historic/nws/wea00549.htm>

---

### 4.3.2 Hurricane Mitch – 10/22/98 – South & Central America

According to the National Weather Service (2003), Hurricane Mitch originated from a tropical wave that moved across southern Africa on October 8<sup>th</sup>. The storm became Tropical Storm Mitch on 10/22 while 415 km east-southeast of south of San Andreas Island. Mitch then strengthened and moved north. Mitch reached its peak on October 26<sup>th</sup> with estimated winds of 287 km per hour (155 knots) making it a Category 5 hurricane on the Saffir-Simpson scale. On October 27<sup>th</sup>, Mitch then turned southwestward and passed near the island of Guanaja (Honduras) as a Category 4 hurricane. From October 28<sup>th</sup> to October 30<sup>th</sup>, Mitch stalled over Honduras while gradually weakening. Mitch was a tropical storm by October 30<sup>th</sup> and a tropical depression by October 31<sup>st</sup>. The remnants of Mitch moved toward Merida, Mexico and became a tropical storm again by November 3<sup>rd</sup>. After making landfall over the northwestern Yucatan peninsula, Mitch accelerated northeastward and made landfall near Naples, Florida with winds of 102 km/hr (55 knots). Mitch continued to move northeastward, moved offshore and became extra-tropical. The overall motion of Hurricane Mitch was less than 7.5 km per hour (4 knots). This resulted in very heavy rainfall estimated at up to 890 mms, primarily over Honduras and Nicaragua. To put this into perspective, consider that this 3-4 day rainfall amount is comparable to that for an 8-month period in Halifax, NS (National Weather Service, 2003).

The estimated death toll stands at 9,086. One of the deadliest hurricanes in history, most fatalities occurred as a result of large-scale flooding especially in Honduras and Nicaragua. It was also devastating from an economic perspective. It has been estimated that there was a 50% loss to Honduras' agricultural crops (see Figure 10.0 below); and the UN estimated that 70% of Honduras economic output was lost. At least 70,000 houses were damaged and over 92 bridges were damaged or destroyed. Several communities became isolated as roads were damaged and blocked (see Figure 11.0 on the following page). Total damage from the hurricane is estimated to over \$5B dollars. In Florida alone, the insured damage is estimated to cost \$20M.

---

**Figure 10.0 – Hurricane Mitch Crop Damage, Honduras**



Source: Michael Battistoni, Honduras.com  
<http://snrs.unl.edu/amet351/naiman/honduras.html>

**Figure 11.0 – Mitch Caused Massive Road Damage, Honduras**



Source: Disaster Survey Website  
[http://long.linux-dude.net/~cyrille/disaster/main.php?menu\\_choice=6](http://long.linux-dude.net/~cyrille/disaster/main.php?menu_choice=6)

---

### 4.3.3 Quebec Ice Storm – 01/04/98 – Northern U.S. and Canada

According to CBS Newsworld (1999), scientists called the four consecutive days of freezing rain an “unprecedented phenomenon”. The rains began the night of January 5<sup>th</sup>, 1997, during an unusually mild winter. The abnormal conditions were the result of warm, moist air flowing from the U.S. into Ontario and Quebec. As snow fell into the mass of warm air, it melted and fell as rain only to later meet a mass of cold air at lower altitudes where it was transformed once again to freezing rain. The result was the biggest ice storm to hit central Canada in 40 years. The scope of the disruption, illustrated in Figure 12.0 below, stretched from Kingston in Ontario, to Quebec City (CBS Newsworld, 1999). Over the next four days, three consecutive ice storms raged non-stop and deposited up to 100 mm of ice in some areas, topping the previous record of 40mm. Freezing rain fell for four days without stop.

On Day 1, an initial layer of ice coated everything from trees to cars to power lines. This caused 1000 transmission towers and 30,000 wooden utility poles to be knocked down. By the end of the day, more than 750,000 homes were completely without power. Hardest hit at first was the region in and around Montreal. According to CBS Newsworld, in all, 120,000 km of transmission and distribution lines, which took more than half a century to create, were brought down within a week (CBS Newsworld, 1999). HydroQuebec, the area’s major provider of electricity, deployed crews from across the country to work at rebuilding the network. The task required hundreds of hours of reconstruction at an estimated cost of roughly \$500M. The extent of the damage is described further in Figure 44.0, an appendix item that shows the status of HydroQuebec’s electric grid during peak storm conditions.

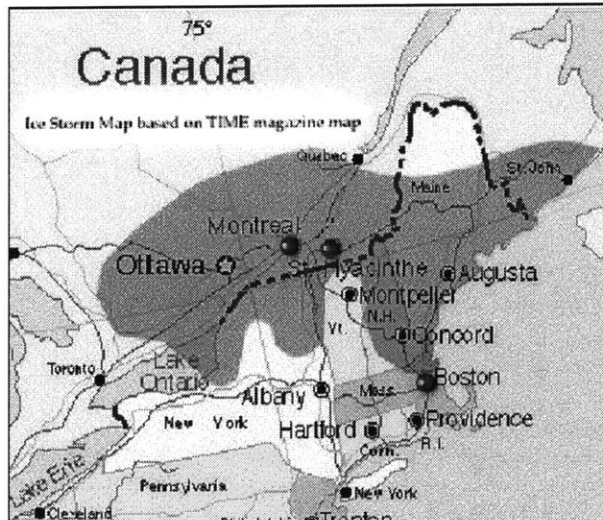
The storm would go on to incapacitate nearly 20% of the Canadian work force and leave approximately 1.5 to 2M people in Canada and the US without electricity. Approximately 100,000 Canadians were forced to seek refuge during the disaster. Even a month after the power loss, 700,000 people were still without electricity. In addition to the obvious effects of a significant power outage, several not-so-obvious effects caused major problems. Without electricity, farming equipment could not be operated and cattle could not be milked. When milking cycles are interrupted for a significant period of time, a condition called *mastitis*, an often-fatal infection of the udder, occurs. According to the Quebec Ice Storm website (2003), this ultimately killed thousands of cows before power could be restored throughout Quebec. Over 45 human fatalities were also directly attributed to the Quebec Ice Storm; from injuries

---

---

ranging from hypothermia to carbon monoxide poisoning to chainsaw accidents. In total, the economic losses of Montreal and Ottawa totaled approximately \$700M, with insurance claims totaling over \$1B (Quebec Ice Storm Website, 2003).

**Figure 12.0 – Area Affected by Quebec Ice Storm**



Source: Disaster Survey Website  
[http://long.linux-dude.net/~cyrille/disaster/main.php?menu\\_choice=13](http://long.linux-dude.net/~cyrille/disaster/main.php?menu_choice=13)

**Figure 13.0 – Tower Damage, Quebec Ice Storm**



Source: Disaster Survey Website  
[http://long.linux-dude.net/~cyrille/disaster/main.php?menu\\_choice=13](http://long.linux-dude.net/~cyrille/disaster/main.php?menu_choice=13)



---

## 4.4 Floods

It is often said that water is the most destructive force on earth. Most flood survivors would probably agree. Major floods, such as the 1993 Mississippi River Flood and the Summer 2002 floods that submerged much of Central Europe, transformed landscapes, destroyed public and private property, brought local commerce to a grinding halt, and claimed countless lives. In each case, the waterways that had formed the basis for much of the regions' economic development and prosperity over the years proved to be a double-edged sword when heavy rains swelled the rivers to overflow conditions. For area residents and businesses, the results were horrific. For area residents and businesses without insurance – 85% of the 2002 Euro flood losses were uninsured – or a resilience strategy, the results were catastrophic. Three cases – the '93 Mississippi River Flood, the 2002 European Floods, and a 2001 building flood – are outlined below to provide accounts of how devastating these events can be.

### 4.4.1 1993 Mississippi River Flood – Summer 1993 – Midwestern U.S.

The Mississippi River begins at Lake Itasca in Minnesota and stretches over 2,000 miles south to the Gulf of Mexico. While the residents along its banks are certainly not strangers to periodic flooding, none of them were ready for what the river had in store during the summer of 1993. From late June to mid-August that year, the most devastating flood in U.S. history washed over the upper and middle Mississippi Valley. At its peak, 17,000 square miles of land were covered by floodwaters in an area that included all or part of nine states (see Fig. 14.0 below). Minnesota, Iowa, Illinois, and Missouri were the hardest hit. At St. Louis, for example, the river crested at 49.6 ft. – more than 19 ft. above flood stage and more than 6 ft. above the previous record set in 1973 – and remained over flood stage for two months. Homes were destroyed, farmland was ruined, and businesses were disrupted if not completely wiped out.

The chain of events that caused the deadly flooding that summer was set in motion as early as the Fall of 1992. That year, cooler than normal conditions prevailed, and resulted in lower than normal evaporation activity after fall and winter storms. Eventually, the soil became saturated, so spring precipitation and snowmelt, normally able to soak into the ground, could only run off into nearby streams and rivers. As individual storms continued to dump large volumes of precipitation on the area that Spring, local streams quickly reached capacity. By June 1<sup>st</sup> of 1993, the Mississippi and its tributaries were already running higher than average. At that point, a persistent southward displacement of the jet stream began to develop and the situation began to

---

---

worsen when a series of severe thunderstorms stalled over the Midwest. As the University of Akron's David McConnell (1998) explains, "The abnormal rainfall was attributed to a weather system formed when warm moist air from the Gulf of Mexico collided with cold, dry air from Canada over the Midwest. When the warm Gulf air cooled, it lost the moisture it carried as rain. Normally, this rainfall would have been distributed throughout the northeastern states, but a stalled high-pressure system over the southeast blocked the flow of the jet stream bringing a constant stream of storms over the Midwest" (McConnell, 1998). This stationary system dominated weather patterns in the U.S. for much of June and July, bringing wave after wave of drenching thunderstorms to the already saturated Mississippi River basin. According to Weather.com Storm Encyclopedia (2003), by the end of the summer, many locations had received over 30 inches of rain which was nearly 200% over normal (Weather.com, 2003).

The persistent flood conditions that summer brought widespread destruction and misery to the Mississippi Valley. The greatest economic losses occurred in cities on the floodplain. To illustrate the extent of the flooding, Figures 15.0 and 16.0 below show satellite images of St. Louis, Missouri, under both pre and post-flood conditions. According to Weather.com (2003), the 250,000 residents of Des Moines, Iowa, located in the center of the flood region, were without drinking water for nineteen days when the city's waster treatment plant flooded. Before the municipal water supply could be restored, the water pipes, contaminated by floodwaters carrying sewage and agricultural chemicals, had to be thoroughly flushed out. Economic losses in Des Moines alone totaled over \$716M (McConnell, 1998). In all, over 70,000 people were displaced by the floods. Roughly 50,000 homes were damaged or destroyed and 52 people lost their lives (Weather.com, 2003).

The flooding also wreaked havoc on the local economies. According to McConnell (1998), over eight million acres of farmland was submerged rendered useless. As a result, production of corn and soybeans were down 5-9% and corn prices rose by \$0.15 per bushel. The river's role as a major transportation lane was also severely compromised. Barge traffic, which normally moves through a system of 29 locks between Minneapolis and St. Louis, transports 20% of the nation's coal, 33% of its petroleum, and half of its exported grain. Barges were halted for two months during the flooding, costing carriers an estimated \$1M per day. Some power plants along the river saw their coal stocks shrink from a two-month supply to just 20 days worth. Land transportation was also affected. Hundreds of miles of roadways that ran through the floodplains

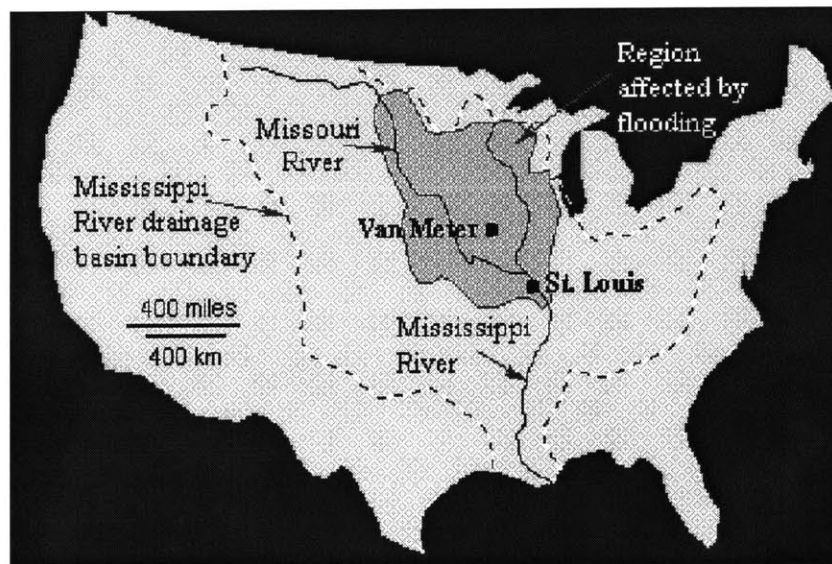
---

---

were damaged with repair costs were estimated to have reached \$500M (McConnell, 1998).

Before the waters began to recede that August, the floods had covered an area covering 500 miles long and 200 miles wide. 534 counties in nine states were declared federal disaster sites. According to Ramsey (2002), total economic losses reached \$10-15B, although indirect losses in the form of lost wages and production are difficult to accurately calculate and would likely raise loss estimates significantly (Ramsey, 2002). By all measures, the 1993 Mississippi River Flood was the most destructive in recorded U.S. history.

**Figure 14.0 – 1993 Mississippi River Flood Region**



Source: McConnell, 1998

**Figure 15.0 – Pre-Flood St. Louis, MO**



Source: NASA (<http://svs.gsfc.nasa.gov>)

**Figure 16.0 – Post-Flood St. Louis, MO**



Source: NASA (<http://svs.gsfc.nasa.gov>)

---

#### **4.4.2 Central European Floods – Summer 2002 – Germany, Czech Republic, Austria**

The flood conditions that affected that washed over large portions of Central Europe over the Summer of 2002 were triggered by unusual, but not extraordinary, meteorological conditions. As an EQE Technical Report (2003) explains, two rain-bearing depressions crossed Europe in close succession during the first half of August. The first high-altitude, low-pressure system formed in the Atlantic and crossed Northern England and Scotland on July 31<sup>st</sup>, causing minor flooding in northern England. By the 6<sup>th</sup> and 8<sup>th</sup> of August, the system had reached southern Germany and Austria, where torrential rainfall resulted. The system then moved eastwards along the southern side of the Alps, resulting in further heavy rainfall in Romania, The Czech Republic, and the eastern coast of the Black Sea. This first depression was quickly followed by “Ilse”, a second rain-bearing storm, which moved southeast from England, causing heavy rain in northern Italy, before shifting direction northeast and causing further rains in Austria, The Czech Republic, and southern Germany (EQE, 2003). The heaviest precipitation centered over Austria and The Czech Republic, and produced cumulative rainfall in excess of three times the seasonal average, triggering sequential flood waves along the region’s two major river systems. The flood waves moved down the Danube through Austria and down the Vltava, Labe, and Elbe rivers into The Czech Republic and Germany. The geographic reach of the flood is illustrated in Figure 17.0 below.

The first flood wave hit the area over the weekend of August 10<sup>th</sup>, triggering flash floods and landslides across northern Italy, southern Germany, Austria, Romania, and the Baltic Sea coast of Russia. By the following Monday, August 12<sup>th</sup>, the river Danube in Austria overflowed its banks at several points, damaging or destroying an estimated 10,000 houses. Across the border in The Czech Republic, the intense rainfall entered the headwaters of the river Vltava, causing similar overflow. As the flood waters approached the capital city of Prague, roughly 50,000 residents were evacuated, all bridges over the Vltava were closed to traffic, and 9ft.-high flood barriers were erected along the banks to protect the city center (RMS, 2003). As the flood wave continued downstream towards Germany, many small town and villages in its path were severely damaged. Across The Czech Republic, seventeen people were killed and an estimated 220,000 evacuated. In Dresden, about 200 km (124 mi.) from Prague, flooding submerged the main railway station and numerous parts of the historic city center. Fortunately, early warnings allowed many paintings and other priceless works of art to be removed from the lower levels of the damaged buildings. More catastrophic flooding occurred further downstream around the

---

---

towns of Dessau and Bitterfeld. Across the effected regions of Germany, 180 bridges were damaged along with 740 km (460 mi.) of roadways and 538 km (334 mi.) of railway track (RMS, 2003).

Besides the human toll, the floods also did something almost unheard of according to Green & Pohl (2002) in a 2002 New York Times article – they stopped production of The Czech Republic’s two most famous beers, Pilsner and the original Budweiser. Production at both breweries was halted for over a week because of the flooding (Green & Pohl, 2002). The Prague Stock Exchange was also closed for two days while rising water levels threatened the trading floor and prevented access to the building. The Prague subway was especially hard-hit. According to The Guardian (2002), damage was estimated at two billions crowns (\$64M) with seventeen stations closed due to the flooding. The Unipetrol plant in Spolana, Czech Republic, 20 km from the capital city of Prague, issued a third degree chemical alert (just one level short of evacuation) when a leak of toxic chlorine gas was caused by the rushing waters (The Guardian, 2002). Fortunately, the leak proved to have negligible environmental effect and no direct impact on the region’s citizens. And perhaps the most unexpected fatality occurred when, as reported by CNN.com (2002), a civilian was killed by shrapnel when Czech forces blew up runaway barges that threatened to slam into bridges (Hanna, 2002).

Throughout Central Europe, unprecedented flood heights were reached along the major river systems and over 110 people lost their lives before the waters receded. By December 2002, total economic damage estimates exceeded €15B, of which only about 15% was insured according to RMS (2003). Germany was the hardest hit, with over two thirds of the total losses. After Germany, The Czech Republic suffered the next largest loss at €3B, of which over one third was attributed to Prague alone.

**Figure 17.0 – Major Rivers and Cities Affected by 2002 Central European Floods**



Source: RMS, 2003

**Figure 18.0 – Flood Damage in Prague, 2002**



Source: RMS, 2003

---

#### 4.4.3 *Seven Building Flood.* – 01/06/02 – London, England

*Seven Worldwide*, one of Europe's largest digital asset management companies, experienced a significant business disruption that stemmed from a very unlikely source. As Bernard (2003) describes in a 2003 case study, the company's headquarters, a 5-floor 45,000 sq. ft. building in the City of London, leased its top floor to a leading international disaster recovery supplier, which used the space to house a hot back-up site. To protect its expensive, mission-critical information technology (IT) hardware assets from fire, the firm had installed a powerful sprinkler system. Ironically, the system would prove to have just the opposite effect (Bernard, 2003).

In the early morning hours of Sunday, January 6<sup>th</sup>, 2002, a 5<sup>th</sup>-floor water supply pipe failed which activated a water pump that ran uninterrupted for several hours, effectively flooding the building by 4 a.m. Before the problem was discovered, water had cascaded through all five of the building's floors, including computer server rooms, reprographics and artwork suites, proofing and printing equipment, and several general computing suites. Sub-floor IT and electrical systems flooded and elevator shafts became partially submerged. Because the failure occurred after-hours and on the weekend, there was nobody on-site to detect and resolve it.

*Seven* staff discovered became aware of the problem on Sunday afternoon and immediately initiated the disaster recovery plan that the firm had designed with the help of a 3<sup>rd</sup>-party business continuity firm, London-based *Restorex*. Despite a total loss of power and services, and with the help of *Restorex*, the company was able to service its clients without interruption and resumed most production services within 24 hours of the flood. And because they responded quickly and prudently, almost all of their £2.5M in state of the art data management equipment was salvaged. *Seven's* investment in a sound disaster recovery plan with a reliable partner prepared them to fail smartly, thus minimizing the impact of the disruption. This example shows that potential supply chain disasters are lurking everywhere. Sharing your headquarters with a disaster recovery service provider does not necessarily mean your operations are any less vulnerable. A sound business continuity or disaster recovery plan can however, do much to mitigate the risks regardless of the root cause of the disruption.

---

## 4.5 Fires

While not often as destructive, in terms duration and magnitude, as natural disasters like floods or earthquakes, fires can be just as devastating for the residents or businesses that are directly affected. An unexpected blaze can quickly devour a manufacturing plant, a warehouse, or even a truckload of in-transit inventory. And for many high-technology industries the employ sensitive, calibrated manufacturing equipment, even the smoke from a fire can cause significant damage and bring down a production line for days, if not weeks. Three cases – a 2000 Philips Plant fire, a 1999 blaze at a plastics manufacturer, and a 1997 fire at a key Toyota supplier – are outlined below to provide accounts of how devastating these events can be, especially for the unprepared and overexposed.

### 4.5.1 Philips Plant Fire – 03/17/00 – Albuquerque, NM

At approximately 8 p.m. on March 17, 2000, a bolt of lightning struck an electric power line in New Mexico, setting off a chain reaction that would eventually pit two of the world's largest mobile communications companies against each other in a test of supply chain resiliency. The strike caused major fluctuations across the state's grid power grid, which led to a fire in Fabricator No. 22 at an Albuquerque semiconductor plant owned and operated by Philips Electronics NV. The blaze lasted only ten minutes before workers smothered the flames, but that was enough time to ruin eight trays of silicon wafers – enough to produce chips for thousands of mobile telephone handsets – and cause significant damage to the plants high-precision fabrication equipment. Between the smoke from the fire and the activation of the sprinkler system, the ten minute blaze rendered the plant completely unable to produce the computer chips that companies like Nokia and Ericsson depended upon for the production of mobile telephone handsets. It would take Philips weeks to bring the Albuquerque plant back online, time that neither Nokia nor Ericsson could afford to wait given the recent boom in global mobile-phone sales. While both companies were affected in very much the same way, they could not have reacted more differently to the sudden disruption in the flow of these most critical components.

Nokia managers outside of Helsinki detected a problem in the flow of chips even before Philips contacted them with the news of the fire in Albuquerque. When order numbers began failing to add up, the company's chief component purchasing manager immediately contacted their Philips account representative to investigate. After discovering the nature of the disruption, the

---



---

purchasing manager quickly sent word of the situation through the chain of command to the highest levels of management. As reported by the Wall Street Journal (2001), according to Pertti Korhonen, Nokia's chief supply troubleshooter, they "encourage bad news to travel fast. [They] don't want to hide problems" (Latour, 2001). Within days, a crisis management team was assembled and deployed across Europe, Asia, and the U.S. to develop a solution to the supply problem. The team "redesigned chips on the fly, sped up a project to boost production, and flexed the company's muscle to squeeze more out of other suppliers in a hurry" (Latour, 2001). They were determined to secure enough alternate sources of radio frequency chips to prevent any impact to overall production. In the meantime, Nokia checked in with Philips daily to check the status of recovery process and applied constant pressure, up to the CEO level, to ensure that they were allocated any capacity that Philips could provide from their other fabrication plants. Because of Nokia's size, tenacity, and almost immediate response to the situation, they were quite successful in pushing Philips to reroute capacity. More than ten million chips were replaced by a Philips plant in Eindhoven, the Netherlands, and another plant in Shanghai was freed up for Nokia as well.

Ericsson, on the other hand, did not fare quite so well. First of all, they were not as prepared for the problem as Nokia was. Philips was their sole supplier for radio frequency chips (RFCs). There were no other alternate suppliers to turn to for failover capacity. Ericsson was also much slower to detect the problem than their Finnish competitors. News of the fire was first communicated by an informal conversation between two technicians. When official word finally came from Philips as to how serious the problem really was, still more time passed before middle managers notified their bosses. In fact, the head of the mobile phone division did not find out about the fire until several weeks after it occurred. Without alternate suppliers to turn to, Ericsson was left with only one option – try to pressure Philips to reroute capacity from other plants until the Albuquerque plant was back online. As they soon found out, Nokia has beaten them to the punch and had claimed all of the capacity that Philips had to give. Ericsson was left with severe component shortages, the wrong product mix, and myriad marketing problems – all at a time when reported demand was at record levels.

When the smoke finally cleared and the full impact of the Albuquerque fire was known for both companies, the results clearly reflected the companies' contrasting approaches. Nokia was able to meet its production targets despite the fire and maintained aggressive growth projections for

---

---

handset sales the following year. Ericsson, however, reported that the fire contributed to a 2000 loss of \$1.68B, sending shares down 14% over a period of just a few hours. While the experience drove them to overhaul procurement practices, ensuring that key components come from more than one source, the lesson came too late to save their mobile handset business. After losing significant market share, mostly to Nokia, in the weeks following the fire, Ericsson eventually chose to leave the market altogether and now outsources all handset manufacturing to Flextronics International Ltd. Commenting on the procurement changes that Ericsson introduced soon after the fire, Jan Wareby, the head of the mobile-phone division, stated that “[they] will never be exposed like this again” (Latour, 2001). Unfortunately for Ericsson, there wouldn’t be an “again”, at least not for the mobile handset division.

#### **4.5.2 Avon Injected Rubber & Plastics Plant Fire – 04/02/99 – Albion, NY**

Avon Rubber and Injected Plastics (Avon) is the automotive division of Avon Rubber, a manufacturer of diversified rubber products founded in Wiltshire, England in 1885. The division occupies a single 200,000 ft<sup>2</sup> production facility located in Albion, NY and supplies rubber gaskets, door seals, and other rubber products to most leading automotive OEMs including General Motors, Ford, and Daimler-Chrysler. Over the past several years, Avon had come to enjoy the position of sole supplier of various types of rubber gaskets to several of these leading OEMs. As in many industries, it was thought that consolidating the supply base would provide cost savings through economies of scale and lower procurement overhead. It is also likely that rubber gaskets were not considered a key component and therefore presented little risk of disrupting operations should a supply problem develop. On a Friday afternoon in April, 1999, the OEMs would learn otherwise.

The fire was reported shortly after 2pm on Friday, April 2, 1999. Ten fire departments responded to fight the 3-alarm blaze, but could not prevent the complete destruction of Avon’s 40,000 ft<sup>2</sup> production floor, rendering the Albion plant completely unable to produce. According to Dean Depew, the Albion plant manager, “several automotive plants were dependent on Avon’s products in order to continue their own production and a shutdown of those plants would result in at least \$10,000,000 a day in losses” (MJ Mechanical, 2001). At the time of the fire, Avon had ten days worth of product in stock before the losses would begin piling up. Once notified, many of Avon’s customers turned to alternate suppliers to protect against a likely shortage of rubber gaskets. At least one of the OEMs that sole-sourced from Avon was not so fortunate.

---

---

When they turned to other suppliers, they found that none could form gaskets with exactly the same properties. It turned out that Avon used unique steam-driven production equipment, which could not be found anywhere other than the Albion plant. After quickly running out of options, the auto maker was forced to partially subsidize the complete restoration of Avon's manufacturing capabilities if they hoped to restore supply before Avon's ten days of finished goods inventories, in addition to whatever inventory the auto maker may have been holding on-site, was consumed. Fortunately for all, the Albion plant was brought back online without the OEM having to completely halt production, although not without incurring significant cost at the expense of both Avon and one of its largest customers.

Important lessons can be taken from the Avon case; from both the supplier and the OEM perspective. Avon learned that complete centralization of manufacturing resources can be disastrous, regardless of the operating efficiencies that it may provide. The large auto maker that had to finance part of its supplier's recovery learned that sole sourcing can be dangerous, regardless of how important, or not, that component may seem to the finished product. In this case, a rubber gasket came very close to halting production. In addition to arranging for multiple suppliers in different locations, it is also important to understand the capabilities and vulnerabilities of those suppliers to determine what their exposure to supply risk. The OEM could have transitioned to an alternate supplier had it not found that their gaskets, as specified, demonstrated characteristics that limited production only to Avon's unique steam-driven machinery...which existed only in the Albion plant. This fact dramatically increased their exposure to risk and taught them a painful lesson in effective sourcing strategy.

#### **4.5.3 Toyota P-Valve Supplier Plant Fire – 02/01/97 – Kariya, Japan**

Just after 4 a.m. on Saturday February 1, 1997, sparks from a broken drill ignited several wooden platforms at the Aisin Seiki Co. Factory No. 1 in Kariya, Japan. The fire spread quickly, was swept through an air duct, and ignited the roof. The building was soon completely engulfed in flames. And to compound the tragedy, Aisin's Kariya factory was the sole-source of brake fluid proportioning valves – or “P-valves”, which pressure on rear brakes and help prevent skidding – for Toyota's 20 automobile plants in Japan. At the time, Toyota's Japanese plants were producing roughly 14,000 cars per day and were operating under a Just-In-Time operating strategy that permitted only about four hours worth of inventory to be held at any given time.

---

When the blaze was finally extinguished, virtually all of the plant's 506 highly specialized machines, which made other brake parts in addition to P-valves, were rendered charred and useless. As noted above, under Toyota's JIT inventory strategy, most plants kept only a four-hour supply of the \$5 valve on-hand. Without the part, Toyota had no choice but to shut down all 20 of its auto plants in Japan. It was estimated that more than two weeks would be needed just to restore a few milling machines to partial production and six months to order new machines. In a period of strong domestic demand and an increasingly brisk-selling U.S. market, this was not acceptable. Outside of the significant financial loss for Toyota, the effects would be disastrous for the local and national economies as well. As quoted in a 1997 Wall Street Journal article by Philip Reitman, one state agency estimated that each day Toyota is shut down cuts Japan's annual industrial output by 0.1 percentage points (Reitman, 1997).

For most parts, Toyota had at least two suppliers. But over the years, it had turned to Aisin to produce all but 1% of its P-valves because of their high quality and low cost. Aisin shipped parts to Toyota plants several times a day, replenishing just enough valves for a few hours of production. Toyota managers conceded that depending on a single source and holding essentially zero inventory was risky however, it is also what kept Toyota's production costs low. Aisin achieved significant economies of scale that it passed on to Toyota in the form of lower prices, while JIT effectively minimized inventory carrying costs. Toyota also acknowledged that it didn't figure in the risk of fire. Regardless, the situation was what it was and the focus of Toyota and its supply base was now directed solely on recovering production capability as soon as humanly possible.

Even as the fire burned, Aisin officials organized a committee to assess the situation, notify customers and labor unions and, following Japanese custom, visit neighbors to apologize. A sub-committee ordered 320 cell phones, 230 extra phone lines, and several dozen sleeping bags for executives who were expected to live at headquarters in the days following the fire. At 8 a.m., Aisin asked Toyota for help. A senior Toyota managing director was tracked down at a golf-course clubhouse, where he left his wife and rushed to Toyota headquarters to help establish a war room to direct the damage-control operations. They immediately sent 400 engineers to Aisin. Later that afternoon, a second war room was set up at Aisin headquarters where Toyota summoned officials from several of its other major parts suppliers to discuss plans to resume the flow of the valves. With over 200 P-valve variations required for the range of Toyota models

---

---

that Aisin supplied, the task was daunting. And chances that anyone else would quickly take up production were slim to nil. The valves have many complex tapered orifices that require highly customized jigs and drills. Everyone involved quickly realized that the best chance for a timely recovery lied in allocating production across the supply base. After receiving their respective valve-making assignments from Toyota executives, each supplier quickly set off to mobilize their respective teams in pursuit of a solution. For example, Somic Ishikawa Inc., a supplier of brake parts and suspension ball joints, called an emergency planning meeting with its top production engineers on Sunday night to map out a strategy. At 6 a.m. Monday, the company began an around-the-clock effort to make the jigs that it would need. On Wednesday, February 6<sup>th</sup>, they delivered their first P-valves to Toyota, as promised. Similar work efforts were also exerted by the other suppliers, each wanting to be the first to deliver its allocation of valves to Toyota. In fact, so many suppliers were rushing to please Toyota that an unofficial race ensued.

Toyota received trucks bearing the first 1,000 usable P-valves by late Wednesday. The following day brought 3,000 units with 5,000 arriving Friday. Slowly, Toyota's assembly lines began to spark back to life. When all was said and done, Toyota lost production of 72,000 vehicles however, with overtime and extra shifts, it claimed to have almost completely recouped the lost output over the months following the shutdown. The Aisin fire prompted Toyota to make several changes, however, allocating the supply of P-valves across more than one source was not one of them. Management remained convinced that they had the right balance of efficiency and risk. After tempering the benefits of multiple supply sources with the costs of setting up expensive milling machines at each site, they stayed true to their pre-fire operating strategy. The experience did drive Toyota to begin reducing the number of its parts variations, a problem that had made the P-valve recovery all the more challenging. It also motivated other sole-suppliers to invest in fail-safe mechanisms. For example, Somic Ishikawa revamped its system to allow them to quickly shift production to a secondary site if it had to.

Most experts predicted that the recovery would take many weeks. Toyota was back up after only 5 days. The secret of Toyota's miraculous recovery lay primarily in its close-knit family, or "keiretsu", of parts suppliers. Within hours of the disaster, they had begun taking blueprints for the valve, improvising tool systems, and setting up makeshift production lines. By the following Thursday, the 36 suppliers, aided by more than 150 other subcontractors, had nearly 50 separate lines producing small batches of the brake valve. In one case, a sewing-machine maker that had

---

---

never made car parts spend about 500 man-hours refitting a milling machine to make just 40 valves a day. As quoted by Reitman (1997) in the Wall Street Journal, “toyota’s quick recovery”, said Yoshio Yunokawa, general manager of a Toyota–group maker of machine tools and steering systems, “[was] directly attributable to the power of the group, which handled it without thinking about money or business contracts” (Reitman, 1997). Indeed, suppliers never asked Toyota or Aisin how they would be compensated for rushing out the valves. Says Somic’s Mr. Ishikawa, “we trusted them” (Reitman, 1997). That trust was validated when Aisin, as the first valves arrived at Toyota assembly plants, told suppliers that it would reimburse them for all costs incurred; from drills and overtime pay to lost revenue and depreciation. In similar fashion, Toyota promised suppliers bonuses totaling roughly \$100M “as a token of their appreciation.” It is little wonder that Toyota Motor Corp. remains among the world’s most admired and feared manufacturing companies in the history of business.

#### **4.6 Port Explosions/Disruptions**

In a 2002 InformationWeek.com article, Eileen Cuneo estimates that over 90% of world trade travels in containers aboard ocean–going ships. About 20 million containers move through 220 ports around the globe every year. Six million enter U.S. ports each year alone. That works out to 17,000 every day (Cuneo, 2002). Considering those statistics, it is not difficult for one to understand how devastating a major port disruption could be to the flow of global commerce. With these volumes, it is also not difficult to understand just how daunting a task port security can be. It is simply not practical, let alone feasible, to screen every container that enters a U.S. port on any given day. As industry and governments begin moving towards a solution that maximizes security without compromising the flow of goods, several federal and commercial initiatives have been introduced, including Smart and Safe Tradelanes (SST) and the Customs-Trade Partnership Against Terrorism (C-TPAT). At this point, it is too early to tell how successful these initiatives will be, but early both SST and C-TPAT appear to be gaining significant traction among port operators, shipping companies, importer, and exporters. Fortunately, there have been no major port disasters in the last fifty years to learn from, however, two early cases, the 1917 Halifax Port Explosion and the 1947 Texas City Disaster, are outlined below to provide accounts of how devastating a large explosion at a major shipping port can be.

---

#### 4.6.1 Halifax Port Explosion – 12/06/17 – Nova Scotia, Canada

During the First World War, the port of Halifax, Nova Scotia was a strategic supply point used for shipping soldiers and military cargo across the Atlantic. At approximately 7:30 a.m. on December 6, 1917, a French munitions ship, the *Mont Blanc*, was headed north into the Halifax Harbor, where it was to wait for the rest of its convoy before setting off for Europe to supply the French military. The 3,000 ton ship was loaded with 200 tons of TNT, 2,300 tons of picric acid, 61 tons of gun cotton, and 35 tons of highly flammable Benzyl. At the same time, a Belgian ship, the *Imo*, was headed southward through the Harbor's channel headed out to the open sea and bound for New York to pick up relief supplies for Belgium.

The ships were supposed to pass each other in the Narrows (see Figure 19.0 below) “port-to-port”, with each captain staying to his right, as the left sides of the ships went by each other. The *Mont Blanc* observed the much-larger *Imo* bearing down fast and too far east, threatening to force the *Mont Blanc* precariously close to the shore on the right. Because the *Mont Blanc* failed to fly the requisite red flag indicating that it was explosives, the captain of the *Imo* could not have known the potential danger of the situation. The *Mont Blanc* signaled that it was in the correct channel however, the *Imo* signaled back that it intended to bear even farther into the *Mont Blanc*'s path. The captain of the *Mont Blanc* then signaled that it would pass on the starboard side, not “port-to-port” as protocol usually requires. The *Mont Blanc* then expected the *Imo* to turn towards Halifax to let it pass, but the *Imo* failed to change its course. Desperate to avoid a collision, the captain of the *Mont Blanc* decided to swing drastically left toward Halifax. Unfortunately, it was too late. When both ships realized that a collision could not be avoided, they reversed their engines and braced for impact.

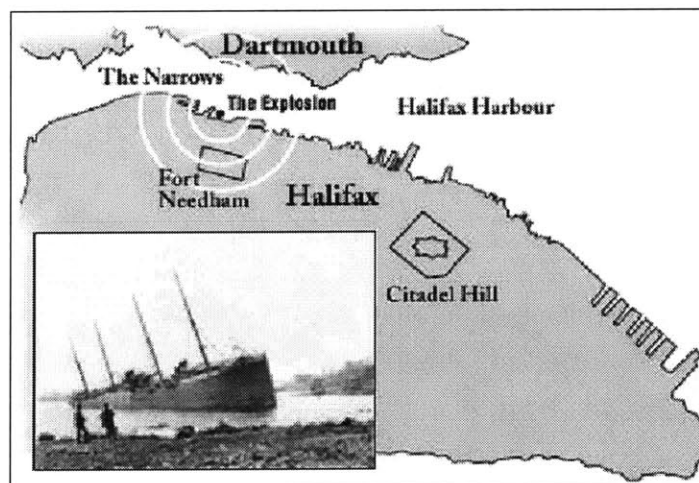
The *Imo* struck the *Mont Blanc*, sending sparks flying from the steel-on-steel impact. Although the impact was not severe, the *Mont Blanc*'s highly flammable cargo immediately erupted in flames. The crew of the *Mont Blanc*, aware of its cargo and realizing the disaster that was unfolding, dove into the frigid waters and swam for their lives. The *Imo* pulled away in an attempt to disentangle itself from the burning ship, but was unaware of the true scope of the situation. The *Mont Blanc* crew that made it to shore tried to warn people of the danger lurking just off shore, but the citizens could not understand the French sailors and instead gathered on at the harbor to watch the fire.

---

The *Mont Blanc* burned for approximately twenty minutes and drifted towards Pier 6 at the North end of the harbor, drawing the growing crowd of curious onlookers even closer. Just before 9:05 a.m., the *Mont Blanc* erupted in what was the largest man-made explosion until the atomic age. In fact, its effects were studied by Oppenheimer during the Manhattan Project to calculate the strength of the bombs destined for Hiroshima. The blast immediately created a colossal tidal wave that hurled itself onto the shores of the harbor destroying everything in its path. For an instant, the bottom of the harbor was visible. The explosion also sent the *Mont Blanc*'s 1,140 lb. anchor shaft over 2 miles and shattered windows 50 miles away. 1,600 people were killed instantly and 9,000 others were wounded. Flying glass claimed the eyesight of 200 people that were watching from windows. The explosion, and the fires that followed it, devastated the entire north end of Halifax (325 acres) and completely destroyed 1,630 homes.

Initially, the captain of the *Mont Blanc* thought to have not obeyed the rules of the harbor, was charged with manslaughter and released on bail. The charges were eventually dropped as gross negligence causing death could not be proved. After a series of court hearings, both ships were found equally at fault and no blame was ever truly laid for the devastating Halifax port explosion.

**Figure 19.0 – Halifax Explosion Blast Radius (S.S. Imo in Inset)**



Source: Maritime Museum of the Atlantic  
<<http://museum.gov.ns.ca/mma/AtoZ/HalExpl.html>>



---

#### 4.6.2 Texas City Disaster – 04/16/47 – Texas City, TX

On the morning of April 16, 1947, the *S.S. Grandcamp*, a French cargo ship, was docked in the Texas City harbor awaiting the remaining pallets of a large consignment of ammonium nitrate fertilizer destined for Europe. Over 2,300 tons of the material was already onboard, 800 tons of which was loaded in the lower part of Hold 4. The ship also held drilling equipment, tobacco, cotton, large balls of sisal twine, and several cases of small arms ammunition.

Just before 8:00am, several longshoremen descended into Hold 4 to begin loading the remaining pallets of 100-lb. fertilizer bags. Before the first pallet could be loaded however, a fire was discovered smoldering deep within the stacks of loaded cargo. Equipped with only a jug of drinking water and two small fire extinguishers, the crew's initial attempts to quell the blaze were futile. While the crewmembers in Hold 4 summoned for a hose, others began hastily unloading the boxes of ammunition stored in Hold 5 to prevent an explosion. The hose soon arrived and was lowered into Hold 4, but before it could be turned on, the Captain of the ship interfered. He was afraid that the water from the hose would ruin the ship's precious cargo and ordered the men to suffocate the flames instead. So they battened the hatches and covered them with wet tarpaulins, closed the ventilators, and activated the ship's steam system. The fire continued however, and soon the entire Texas City Fire Department was dispatched to help contain what had quickly become a raging inferno. Large crowds, drawn by both the bright orange smoke and the spectacle of the firefighting effort, began to gather at the scene. Crowds even took to the skies, as two airplanes loaded with spectators circled the port from above. The crowds did not realize however, that the cargo hold of the burning ship contained over 2,400 tons of highly explosive ammonium nitrate. While most of the crew and perhaps some of the firefighters knew what was on the ship, it seems that nobody at the scene knew how dangerous the cargo really was. Recall that the explosive device used in the 1995 Oklahoma City bombing was fueled by just three tons of ammonium nitrate, 1/800<sup>th</sup> the load of the *Grandcamp*. An executive at Texas City Terminal Railway even telephoned an engineer at a nearby chemical plant to ascertain the danger of burning ammonium nitrate. The engineer advised the executive not to worry as the material would not explode without a detonator.

Just before 9:00am, the ammonium nitrate in Hold 4 of the *Grandcamp* exploded, causing a hellish chain reaction that decimated the port of Texas City and much of the city itself. The blast lifted the 176-ton ship 20 feet in the air and ignited the larger cache of fertilizer in Hold 2,

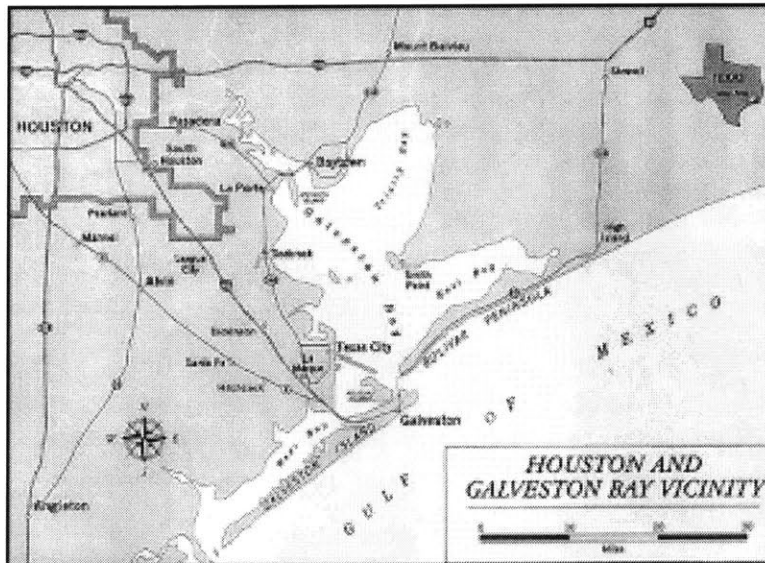
---

---

triggering another violent explosion. Most of those gathered at the scene were killed instantly, even those in the sky. The shockwave from the second blast felled both of the airplanes that were circling above. Flaming debris rained down on Texas City, creating a chain reaction of fires that soon engulfed a nearby industrial park, the Monsanto Chemical Plant, and scores of other residential and commercial structures. The explosion also created a 15-ft tidal wave that wiped out everything in its path as it pushed oil and debris, including a 150-ft barge, over the banks of the harbor. As the town struggled to assess the damage and tend to the injured, yet another disaster was in the making. The SS *High Flyer*, docked in the Texas City harbor for engine repairs, was knocked from its moorings and ignited by the *Grandcamp* explosion. It was also loaded with ammonium nitrate. The fire was discovered in the late afternoon and reported to rescue workers, but several hours passed before the danger of the situation was fully realized and a tugboat team was assembled to remove the smoldering ship from the harbor. Unfortunately, it was too late. After two hours of futile effort, including severing the ship's anchor lines, the team was unable to move the vessel and was forced to retreat as flames began to rise from the cargo hold. Ten minutes later, the *High Flyer* exploded with a force reported to be even greater than that of the *Grandcamp*. This triggered a second chain reaction of fires and explosions that claimed many of the buildings, crude oil tanks, and various other structures that had been somehow spared during the previous day's destruction.

When the smoke cleared, the Texas City Disaster had claimed over 500 lives and caused over \$100 (1947 dollars) million in reported property loss, not including the \$500 million in petroleum products consumed in the blaze. 2,000 Texas City residents were rendered homeless after one third of all residential homes were condemned. The town would take many years to recover. In terms of commercial operations, Stephens (1997), reported that "even though the port's break-bulk cargo-handling operations never resumed, Monsanto was rebuilt in little more than a year, and the petrochemical industry recovered quickly" (Stephens, 1997)

**Figure 20.0 – Map of Galveston Bay and Texas City Harbor**



Source: The Texas City Disaster, 1947  
<http://205.172.60.10/comm/virtual/readingroom/books/blast.htm>

**Figure 21.0 – 150-ft Barge Washed Ashore by Tidal Wave, TX City Disaster**



Source: <<http://www.local1259iaff.org/disaster.html>>

---

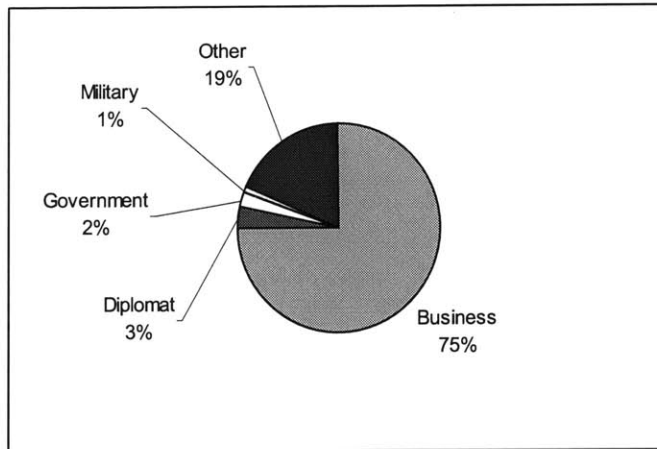
## 4.7 Terrorist Attacks

The world entered a new age of global terror when the twin towers of New York City's World Trade Center were felled in a terrorist attack of unprecedented ferocity and magnitude. While terrorism certainly moved to the forefront of world consciousness that morning, many would argue that the threat has been present for many years. According to a 2001 U.S. Department of State report, from 1996 to 2001, 2,784 individual acts of physical terror were successfully executed around the world - 68% of which were targeted towards business interests (See Figure 23.0 below). As illustrated in Figure 22.0 below, in 2001 alone, 75% of the 531 terrorist acts on record were aimed at commercial targets (U.S. Department of State, 2001). Consistent with the historical data, commercial targets are widely considered to be favored over military, government, or diplomatic alternatives for several reasons:

- “Softer” or lighter security make them much easier to strike against,
- There is often a high probability of inflicting a significant number of casualties, and
- Commerce and trade are symbolic of the capitalist western economic system that groups like al Qaeda are intent upon disrupting.

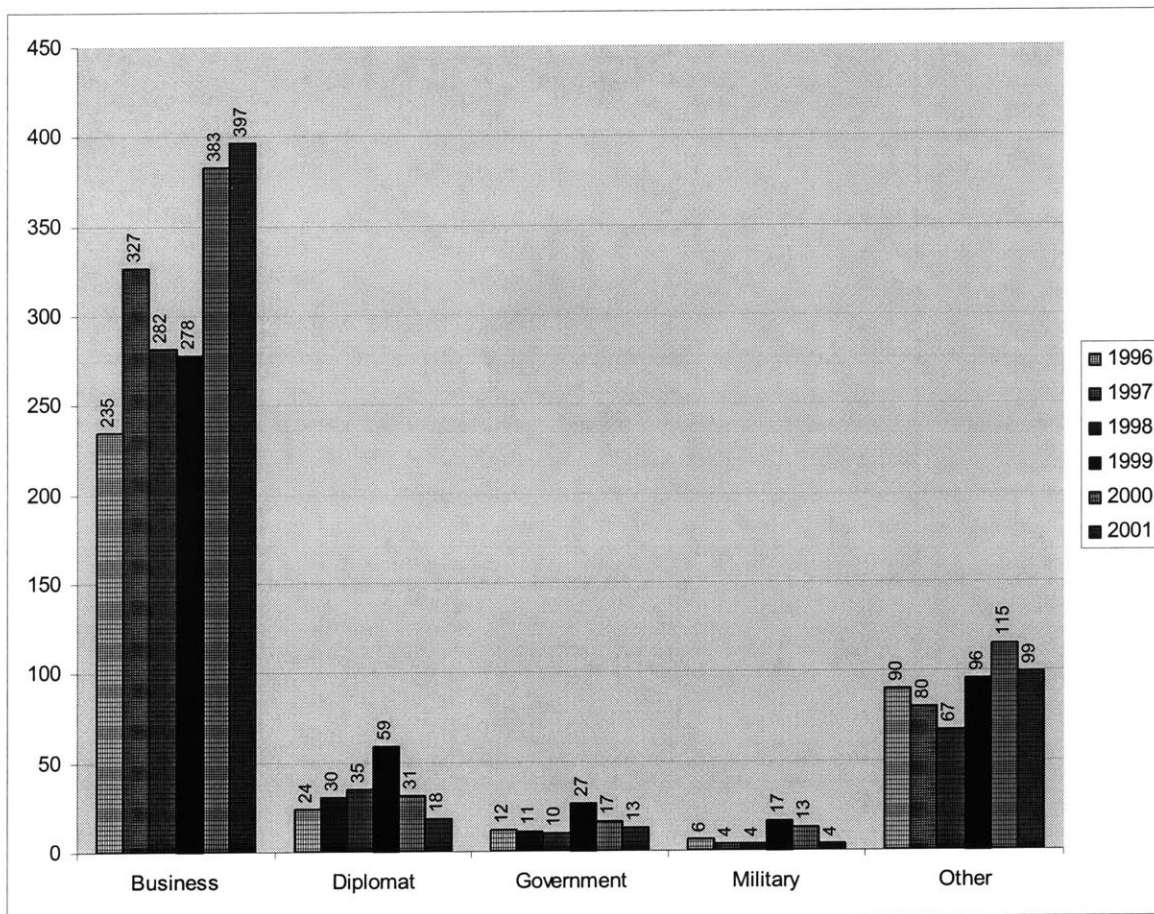
So clearly, terrorism is not just a political or diplomatic problem. Just as an earthquake, a flood, or a fire at a manufacturing plant can render a supply chain inoperable, so too can a car bomb or a hi-jacked Boeing 767. Commercial enterprises must take steps to understand their vulnerabilities and include acts of terrorism in their enterprise resilience strategies. While the probability of any one company becoming the target of a terrorist attack is likely very remote, the proximity of assets to high-profile city centers like New York City, Washington, D.C., or London can certainly increase the chances and is evidenced by the range in terrorism insurance premiums now becoming widely available to firms operating in the U.S. (see Figure 35.0 in Chapter 6). Regardless of the perceived risk however (i.e. the probability it occurring), the impact of a terrorist attack can and should be assessed in the same context as any other potential disruption – by the impact on the functions of the supply chain – not by the event itself. This concept will be discussed further in Chapter 5. Three cases – the 1993 World Trade Center bombing, the 1998 Oklahoma City bombing, and the attacks on September 11<sup>th</sup>, 2001 – are discussed below to provide accounts of just how devastating these events can be.

**Figure 22.0 – Total Facilities Struck by International Attack, 2001**



Source: U.S. Department of State, 2001

**Figure 23.0 – Total Facilities Struck by International Attacks: 1996 - 2001**



Source: U.S. Department of State, "Patterns of Global Terrorism: 2001"  
[www.state.gov/s/ct/r/s/pgtrpt/2001/pdf](http://www.state.gov/s/ct/r/s/pgtrpt/2001/pdf)

---

#### **4.7.1 1993 World Trade Center Bombing – 02/26/93 – New York City, NY**

At approximately 12:17 p.m. EST on Friday, February 26, 1993, an explosion tore through the 110-story twin towers of New York City's World Trade Center. The source of the blast was tracked to a van parked on the B-2 level of an underground garage. The rented van had been packed with nitrates and other explosive materials effectively transforming it into a mobile device capable of producing significant destructive force. The attack killed six people and wounded over 1,000 while causing over \$300M in property damage. An example of the damage is shown in Figure 24.0.

According to Anne McCarthy's 1993 article in the Disaster Recovery Journal, over 900 businesses in the World Trade Center were disrupted as a result of the attack, all exhibiting varying levels of preparedness. "One company, Fiduciary Trust International, was prepared and implemented their business recovery program even before they knew the cause of the disruption. 'The explosion occurred a little bit after 12:00 noon and even before we knew the extent of the damage, we had an instinct that this was more than just turning off the power. We invoked our disaster plan by about 1:00 p.m., long before we had any information about the bomb,' commented Lawrence Huntington, Chairman of Fiduciary Trust International" (McCarthy, 1993). And for those firms that were not prepared, the 1993 bombing served as a much-needed wake-up call. Many companies began formal business continuity and disaster recovery programs that would pay dividends when terrorists targeted the World Trade Center yet again in 2001, that time toppling the twin towers using commercial airplanes as guided missiles. One such program was initiated by the city government. In 1999, Mayor Rudolph Giuliani opened a \$13 million emergency crisis center located on the 23rd floor of 7 World Trade center; a building near the twin towers. Giuliani intended the center to serve as a command center during city emergencies, including blackouts, storms and terrorist attacks. Unfortunately, the crisis center would be destroyed with the twin towers during the September 11<sup>th</sup>, 2001, attack which made the coordination of initial response and recovery efforts all the more difficult.

---

**Figure 24.0 – Bomb Squad Investigators Look for Evidence after 1993 WTC Bombing**



Source: Dan Sheehan, NY News Day

#### **4.7.2 Oklahoma City Bombing – 04/19/95 – Oklahoma City, OK**

At 9:03 a.m., Wednesday April 19, 1995, the day seemed just like any other day for the residents of Oklahoma City. One minute later, all of that changed. At 9:04 a.m. CST, a bomb was detonated in front of the nine-story Alfred P. Murrah Federal Building in downtown Oklahoma City. The sound from the blast, the worst act of terrorism ever attempted on U.S. soil to that point, was heard up to 15 miles away. 169 people were killed and several hundred were injured in the explosion and partial collapse of the building.

The bomb that ripped through the Murrah building that day was composed of two to three tons of ammonium nitrate fertilizer mixed with combustible fuel oil. It was placed inside of a rented Ryder truck, which was then parked in front of the north side of the building. The blast effectively destroyed one-third of the building from roof to ground, leaving a crater eight feet deep and 30 feet wide (see Figure 25.0 on following page). As described in a 1999 article by Richard Arnold in the *Disaster Recovery Journal*, the design of the Alfred P. Murrah building was fairly simple and plain; a basic cast-poured concrete and glass structure not unlike many large office structures seen in city centers across the United States. However, to create an aesthetic entrance, four main support columns were exposed at the front entrance and ran the full height of the first and second floors. This design effect created an atrium at the street level (Arnold, 1999). Unfortunately, it also left the structure vulnerable to a well-placed ammonium

---

nitrate bomb. When the blast hit, it knocked out three of the four support columns. So when the second and third floors failed, the higher floors tore away from the compromised structure and collapsed one on top of another, thus creating somewhat of a tragic domino effect.

The building housed several federal offices including the Drug Enforcement Agency, the Bureau of Alcohol Tobacco and Firearms, U.S. Customs Service, U.S. Department of Housing and Urban Development, Veterans Administration, and the Social Security Administration. It also held a day-care center and a variety of civilian businesses, including a day-care center and the Oklahoma Federal Credit Union, a case that is discussed in detail in Chapter 5. The destruction was not limited to the Murrah building however. Several buildings in the surrounding area also sustained damage also. Located directly across the street, both the *Oklahoma Water Resources* and the *Journal Records* buildings suffered extensive damage to windows and exterior walls. And as one indicator of the bomb's destructive force, parts of the federal building were actually blown into the facades of these nearby office buildings. For seven days immediately following the blast, all property within an entire eight-block radius of ground zero was closed to the general public. As it was considered a crime scene, security was very tight, making it difficult for corporate recovery teams to assess the damage to their respective office locations. This only exasperated the situation for those businesses located within the blast radius.

**Figure 25.0 – Bomb Damage to Murrah Federal Building**



Source: The Associated Press  
[http://www.azstarnet.com/public/packages/okc\\_verdict/](http://www.azstarnet.com/public/packages/okc_verdict/)



---

### 4.7.3 9/11 Terrorist Attacks – 09/11/01 – NYC, DC, PA

On the morning hours of September 11, 2001, the worst international terrorist attack in modern history occurred in the United States. A well-planned and highly organized strike – involving the simultaneous hijacking of four U.S. commercial airliners – was directed at multiple targets in New York City and Washington D.C. As outlined in a 2002 U.S. Department of State report, five terrorists hijacked American Airlines flight 11, which departed Boston for Los Angeles at 7:45 a.m. At approximately 8:45 a.m., the plane was deliberately flown into the North Tower of the World Trade Center in New York City, NY. Five terrorists commandeered American Airlines flight 175, which departed Boston for Los Angeles at 7:58 a.m. At 9:05 a.m., the plane was piloted into the South Tower of the World Trade Center. Shortly thereafter, both towers collapsed, killing approximately 3000 people, including hundreds of firefighters and rescue personnel who had arrived on the scene to treat the injured and help to evacuate the buildings.

Four terrorists hijacked United Airlines flight 93, which departed Newark for San Francisco at 8:01 a.m. At 10:10 a.m., the plane crashed in Stony Creek Township, Pennsylvania killing all 45 persons on board. While the intended target of this hijacked plane is unknown, officials speculate that it was headed for Washington D.C. It is also believed that passengers overpowered the terrorists and forced the plane to crash prematurely in a relatively unpopulated area of Pennsylvania (U.S. Department of State, 2002).

Five terrorists hijacked American Airlines flight 77, which departed Washington D.C. for Los Angeles at 8:10 a.m. At 9:39 a.m., the plane was deliberately flown into the Pentagon building in Arlington, VA. A total of 189 people were killed, including the passengers onboard flight 77. It is estimated that 10% of the office space in Manhattan was lost on September 11. It would cost over \$5B to replace the towers today.

The direct impact to businesses located within the blast radius was massive. The financial services industry was particularly hard-hit. As reported in a 2001 Fortune article by Shawn Tully, of the nearly 5,000 initially thought dead or missing, some 2,000 worked for financial firms. This meant that one Wall Street worker in 100 was thought to have been lost. In addition, over 15 million square feet of office space was either completely decimated or badly damaged, an area equivalent to the entire downtowns of Atlanta or Miami (Tully, 2001). Nearly every company on Wall Street suffered losses in one or more of the following key areas: people,

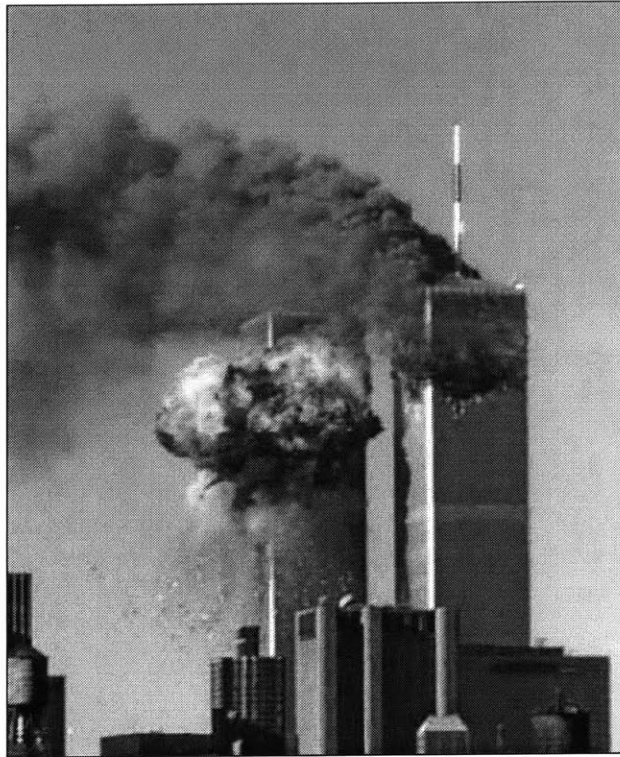
---

equipment, real estate, and trading capacity. Firms like Cantor Fitzgerald, a case detailed in Chapter 6, were suddenly faced with the daunting prospect of replacing highly paid traders and other specialists from a small, exclusive pool of Wall Street elites. And firms like Sidley Austin Brown & Wood LLP and Merrill Lynch – also profiled in Chapter 6 – suffered virtually a complete loss of information technology infrastructure that now needed to be replaced by a plethora of routers, switches, and servers. They weren't alone. Within two days, Dell Computer had been called by all 85 of its New York clients directly affected by the attack. They quickly arranged for the shipment of 5,000 PCs and servers by truck; it promised delivery within 24 hours – another example of Dell's ability to deliver for its customers. Some firms however, took matters into their own hands. According to Tully (2002), "Thacher Proffitt & Wood, a law firm that normally has 300 people on floors 38 to 40 of Tower 2 (no casualties), didn't wait for Dell to deliver; it sent a truck to Austin to collect the 400 computers and printers it had ordered" (Tully, 2002).

For the most part, Wall Street firms were uniquely prepared for such an event and responded well; many were back online with virtually zero downtime. This would never have been the case were it not for the industry-wide investments in contingency planning that began after the 1987 stock market crash and accelerated after the 1993 World Trade Center bombing and the Year 2000 scare. Until the 1993 attack, few companies had implemented robust systems for backing up data or mirroring critical computing power. While the 1993 bombing didn't destroy significant amounts of data, it did persuade many enterprises to focus on contingency planning and rapid recovery capabilities. And while only some firms may have made the initial investments in these areas, the rest of Wall Street quickly followed suit as no single firm could afford to be any more vulnerable than its competitors. Says Wick Simmons, chairman of the Nasdaq at the time: "The scare we had in 1993 put into us the fear we always have in such times: that we'll be down and no one else will" (Tully, 2002).

---

**Figure 26.0 – Terrorists Strike the World Trade Center, 9/11/01**



Source: Disasters of the Last Decade Website

<[http://long.linux-dude.net/~cyrille/disaster/main.php?menu\\_choice=28](http://long.linux-dude.net/~cyrille/disaster/main.php?menu_choice=28)>

**Figure 27.0 – Footprint of WTC Damage, 9/11/01**



Source: Journal of Disaster Recovery Special Report

<<http://www.drj.com/special/wtc/drjwtspecialh.pdf>>

---

## **4.8 Labor Strikes**

Disruptions need not be physical in nature to severely interrupt the flow of goods, information, or funds throughout a supply chain. Any event or scenario that restricts the available capacity of one or more operating partners, or functional nodes of a network, can be crippling to health of the system, regardless of the root cause. For example, work stoppages, or even slow-downs, can be disastrous to the businesses that rely on those services to manufacture and distribute their products. We will discuss three such events that proved to be just that: the 1993 General Motors strike, 1997 UPS strike, and the 2002 West Coast Port Lockout. In each case, the effects were widespread and financially devastating to a great many businesses that were directly or indirectly linked to the striking, or “locked-out”, organizations.

### **4.8.1 1997 UPS Strike – 08/04/97 – Atlanta, GA**

For fifteen days in August, 1997, a company-wide strike at Atlanta, GA-based United Parcel Service (UPS) brought the carrier’s operations to a grinding halt and severely disrupted the flow of goods across the United States and abroad. The major issues in the strike, which began August 4, four days after the old contract expired, revolved around part-time work, pensions and subcontracting. Labor, which was represented by leaders of the Teamsters union, forced UPS through a grueling fifteen day period of negotiations that had garnered much greater public support than anticipated while effectively paralyzing many small businesses across the nation that relied on UPS as their primary, and in some cases only, transportation service provider. Many such businesses worked exclusively with UPS and did not have the relationships in place with other that would have facilitated a relatively painless failover solution. Most concede that they simply did not consider the risk. When these companies tried to shift business to FedEx, or even USPS, they found that delivery times could not be guaranteed due to the sudden strain on capacity. In many cases, carriers like FedEx and Airborne would not take on any new business at all from new customers, citing a commitment to meet expected service levels for their current customers as the reason. The impact was so great that it was estimated that roughly 300 small businesses eventually closed as a result of lost sales, business interruptions, and/or significantly higher shipping costs.

After talks broke down five days into the strike, UPS unsuccessfully sought government intervention to force labor back to work. President Clinton resisted repeated calls to intervene, saying that the strike did not threaten national security or health, and therefore it was

---

---

unnecessary for him to get involved. He believed that the solution to the dispute lied on the bargaining table. His Labor Secretary, Alexis Herman, however was involved in the entire process of the negotiation.

On Monday night of August 18th, 1997 the UPS and the Teamsters' five day marathon negotiation finally ended with a contract agreement. In the new contract, the Teamsters received an increase in pension to \$3000 per month for retired employees after working for 30 years. The pension fund will remain under the control of the union. According to Voorhis (1997), part-time workers' salary would increase from \$11 to \$15 per hour, and UPS agreed to create 10,000 full time jobs over the five year duration of the contract. Although it seemed to be a victory for organized labor, UPS was forced to lay off many employees in the following months due to loss of business during the strike, claiming that the company had already lost \$650M in revenue. While the strike certainly cost UPS dearly in lost revenues and disgruntled customers, the loss in business was a gain competitors like Federal Express, Airborne, RPS, and even the United States Postal Service. Smaller, up-and-coming delivery companies, such as Eastern Connection in Wellesley, MA also made gains. At Eastern, a \$30M overnight delivery company, drivers are delivering 9,000 packages a day, up from 6,000 before the UPS strike, according to company officials (Voorhis, 1997).

#### **4.8.2 1998 General Motors Strike – 06/05/98 – Flint, MI**

On June 5<sup>th</sup> and June 11<sup>th</sup>, 1998, respectively, strikes by members of the United Auto Workers 659 and 651 in Flint, MI resulted in the shutdown of two General Motors (GM) component plants. Those stoppages resulted in parts shortages that eventually led to the shutdown of most of GM's North American assembly plants in late June and early July. The core reason for the conflict between GM and the UAW lied in GM's desire to utilize outsourcing to improve its competitive position. Union work rules had been preventing the company from reaping the benefits of new equipment investments. As Nauss reports in a 1998 article, workers in many sectors worked "under a quota system that allowed them to stop work once their production targets were met. This means workers could put in 4.5 to 6.5 hours but get paid for 8 hours of work. As a result, production lines were running at only slightly more than half of the available capacity" (Nauss, 1998).

On July 28, 1998, the work stoppages at both facilities were finally resolved. From the

---

---

beginning of the third quarter to the point that normal production levels were resumed, the strike resulted in an estimated loss of 318,000 units. The loss of production had an estimated after-tax impact of \$1.2B; \$965M for GM Automotive Operations and \$270M for its Delphi Automotive Systems parts division. The effects of the strike were also felt by the various industries that were either suppliers to or customers of GM. H.B. Fuller, a maker of adhesives, sealants, coatings, and paints experienced significantly lower third quarter earnings as a result of the lost GM business. Dana Corp. (engine components), Excel Industries (doorframes), Gentex (car mirrors), and Westcast Industries (exhaust systems) all reported reduced earnings due to the GM strike. The earnings of several steel companies were also negatively impacted as third quarter demand for steel products plummeted. While virtually all of GM's suppliers suffered, the effects of the work stoppage rippled forward as well. The Washington Post's earnings were slowed due to a decline in advertising revenue on its television stations and in its Newsweek Magazine (The Washington Post, 1998).

#### **4.8.3 West Coast Port Lockout – 09/29/02 – Western U.S.**

On Friday September 27, 2002, at 6:00p.m, the Pacific Maritime Association (PMA) locked their doors on 10,500 International Longshore and Warehouse Union (ILWU) dockworkers. The PMA locked their doors as a result of a collaborative "work slowdown" by the union employees, who cut their productivity by at least 50%. ILWU spokespersons insist that they did not slowdown their work capacity, if fact they were instructed by their employer (PMA) to follow safety procedures more closely, since in the past seven months. Five union dockworkers had died while on the job.

The PMA planned to unlock their doors on Sunday September 29, at 8:00a.m, but shortly after they opened, they shut down and locked the doors again, insisting that the union employees were continuing their collaborative slowdown. Slowdowns can be more detrimental to company than a full-scale strike, because slowdowns throw off the scheduling patterns for the ships coming in, and the trucks going out to deliver the cargo to the factories that use just-in-time inventories. This was the first west coast port stoppage since a 134-day strike back in 1971.

---

Both the domestic and global economies were seriously affected by the lockout. The U.S economy alone is \$10.4 trillion per year, or \$28.4B per day. This means that the west coast's import/export ports provide 7% of the daily total. The west coast ports, from San Diego to Portland Oregon, bring in \$300B dollars of cargo each year, or \$1 to \$2B per day. The west coast handles 54% of the nation's imports and exports. Hawaii was particularly vulnerable as it imports 90% of its goods and significant percentage of that 90% comes from the west coast. Additionally, the Port of Oakland is the number one route used to ship technologies coming out of the Silicon Valley.

The manufacturing, retailing and agriculture industries were most vulnerable. An auto manufacturing plant in Fremont, Calif. was forced to shut down production, idling 5,000 workers. The NUMMI plant, a joint venture of General Motors and Toyota that is discussed in detail in Chapter 5, makes the Chevrolet Prizm, Toyota Corolla and Toyota Tacoma pickup trucks. MSNBC's Martin Wolk reported that "although businesses had at least three months to prepare for the shutdown, the fragile economic environment may have made some retailers unable or unwilling to accumulate heavy inventories. In addition, much of the affected cargo was seasonal, and much was perishable" (Wolk, 2002).

#### **4.9 Financial Distress**

It was Andrew Carnegie, the famed steel magnate and one-time richest man in the world, who suggested that one should "put all your eggs into one basket – and watch the basket." Many companies that have turned to sole-sourcing procurement strategies as a way to reduce production costs have learned the hard way what can happen if you take your eyes off of the basket. The global slump that followed the bull market years of the 1990s made for extremely challenging economic conditions for business operating in virtually every industry. As a result, many companies failed to remain solvent and bankruptcies became commonplace. While this was certainly a negative turn of events for the insolvent firms, it also proved troublesome for the customers that relied upon them, particularly in a sole-source supply relationship. Using a single supplier for one or more critical components effectively binds a manufacturer's fiscal health to that of its supplier. If a supplier suddenly becomes unable to supply parts, it is only a matter of time before its sole-source customer(s) is unable to produce its respective products. And with the rapid adoption of lean manufacturing and just-in-time inventory systems, the

---

“matter of time” has been slashed to just days, or even hours in some cases. There is increasingly little margin for error.

For this reason, it is imperative for any manufacturer that chooses to enter a sole-source supply relationship maintain an intimate operating relationship with its supplier. In theory, a company and its sole supplier are in a partnership where both gain from cooperation in design, engineering, logistics, and costs. At the very least, it is in the company’s best interest to ensure that their sole source remains financially viable and capable to fulfill its contractual responsibilities. In many cases, a periodic review of a supplier’s financial health will suffice. Financial woes are rarely sudden and therefore can be detected well before insolvency becomes a real threat. For example, in the Land Rover case discussed below, the problem could have been discovered using simple financial ratios such as Debt-to-Asset leverage or the Current Ratio, which are defined below:

- **Debt to Assets = Total Liabilities / Assets**
- **Current Ratio = Current Asset / Current Liabilities**

In a healthy supply relationship, a firm should be able to rely on its partner to alert them of any impending issues, rather than its own due diligence. However, as Land Rover found out, this is not always the case...regardless of how strong the relationship may be perceived to be.

#### **4.9.1 Land Rover/UPF-Thompson Case – 12/15/01 – UK**

In December, 2001, UPF-Thompson, the sole supplier of chassis frames for Land Rover’s popular Discovery models, suddenly stopped shipping product. They had suddenly and unexpectedly become insolvent and were forced to claim bankruptcy protection. According to Michael Marecki, Director of Legal Affairs for Jaguar, Land Rover, and Aston Martin, “the way [they] learned of this was that one Friday morning no chassis frames were delivered” (Hoult, 2002). And the matter was made more complicated by the fact that Land Rover typically only received delivery of the frames two days before they were due to be used on the production line, as they no longer had the room to store them with the adoption of Ford’s just-in-time inventory system.



---

Many critics pointed out that Land Rover should never have relied on a single source for such a crucial component. At one point, a lawyer from KPMG, who were the receivers of UPF-Thompson, suggested that Land Rover source its supplies from more than one manufacturer, but Marecki was quick to point out that the Land Rover/UPF relationship went back a long time. Land Rover had actually given them business on the strength of that relationship even when they were not the lowest bidder (Hoult, 2002).

In this case, the supply crisis threatened to bring to a halt a product line that accounted for roughly one third of total revenues. Land Rover countered this by noting that single-sourcing was accepted throughout the auto industry as normal. Following the example of many leading Japanese auto manufacturers, Land Rover sourced over 90% of its components from single suppliers, citing high quality through continuous improvement and low costs through volume discounts as the driving forces behind the strategy. But it was not only Land Rover's reliance on a single supplier that had created such a huge problem for Land Rover; the company's vulnerability was also compromised by their new lean inventory system. Before Ford took over the company in May 2000, Land Rover typically had several months of inventory in the distribution pipeline. But under lean distribution, any disruption in the flow of components affected Land Rover immediately.

Only when Land Rover contacted UPF to determine the cause of the shipping delay did they become aware of the true gravity of the situation. UPF's receivers, KPMG, told Land Rover they were not prepared to deliver any more frames unless the company was willing to make a multi-million pound "goodwill" payment. This put Land Rover in a very difficult position as finding a new supplier would have suspended Discovery production for up to nine months while tooling was developed and led to 1,400 lay-offs at the company's assembly plant. An additional 10,000 jobs among Land Rover's other suppliers would also have been severely threatened. Shortly after this, Land Rover received written notification from KPMG asking it to buy the business or agree to a long-term supply contract. Land Rover was in big trouble and KPMG was well aware of the manufacturer's dependence on the flow of chassis from UPF, explicitly pointing out during a follow-up meeting that Land Rover would suffer catastrophic consequences if it did continue to receive frames. Land Rover, refusing to be strong-armed, rejected the offer and opted for arbitration.

---

After weeks of failed negotiations, the two took their cases to England's High Court, where a judge found KPMG's demands to be "arguably illegal" and granted an injunction preventing them from carrying out any of their threats, guaranteeing the flow of chassis on an interim basis (Hoult, 2002). After a lengthy series of appeals and additional hearings, the two parties eventually came to an agreement as to how the dispute would be settled. The final settlement entailed Land Rover paying between £10M and £20M of UPF's £50M debt in exchange for the replacement of KPMG with its preferred receiver.

While the flow of chassis never completely took down the Discovery assembly line, it came dangerously close. As Lester reported in his 2002 article, while Land Rover claims that it "keeps a careful and continuous financial review of all its suppliers, delving into order books and business and revenue plans (Lester, 2002)," UPF somehow managed to slip through the net. In the end, Land Rover was forced to absorb a portion of the supplier's debt to keep them financially viable and capable of supplying them with an uninterrupted flow of auto chassis. Had the company taken steps to maintain a tighter relationship with the UPF, the crisis may have been averted. But as it was, Land Rover took its eyes off of the "basket" and was left with a few broken eggs.

---

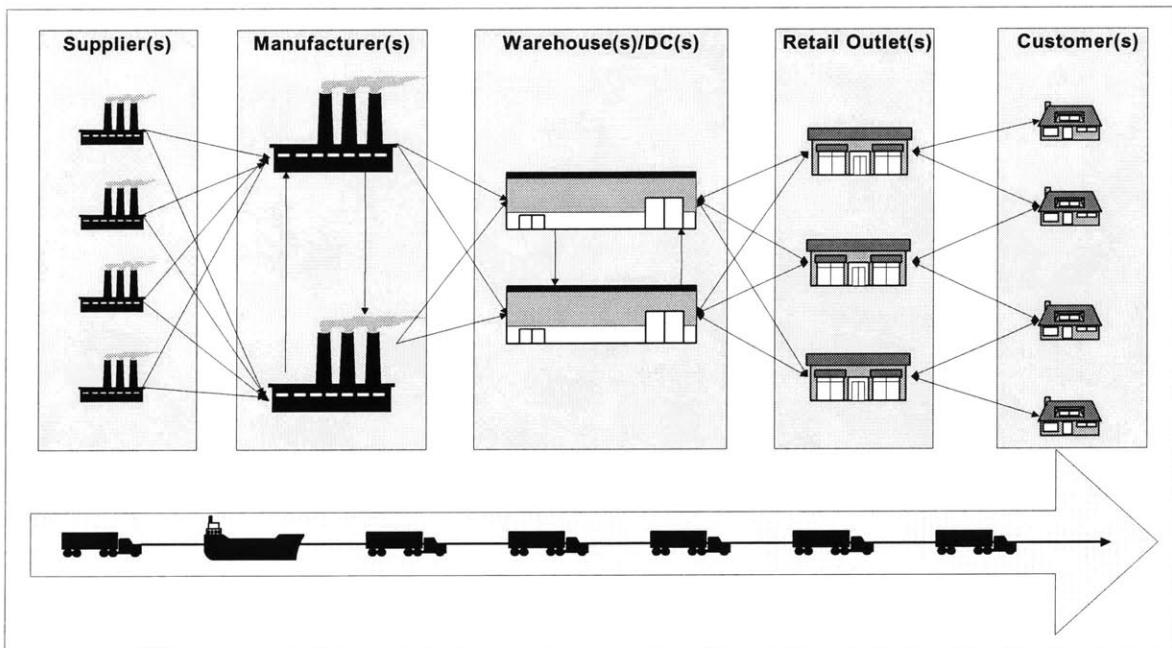
## Chapter 5: Vulnerabilities of the Modern Supply Chain

### 5.1 Survey of the Modern Supply Chain

As described in previous chapters, the modern supply chain can be extremely complex and fragile. Figure 28.0 below illustrates an example of a basic multi-tiered, multi-node supply network – one that can be found in a wide variety of product-oriented industries. Raw materials flow from suppliers to manufacturing centers and finished goods flow from the manufacturing centers to regional/local warehouses/distribution centers to one or more retail outlets and finally to the end consumers. However, recent trends have made for a much less linear and much more complex flow of goods, information, and funds across the supply chain.

Global outsourcing has pushed much supply chain functionality and responsibility out to 3<sup>rd</sup>-parties (contract manufacturers, 3PLs, transportation service providers, component/assembly suppliers, etc.) spread across an increasingly dispersed geographic area. In fact, modern product-oriented companies may not own a single plant, truck, or warehouse! Concurrently, the drive towards lean operations (JIT, etc.) has made supply chains very efficient but also very fragile, where a disruption at any node in the network can severely impact the overall flow of products, information, and funds. So in practice, an enterprise's supply network is often much more complex, however, for the purposes of this discussion, this simplified model will suffice.

Figure 28.0 – Modern Networked Supply Chain



---

## 5.2 Supply Chain Failure Modes

To reduce the task of planning for an infinite array of potential supply chain disruptions into an endeavor that is both manageable and useful, it is important to focus not on the specific nature of the disruption, but on how supply chain operations are likely to be impacted. In other words, organizations should focus on the failure modes, not on the failures themselves!

There are two primary reasons for this:

1. Firms cannot foresee every potential threat, let alone the probability of each threat coming to fruition. It simply isn't feasible, nor would it be practical. For example, prior to September 11<sup>th</sup>, 2001, it would have been unreasonable to expect most firms to have planned for a commercial airplane hitting their building.
2. Companies do not have to! As this study will describe, a very wide variety of disruptive events – whether they be earthquakes, hurricanes, ice storms, terrorist attacks, labor strikes, or supplier bankruptcy – tend to have very similar effects on the supply chain.

That is to say that while the root cause of a disruptive event may vary significantly over time, the impact on that event on the supply chain is likely to be very similar. So by analyzing the supply chain as a network of interconnected operational nodes and understanding the potential failure points within that network, firms can mitigate much of their risk regardless of the specific type of disruption the future may hold. These “potential failure points” are referred to as a supply chain's failure modes throughout much of this thesis. The six failure modes that provide the framework for this study are:

- Non-IT Physical Infrastructure
- IT/Communication Infrastructure
- Key Supply Source
- Manufacturing Capability
- Transportation/Distribution Capability
- Key Customer

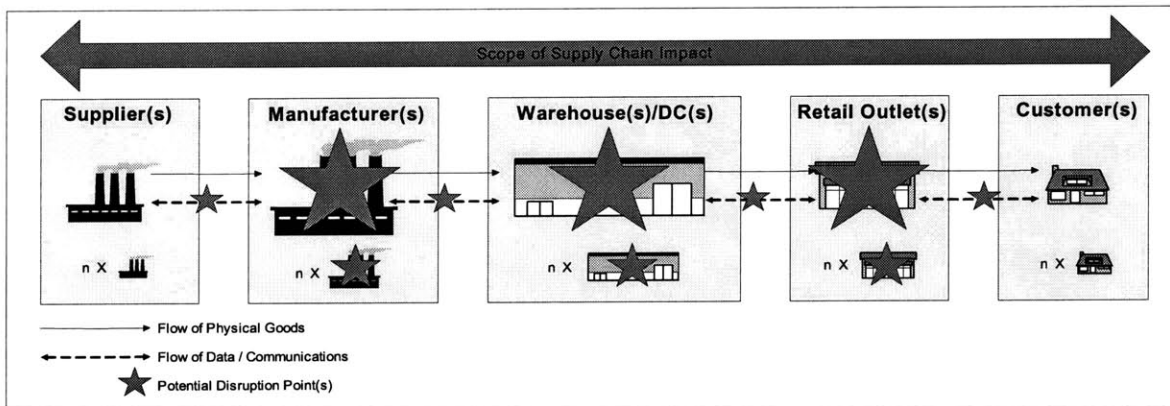
The remainder of Chapter 5 is devoted to describing these failure modes and exploring the different ways that they can be compromised, through a series of case studies, by the various types of disruptive events surveyed in Chapter 4.

---

### 5.2.1 Physical Infrastructure Disruption (Non-IT)

This refers to the scenario where a firm's physical assets (i.e. non-IT) were directly impacted by a disruptive event. For any number of reasons (earthquake, hurricane, power outage, terrorist attack, etc.), a company is faced with the task of re-locating and recovering significant operational assets in order to continue doing business. This could apply to key business functions, manufacturing capabilities, or even employees. Figure 29.0 below describes the impact of such a disruption on the flow of physical goods and/or information throughout the generic supply network. In addition, two cases – the Oklahoma Federal Credit Union and the New York Board of Trade – are outlined below to provide accounts of how this type of failure mode can occur, what it means for a firm, and how two such firms responded.

**Figure 29.0 – Potential Impact of Infrastructure Disruption**



#### 5.2.1.1 Oklahoma Federal Employee Credit Union – 04/16/95 – Terrorist Attack

Just after 9:00 a.m. on April 19, 1995, a powerful bomb ripped through the Alfred P. Murrah Federal Building in downtown Oklahoma City, proving to be one of the most brutal terrorist attacks in ever carried out on U.S. soil, second only to the events of September 11<sup>th</sup>. The blast, caused by a two to three ton device comprised of ammonium nitrate fertilizer and combustible fuel oil, destroyed one-third of the nine-story building from roof to ground and left a crater that was eight feet deep and over 30 feet wide. In all, 169 people were killed in the explosion that could be heard up to fifteen miles away. Of the various federal and private offices housed in the Murrah building – including the Bureau of Alcohol Tobacco and Firearms, the U.S. Customs Service, the Veterans Administration, and the U.S. Department of Housing and Development – the Oklahoma Federal Employee Credit Union (FECU) was dealt perhaps the fiercest blow.

---

While most of the building's tenants were branches of larger federal organizations, FECU was wholly located in the smoldering structure.

The FECU, located on the third floor, served over 15,000 members and held roughly \$75M in deposits and other assets. As Grayson Towler reports in his 1999 article on the event, "all information technology (IT) and infrastructure, all telecommunications equipment, all records, and all files were utterly laid to waste. Hundreds of thousands of dollars in checks, traveler's checks, and cash vanished into the smoldering rubble" (Towler, 1999). It was the human loss however, that was the most devastating. Of the credit union's 33 employees, 18 were killed in the blast, five were hospitalized with serious injuries, and the rest were left severely traumatized by the disaster that they had just witnessed. But with only three employees and the aid of numerous volunteers, FECU was re-opened for business by Friday morning, just 48 hours after the tragic bombing.

FECU's miraculous recovery can be attributed to three factors: a sound disaster recovery strategy, the support and assistance from other credit unions, and a little bit of good luck. Because the credit union already had a comprehensive yet flexible recovery plan in place, there was little doubt or confusion as to where recovery efforts should be directed in the hours and days following the attack. But it was only through the generosity of others and the fortunate survival of its key leadership structure that it was possible to for the plan to be implemented so successfully. As Towler notes, "amongst the survivors were CEO Florence Rogers, Vice President and Comptroller Raymond Stroud, and the FECU data processing specialist, Brad Grant. It was by sheer coincidence that Grant and Stroud were both out of town at the time. Florence Rogers was in the building when the blast struck – her survival is a miracle in and of itself. Thus, when the smoke cleared, the Credit Union had suffered an awful loss, but it did have the three key people it needed for recovery there to help restore it" (Towler, 1999).

A cornerstone of FECU's ongoing disaster recovery strategy was the off-site storage of all daily tape backups at a third-party disaster recovery facility managed by The Rock Island Group (RIG). Soon after the blast hit and RIG was contacted, they were able to ship a complete set of backup data to a hot site in Pennsylvania. And by the very next day, FECU was retrieving records and data at the hot site. The recovery had begun. While the short-term data restoration was underway at the emergency failover site, FECU also contracted RIG to begin rebuilding the

---

---

company's long-term transaction management capabilities and overall technology platform.

In the meantime, the surviving leadership team quickly mobilized to address the many non-technical aspects of the recovery. At 4:30 p.m. the day of the blast, an emergency session of the board was called. In addition to the CEOs of FECU and RIG, key leaders from seven other local credit unions were in attendance as well. Action was quick and decisive. The credit union executives would organize volunteers from their respective organizations and arrange for the personnel required to provide FECU with a functional staff. In addition, Matthew Stratton, CEO of nearby Tinker Credit Union, would manage the media and all public relations (PR) efforts. And because RIG, a third-party not located in the Oklahoma City area, was removed from the personal trauma that the members of the local credit union community were experiencing, it was deemed best suited to handle many of the remaining logistics of FECU's recovery. This included establishing an alternate branch location, which leveraged a training facility operated by one of the local credit unions. This alternate site would house the FECU until more permanent arrangements could be made. That left Florence Rogers, FECU's CEO, tasked with setting the strategic vision of the credit union and free to deal with the pain, suffering, and death of her coworkers, their families, and the credit union's members.

Although easy to overlook, Matthew Stratton's PR efforts were critical to the recovery process. His team organized press releases, ran radio commercials, and advertised in the local newspaper that FECU would be back online soon and that their members' needs would be met. Many members, confused and fearing that their deposits might be compromised, were reassured by the public declarations that FECU would continue to serve them. In addition, Towler notes that "local businesses, which initially feared that the FECU checks were no longer viable, were quickly and quietly informed that the credit union could still honor its payments" (Towler, 1999). These efforts were just as important as the work that RIG and the other credit unions were doing to restore IT systems, establish an alternate branch location, and arrange staffing.

When the FECU re-opened just 48 hours after the bombing, over 500 members visited the alternate site. While much of the physical rebuilding was behind them, the emotional and spiritual recovery had only just begun. As Towler observed, "not only were the employees of FECU and the volunteers struck afresh by the impact of the disaster because of their own experiences in returning to work, but they had to cope with the fact that over 90% of the workers

---

in the Murrah Federal Building were members of the credit union, including virtually all of the missing and dead” (Towler, 1999). In addition to overseeing the reconstruction of the FECU business infrastructure and technology platform, executives and staff dealt daily with the human loss. But through it all, the credit union remained open for business.

Several insights can be gleaned from FECU’s miraculous recovery. After suffering a complete loss of operating assets and information, as well as most of their staff, they were able to re-open their doors a mere 48 hours later. First, the fact that FECU had invested the time and resources to create a disaster recovery plan, which called for, among other things, keeping its computer backups offsite was critical to their resilience. If the credit union had not made backups, or had it kept them in close proximity to their branch office (i.e. in the same building), it could never have recovered from the destruction that it suffered. They also wisely chose to let an outside firm manage as much of the logistical needs of the business as possible. This allowed them to focus on the physical and mental well-being of their employees and customers. FECU’s experience also highlights how “media management becomes vital in a case where customers of a business might be confused about the well-being of that business. In such a high-profile situation, the fact that the attention of virtually all the customers was guaranteed to be focused on the media worked to the advantage of the public relations team” (Towler, 1999). In summary, FECU learned that having a disaster recovery strategy in place, while necessary, is not altogether sufficient. Execution is equally important. The Oklahoma Federal Employee Credit Union was successful only because they demonstrated excellence in both.

#### **5.2.1.2 New York Board of Trade – 09/11/01 – Terrorist Attack**

As with virtually every other organization with office space in or around the twin towers of the World Trade Center on September 11<sup>th</sup>, 2001, the New York Board of Trade (NYBOT) was suddenly left homeless in the aftermath of the al Qaeda terrorist attacks that toppled the towers and decimated much of the surrounding area. Unlike most other organizations however, especially those outside the financial services industry, they were ready with a backup hot site on standby for just such an emergency. As Carol Sliwa reports in her 2001 Computerworld.com article, NYBOT learned its lesson after the 1993 bombing of the World Trade Center and began investing in a “hot site” in Queens, NY that they could failover to in the event that either their main trading floor or central IT systems, or both, were rendered non-operational (Sliwa, 2001).



---

Prior to 1993, their disaster recovery capability consisted of a vacant “cold site” in Philadelphia that they rented from SunGard Data Systems Inc. Cold sites contain only the requisite backup hardware and network and must be activated from scratch using backup data tapes. Hot sites, on the other hand, are actual live systems that function as virtual mirrors of the primary technology platform. While hot sites are more desirable from a disaster recovery perspective, they are also much more expensive to maintain than a cold side. The NYBOT’s hot site cost them \$300,000 per year, which bought them space for a trading floor and a backup Compaq Himalaya 72000 mainframe computer at a business–recovery facility owned by Rosemont, Ill.-based Comdisco Inc. According to CEO Mark Fichtel: “That was a hot topic at the last budget cycle: Why should we continue to spend \$300,000 for something we’ll never use? That’s what insurance is all about. You hate paying the premiums, but you’re sure glad you did when you have to collect” (Sliwa, 2001).

The firm continued to invest in the Queens, NY hot site, but refused to let it lie dormant until the next disaster came around. The Board of Trade also used the backup system as a development environment where it could code and test software updates to its production environment before actually implementing them in the primary system. They also used it to exercise their failover capability. Sliwa goes on to describe how, “on a quarterly basis, IT staffers descended on the deserted Queens facility to test the disaster plan, much as they might conduct a fire drill. A typical test would run an hour and 45 minutes. ‘No one liked to do it,’ said Ian Nelson, vice president of technical operations. ‘It always meant coming in on a Saturday and spending a beautiful day here.’” (Sliwa, 2001) In an ironic twist of fate, the test scheduled for September 8<sup>th</sup> had been moved to September 15<sup>th</sup> because of some utility work being performed at their headquarters in the World Trade Center complex.

But because of the firm’s investment in disaster recovery capability and their disciplined approach to practice and training, they were ready when the unthinkable happened on September 11<sup>th</sup> and the plan had to be implemented for real. This was not a drill. The recovery was executed as planned and all systems were restored within a couple days. As Sliwa describes: “Trades on Tuesday –the day of the attack – got settled that night, and clearings were done Wednesday. IT staffers worked to get software to clearing partners as quickly as they could. By Friday, the Board of Trade was ready for a test run, and on Saturday it did a walk–through with members at the temporary site. On Monday, trading commenced” (Sliwa, 2001). That did not

---

---

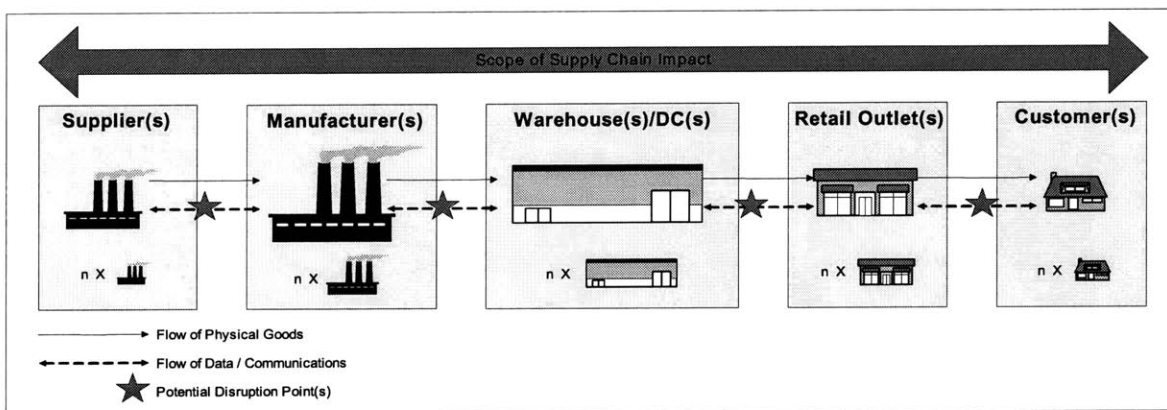
mean, however, that the transition was seamless. The NYBOT soon learned that there were several minor holes in their recovery strategy. For example, employees lost contact in saved e-mail when it was discovered that several applications running on Windows NT were not backed up. The firm also learned a painful lesson in backing up and safeguarding data. The backup tapes that it would need to restore its financial records were sitting in a 4ft. x 6ft. fireproof safe buried beneath many layers of rubble at ground zero in lower Manhattan. Much of the data had to be reconstructed from outside sources.

But outside of a few minor details, the New York Board of Trade made a brilliant recovery. The once-contentious \$300,000 insurance policy had paid off in spades. Says NYBOT CEO Fichtel: "Whether it takes a month or even a few days to return to its headquarters, Fichtel said the \$300,000 insurance policy was worth it" (Sliwa, 1999). He goes on to note that: "if you're not ready and you are effectively shut down for any length of time, it is a very competitive world, and people will take your business away from you" (Sliwa, 1999). Because the Board of Trade was ready, it was able to react to the September 11<sup>th</sup> attacks and ensured that traders would have somewhere to do business, with both a trading floor and a stable computing platform, when trading commenced just a few days later on September 17<sup>th</sup>.

## 5.2.2 IT/Communication Disruption

In this scenario, it is the organization's IT assets (data, communications, applications, etc.) that are primarily affected by the disruptive event. Perhaps none of these operational capabilities were compromised, but the underlying technology infrastructure was. And in this increasingly IT-dependent business environment, that problem is at least as significant, if not more so. Figure 30.0 below describes the impact of such a disruption on the flow of physical goods and/or information throughout the generic supply network. In addition, three cases – ING Property & Casualty, Merrill Lynch, and Sidley Austin Brown & Wood LLP – are outlined below to provide accounts of how this type of failure mode can occur, what it means for a firm, and how three such firms responded.

Figure 30.0 – Potential Impact of IT Disruption



### 5.2.2.1 ING Canada Property & Casualty – 01/15/98 – Quebec Ice Storm

One of the hardest hit casualties of the 1998 Quebec Ice Storm, the massive ice storm that blasted parts of New York State, New England, Quebec and Ontario, was the power grid. Dennis Bueckert (1998) of the Associated Press reported that over 1,000 transmission tower and 30,000 utility poles failed under the burden of several layers of heavy ice (Bueckert, 1998). The extent of the damage is described further in Figure 44.0, an appendix item that shows the status of HydroQuebec's electric grid during peak storm conditions. Downed power lines resulted in extended outages that wreaked havoc on the operation of information technology facilities located within the affected areas. A division of International Netherlands Group, ING Canada Property and Casualty, headquartered in Montreal, was particularly hard-hit. ING was an

---

industry leader with over half a million customers and counted customer service and satisfaction as top priorities and something that differentiated it from competitors. Several years earlier, ING made the decision to outsource the operation of its central data center in Saint-Hyacinthe, Quebec to Computer Sciences Corporation (CSC). A hot site recovery agreement was also in place with Comdisco, a leading disaster recovery specialist.

According to a case study by prepared by Philip Rothstein in March 1998, when the first wave of the ice storm hit at around 10 a.m. on January 7, 1998, a Wednesday, the data center quickly lost power. As expected, an uninterruptible power system (UPS) and backup generator effectively took over the short-term load for ING's mainframe (Rothstein, 1998). So far, so good. Unfortunately, the power outage would not prove to be a short-term inconvenience. Operations were estimated to be impacted for over two weeks. ING, CSC, and Comdisco went to work planning for the extended outage. Says Robert Proulx, First Vice President of Technology and Systems for ING: "Three major risk factors were identified: (1) power, (2) the telecommunications network serving all of Canada, and (3) people. An important characteristic was that [they] were facing a major issue – because of downed poles and wires in the road – getting people to the data center" (Rothstein, 1998). Proulx advised Comdisco that night that ING was formally declaring a disaster, prompting Comdisco to activate their Toronto, Ontario recovery center. Although the Saint-Hyacinthe location was up and running on backup power, they understood that backup systems were designed to run for hours or maybe even days, but certainly not for weeks. The situation was also complicated by the fact that the fuel tank on the back up generator was only half full for a maximum runtime of 24 hours and the chance of getting a fuel delivery within the next 24 hours was uncertain at best. Operations were immediately transitioned to Toronto.

In the meantime, data traffic was also beginning to spike. According to Rothstein, "ING's property and casualty claims processing exceeded five times normal volume" throughout the ordeal and "ING elected to continue claims operations straight through the weekend, compounding the already high stress level on their information systems" (Rothstein, 1998). As the power outage continued, management was forced to make decision after decision, always carefully considering the risks and the likely benefits of each alternative. For example, the chose to immediately install a backup generator and continue running from the Saint-Hyacinthe location rather than risk transitioning live operations to the backup site while in the midst of a

---

---

major traffic spike. Loss of data and customer service were the primary concerns.

During the twelve days that ING operated on generator power from the Saint-Hyacinthe site, they were running in parallel with Comdisco's Toronto recovery site as well. As a precaution, they took backups and refreshed the system on a nightly basis at the recovery site so they were never more than about eight hours out of synch with their primary systems. Utility power returned to Saint-Hyacinthe the following weekend, however, ING chose to remain on generator power for several days. "Proulx worried that utility power would continue to be unstable for some time as continuing repairs added load to the power grid, and as weakened or damaged power supply components failed once power was reapplied. At Proulx's Montreal office, he was unnerved by four power drops during one afternoon" (Rothstein, 1998). Eventually, utility power did stabilize and all operations were restored to normal.

There are several reasons for ING's success, not least of all the concern that the insurer placed on the employees that were keeping the systems running. "Long hours, tremendous workloads and unreasonable stress were only part of the problem. Housing, feeding and caring for hundreds of employees – many displaced from their homes and dealing with personal crises – was essential. [They] were serving over 800 lunches, 700 dinners and 700 breakfasts each day [at Saint-Hyacinthe]. [They] even had to install showers. Many people were working fourteen or fifteen hours a day at five degrees Celsius" (Rothstein, 1998). ING also exercised superb planning and execution. Long before the ice storm, they recognized the potential impact of a data center disruption and had the foresight to develop a contingency plan. As Rothstein notes: "Thanks to a combination of advance planning, extensive testing and fast footwork in the clinch to deal with last-minute revelations, communications were successfully rerouted and, remarkably, ING Canada Property & Casualty never stopped doing business with their customers throughout the Ice Age of 1998" (Rothstein, 1998).

---

### 5.2.2.2 Merrill Lynch – 09/11/01 – Terrorist Attack

When terrorists brought down the twin towers of the World Trade Center on September 11<sup>th</sup>, 2001, Merrill Lynch and Co. suddenly found itself without its world headquarters. One of the world's leading financial management and advisory firms, Merrill Lynch occupied several floors of the World Financial Center, located directly across the street from the World Trade Center towers. Additional Merrill Lynch office buildings in close proximity to ground zero were also affected, displacing a total of 9,000 employees. However, general preparedness, sound contingency planning, and disciplined testing allowed the financial powerhouse to absorb the shock and return to normal operations while barely skipping a beat. "According to Paul Honey, Director of Global Contingency Planning, the financial firm was able to successfully evacuate their headquarters and resume critical management functions within minutes of the terrorist attack"(Ballman, 2001).

Almost immediately after the first plane struck, the company's emergency management jumped into action and initiated the evacuation process. And "within just a few minutes of the evacuation, Merrill Lynch was able to switch its critical management functions to their command center in New Jersey, explained Honey. Since the command center had been pre-designated in corporate-wide contingency plans, all personnel immediately knew where to dial into and transfer information. This allowed transactions throughout the company's global offices to continue as usual"(Ballman, 2001).

While the World Financial Center, where Merrill Lynch had its headquarters, was not toppled in the attack, it did sustain many broken windows and suffered extensive damage from fallen debris. But because the building was located within the area defined as 'ground zero', tenants would not be granted access, outside of the opportunity to perform an initial damage assessment, for up to several weeks or longer. The entire area would be cordoned off to facilitate rescue and recovery operations. Merrill Lynch would have to find somewhere else for its 9,000 displaced employees to work. Managers immediately got to work locating available office space. Fortunately, they did not have to look far, or even outside the company. Explained Honey, "[they] took advantage of all existing Merrill facilities." Miraculously, they had 8,000 employees back at work by Monday, September 17<sup>th</sup>. And when exchanges re-opened the same day, Merrill Lynch was ready and prepared to operate from its alternate location(s) for as long as it had to. Commenting just after the transition, Honey declared that "it has taken a massive

---

---

effort by all of our employees, but it is business as usual at Merrill Lynch. We were very, very well prepared”(Ballman, 2001).

Much of the company’s success can be attributed to the disciplined nature by which it approached contingency planning; plans were tested extensively and constantly upgraded as environmental conditions changed. In fact, the firm had recently tested their plans via a scenario that, while not a terrorist attack, was a disaster of similar scope and had an analogous impact on operations. Their rigorous Year-2000 (Y2K) preparations also proved to be invaluable in conditioning the firm to respond and recover in a time of crisis. Says Honey: “The Y2K tests really helped us to prepare for this event. During that time, we had 60 command centers around the world. We honed our plans and tested them, and have since improved our contingency planning efforts. We learned a lot during the Y2K planning stages and leveraged that knowledge to upgrade and improve our command center operations” (Ballman, 2001).

The support of senior management was another reason that Merrill Lynch was so successful in their recovery efforts. Managers accurately recognized the risks and the impact of downtime to their business, regardless of the cause. They understood the need for continuous upgrading and testing of corporate contingency plans and committed significant firm resources to ensure that they were as prepared as they could be for whatever calamity may lie in their future. As Honey notes, “We are actively involved in keeping our plan current and are even backing up our backup plans” (Ballman, 2001).

The third key to Merrill Lynch’s success lied in their focus on the well-being of their employees. With all of the focus on hot-sites, IT redundancy, and data integrity, they never lost site of the fact that it was the employees that made everything go. Management readily acknowledges that the most important aspect of the recovery was on the human side and expressed great concern for the health of their staff. For example, the firm ensured that emotional/psychological assistance was made available for all employees that needed it, bringing in counselors that had consulted with victims of the Oklahoma City bombing in 1995. In summary, Merrill Lynch made the best of a tragic situation with sound preparation, made possible with executive support for contingency planning initiatives, and an unwavering focus on the well-being of their people. Because as Honey concludes, “[their] employees are the firm’s greatest asset” (Ballman, 2001).

---

### 5.2.2.3 Sidley Austin Brown & Wood LLP – 09/11/01 – Terrorist Attack

On September 10<sup>th</sup>, 2001, Sidley, Austin, Brown, & Wood LLP (SABW), was a multi-national law firm with staff of 1,500 lawyers (3,000 total employees) working from fourteen offices in six countries. Two of those offices were located in New York City, one of which supported 600 employees in the North Tower of the World Trade Center. In the days leading up to the September 11<sup>th</sup> terrorist attacks, SABW was engaged in one of the largest law firm mergers ever and was still in the process of the consolidating the firms' multiple technology platforms. As discussed in a disaster recovery presentation given by SABW's Joy Heath-Porter at the 2002 LawNet conference: "the firms were on two networks with two different hubs, two different e-mail and document management systems, and two different telephony systems" (Heath-Porter, 2002). In fact, they had just moved equipment to the WTC the previous weekend to facilitate the consolidation.

At approximately 8:45 a.m. on Tuesday, September 11th, American Airlines flight 11 was deliberately flown into the North Tower of the World Trade by its al-Qaeda hijackers. The firm's pending merger and technology consolidation initiative suddenly became the least of its worries. Fortunately, all of SABW's employees that were in the WTC office at the time escaped unharmed. Once all employees were accounted for, management immediately went into damage control mode. By mid-morning, a disaster steering group had been assembled, which began to map out a recovery strategy. The recovery of office IT systems and office space were the primary concerns. By noon, the firm had contacted its off-site storage provide and arrangements were made to drive the office's backup data tapes to SABW's Chicago office where system recovery would occur. Because the firm took a self-proclaimed "maniacal" approach to tape backups, backing up daily and transferring the tapes to an offsite storage location outside the NYC metropolitan area, all but only a couple of hours of data could be recovered. This would prove to be a key success factor for SABW's recovery.

While plans were being developed and executed for the firm's IT recovery, they also took steps to reassure their many worried employees that were calling in from around the globe. They established an 800 number, which was posted on its corporate website, for employees and ensured that it was staffed by live operators so that staff calling in would have a "live" voice to talk to. By Wednesday morning, recovery team began contacting other SABW offices to locate surplus equipment – PCs, desks, telephones, etc. – that could be used to help equip an alternate

---



---

New York office location. The firm's PC vendor was also contacted and arrangements were made to ship several hundred workstations within the week.

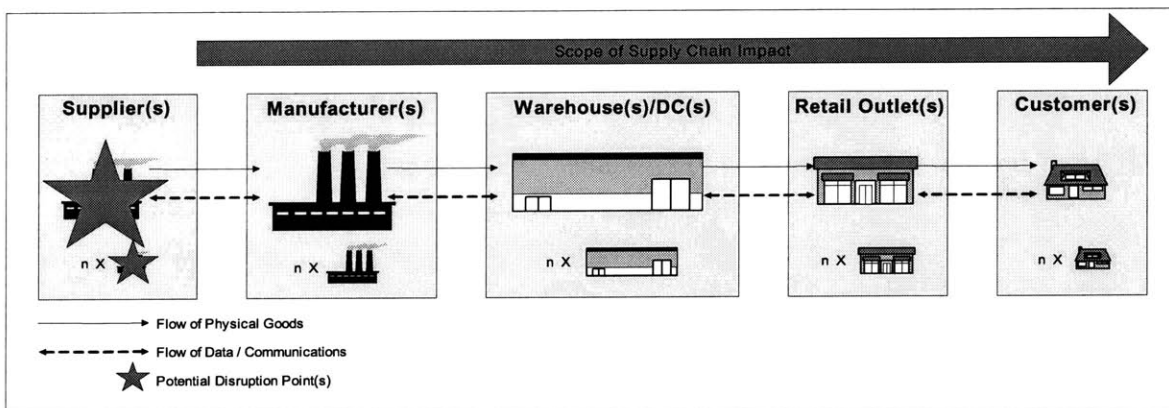
By end of day Wednesday, the tapes had arrived in Chicago and the data restoration process had begun, starting with the e-mail server. All internet mail was then re-directed to the new domain and voice mail accounts were established on an alternate system. By Friday afternoon, a restored document management system was available to New York users and office equipment began arriving at the alternate office location. Throughout the weekend, SABW's IT team worked feverishly to set up phones, network equipment, printers, desks, and PCs at the New York site. At 10 a.m., the firm assembled all New York personnel for a briefing and by noon, they all reported for work at the alternate site. SABW's New York office was fully functional and virtually all firm data was restored. The firm would remain in the temporary location until the following July 4<sup>th</sup> weekend before moving into a permanent home in mid-town Manhattan.

For all intents and purposes, SABW performed brilliantly in the face of the September 11<sup>th</sup> tragedy. The firm was never really "down", their clients were impressed, and most importantly, all of their people were safe. Several key success factors made this possible. First, their disciplined approach to backing up their data significantly reduced their exposure to extensive data loss. Because they backed up daily and stored their tapes offsite, their data was never older than one day and was far enough away so as not to be compromised by the disruption. Had SABW stored their tapes in the South Tower of the World Trade Center for example, recovery would have been much more difficult. Ms. Heath-Porter also points out that maintaining standardized hardware – including network configurations, PC's, and telephones – with standard images dramatically improved their ability to make a rapid recovery (Heath-Porter, 2002). A third key for SABW was the degree to which they planned for and practiced recovering systems under disaster scenarios. While they certainly never anticipated a plane hitting their building, they didn't have to. If well-conceived, basic disaster recovery practices are applicable to virtually any scenario; the source of the disruption is irrelevant. What is relevant is that employees understand what their responsibilities are should disaster strike and be able to implement basic recovery plans "in their sleep" (Heath-Porter, 2002). In simplest terms, SABW was successful because they were prepared. They had a sound recovery plan and an able and determined staff to execute that plan and make adjustments as the situation called for.

### 5.2.3 Supply Disruption

This failure mode applies when an organization may not have been directly impacted by the event, one or more of its key suppliers was. And a company can't produce if it doesn't have the required component parts or subassemblies in the right place at the right time. Figure 31.0 below describes the impact of such a disruption on the flow of physical goods and/or information throughout the generic supply network. In addition, two cases – Dole Vs. Chiquita and Dell Vs. Apple – are outlined below to provide accounts of how this type of failure mode can occur, what it means for a firm, and how four such firms responded.

**Figure 31.0 – Potential Impact of Supply Disruption**



#### 5.2.3.1 Dole Vs. Chiquita – 10/22/98 – Hurricane Mitch

When Hurricane Mitch wreaked havoc on much of Central America in October 1998, it destroyed roads, bridges, railroad tracks, factories, houses...and banana plantations. Of the reported 50% loss to Honduras' agricultural crops – 70% of its total economic output – bananas were especially hard hit. Mitch had claimed 10% of the worldwide crop. According to Martha & Subbarkrishna's (2002) paper, when the rains finally relented, Dole had lost an estimated 70% of its 40,000 acres in Honduras, Guatemala, and Nicaragua; roughly ¼ of its total global production. Chiquita Brands also suffered, losing an estimated \$200M in expected output from its 40+ farms located in the affected regions (Martha & Subbarkrishna, 2002). While these two leading global banana producers lost most of their Central American capacity, they each reacted quite differently to the disaster – producing very different results.

---

Once the impact of the disaster was known, Chiquita immediately implemented a plan to locate and leverage alternate sources of supply in the region. To make up for the lost crops, they increased production at other locations and purchased fruit from associate producers in areas that were not affected by Mitch. Dole, on the other hand, had no strategy in place for alternate sourcing and suffered an interruption in Central American supply for over a year. The end result for Chiquita was a 4% increase in fourth quarter (1998) revenues, while Dole suffered a 4% decline in revenues and was forced to take a special charge of \$100M for the same period. This is a classic example of two firms with identical businesses that reacted very differently when faced with identical disruptive circumstances. Because Chiquita had secondary sources of local supply, Martha & Subbakrishna attest, it was able to successfully avert the prolonged and expensive supply gap that haunted Dole for the entire following year (Martha & Subbakrishna, 2002).

#### **5.2.3.2 Dell Vs. Apple – 09/21/99 – Taiwan Earthquake**

When an earthquake rocked Chi-Chi, Taiwan on September 21, 1999, the widespread loss of power coupled with the physical damage to the manufacturing facilities of several major semiconductor suppliers disrupted the flow of components to many PC and laptop OEMs for several weeks. Two leading computer makers, Apple and Dell, were equally affected yet reacted quite differently to the supply crunch.

According to Martha & Subbakrishna (2002), the earthquake presented Apple Computer with an immediate shortage of semiconductors and other critical components for both its iBook laptop and G4 desktop product lines. And the delay couldn't have come at a worse time as both were relatively new on the market and demand had been growing steadily over the recent weeks. Apple responded by shipping a slower version of the G4, but relented when the move generated an avalanche of customer complaints. The problem persisted into the 4<sup>th</sup> quarter as the company was unable to modify the configurations of previously ordered models. Most customers responded by either ordering lower margin machines instead or canceling their Apple orders altogether.

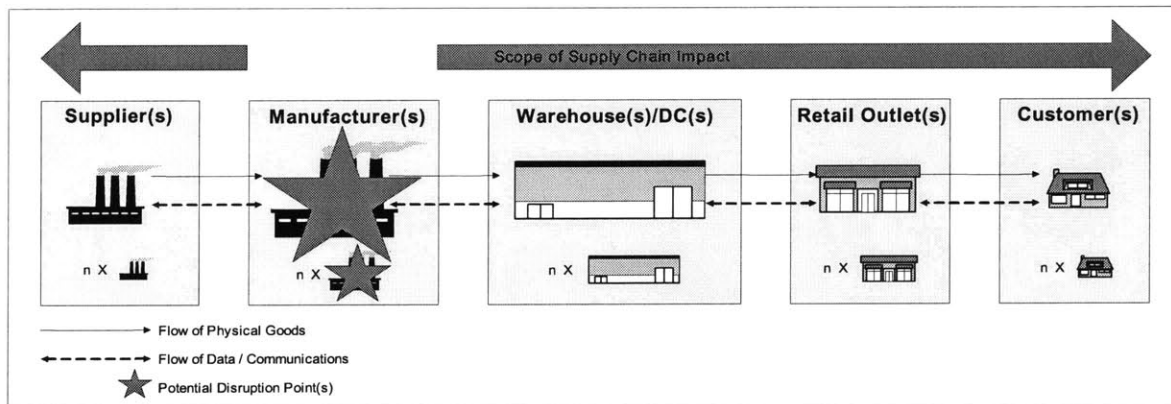
Dell, on the other hand, weathered the storm much better. Although their famously lean build-to-order operating strategy meant that they held only five days of inventory, their “sell-what-you-have” sales model allowed them to direct customers to products for which they could build

with available components. The inherent nature of their build-to-order system also prevented them from experiencing the same “hard-configuration” issues that hurt Apple. Instead of losing customer sales and disappointing customers, Dell actually thrived, achieving higher 3<sup>rd</sup> quarter earnings over the previous year by 41% (Martha & Subbarkrishna, 2002).

### 5.2.4 Manufacturing Disruption

In this scenario, a firm’s ability to produce goods or provide services is compromised by a disruption in the supply chain that directly impacts its manufacturing assets. This could also apply to an outsource situation where a 3<sup>rd</sup>-party contract manufacturer was impacted. For examples, a fire or hurricane at one or more production facilities could significantly diminish a firm’s manufacturing capacity, disrupting both upstream and downstream supply chain operations. Figure 32.0 below describes the impact of such a disruption on the flow of physical goods and/or information throughout the generic supply network. In addition, two examples – Unilever and Compaq – are discussed below and provide accounts of how this type of failure mode can occur, what it means for a firm, and how two such firms have either responded or shielded themselves from future manufacturing disruptions.

**Figure 32.0 – Potential Impact of Manufacturing Disruption**



---

#### **5.2.4.1 Unilever – 10/28/98 – Hurricane Mitch**

According to Martha & Subbarkrishna (2002), when Hurricane Mitch swept through Central America in 1998, a Unilever suffered extensive damage to a manufacturing facility in Puerto Rico that produced roughly half of the North American supply of Q-Tip brand cotton swabs. As a result, they lost two weeks of production and forced many of customers into stock-out situations. Despite this experience, Unilever chose to re-locate 100% of its Q-Tip production back to the Puerto Rico facility after repairs were made. To mitigate their exposure to similar disruptions to production, they increased inventory levels in North America by 10%. They also arranged contracts with barge shippers in the event that road or rail systems were made unavailable. In this case, while Unilever chose to consolidate manufacturing in a single location, likely to take advantage of attractive labor costs and economies of scale, they introduced learned from their experience from Hurricane Mitch and introduced new means to mitigate their risk of future disruptions (Martha & Subbarkrishna, 2002).

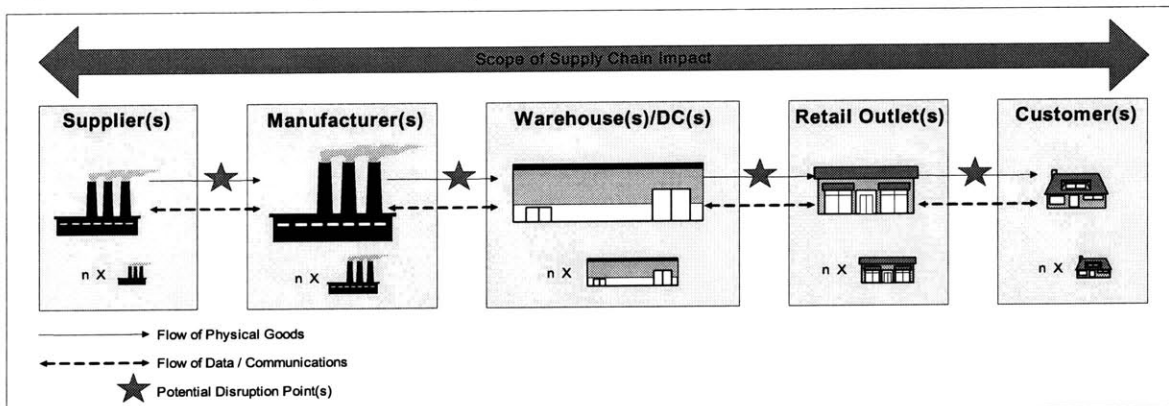
#### **5.2.4.2 Compaq Computer – General Best Practices**

To mitigate the risk of lost production due to supply chain disruptions, Martha & Subbarkrishna (2002) attest, Compaq implemented a formal business continuity plan that includes the ability to shift production to different parts of the world. Compaq has assembly facilities in Europe, North America, South America, and Asia, and can quickly shift production between them in response to extreme weather or political strife, for example, might affect one or more regions. The plan also requires a secondary supplier for all critical components and recommends that foreign suppliers have secondary facilities within the United States (Martha & Subbarkrishna, 2002).

## 5.2.5 Transportation/Distribution Disruption

In many cases, each node in the network may not have been directly impacted mode, but the organization's ability to transport raw materials, WIP, and/or finished goods from one node to another may still be vulnerable. For example, a transportation service provider could suddenly go out of business, a port could close, or a terrorist attack could effectively close one or more borders. All of these could, and have in the past, severely compromise a firm's ability to move materials from point A to point B and hence effectively run its business. Figure 33.0 below describes the impact of such a disruption on the flow of physical goods and/or information throughout the generic supply network. In addition, five cases – Rocket Air USA, Continental Teves, Ford Vs. Daimler-Chrysler, Toyota/GM NUMMI, and Dow Corning – are outlined below to provide accounts of how this type of failure mode can occur, what it means for a firm, and how several such firms responded.

Figure 33.0 – Potential Impact of Transportation Disruption



### 5.2.5.1 Rocket USA Inc. – 08/04/97 – 1997 UPS Strike

Headquartered in Forest Park, IL, Rocket USA is a marketer of toys, games and collectibles that feature characters from cartoons like *Futurama* and *The Simpsons*. In the space of just a few short months during the summer of 1997, the 5-person start-up company had done virtually everything that it could to prepare for its first product launch. According to Ruberry's 1998 article in *Entrepreneur* magazine, all that was left was to sign the contract with a Japanese company that would be the sole distributor for a line of collectible windup toys, including the robot from the original "Lost in Space" television series (Ruberry, 1998). Michael Perry, the company's President and Co-founder had planned for everything, or so he thought. Just as

---

C.O.D. orders began to stream in and the first inventory of robots filled the warehouse, UPS declared a company-wide labor strike that effectively brought all operations to a grinding halt. While the shutdown proved to be a major inconvenience for many small businesses, it was a catastrophic disaster for Rocket. The struggling start-up did not have accounts with alternate carriers and quickly discovered that many carriers would accept business only from current customers. Says Perry: “We were totally in the dark about how we were going to ship. We had to hand-carry orders to the post office [because] we really had no backup plan” (Ruberry, 1998).

Rocket USA’s experience should serve as an important lesson for other small business owners. While supply chain disruptions can certainly be damaging for large businesses, small operations are even more susceptible and can be forced out of business by even a minor crisis. The margin for error is often razor thin for cash-strapped businesses trying to establish themselves in an increasingly competitive marketplace. Rocket was able to weather the UPS storm and took valuable lessons from the harrowing experience. They quickly transitioned to a much more diverse distribution system with enough contingency shipping relationships to ensure that orders flow smoothly even if one of the major were to strike.

#### **5.2.5.2 Continental Teves – 09/11/01 – Terrorist Attack**

As the management team of Continental Teves, a tier-1 supplier to the auto industry, monitored the September 11, 2001 terrorist attacks from their headquarters in Auburn Hills, MI, they quickly realized that global supply chain operations would be significantly affected. A crisis team, comprised of purchasing and logistics managers, was immediately assembled to determine the magnitude of the disruption. As outlined in Martha & Subbakrishna’s 2002 paper, they first assembled a list of customers, parts, and supplier orders outstanding. Next, they identified where each order came from, whether or not it was deemed critical, and whether or not it was vulnerable to delay from the quickly deteriorating U.S. transportation environment. By the afternoon, they had identified all North American shipments that required immediate attention, expediting many of those via ground transportation. For parts sourced from overseas, the crisis team leveraged existing contingency plans with its carriers to expedite some scheduled and planned using air transport. Continental’s quick response and comprehensive impact assessment allowed it to deliver with minimal disruption over the weeks following the attacks (Marsh & Subbakrishna, 2002).

---

### **5.2.5.3 Ford vs. Daimler-Chrysler – 09/11/01 – Terrorist Attack**

The aftermath of the September 11<sup>th</sup> terrorist attacks included an immediate and dramatic increase in security at all customs points along the U.S. borders with Canada and Mexico. Air traffic was also brought to a standstill for several days; several weeks would pass before the government permitted carriers to resume unrestricted operations. These actions, as necessary as they may have been for national security, resulted in long delays at border crossings for many weeks after the attacks. The delays significantly disrupted the flow of goods across North America, wreaking havoc on the just-in-time inventory systems implemented by many industries, particularly the large auto makers, over the past twenty years. To minimize inventory carrying costs, attest Martha & Subbakrishna (2002), companies like Ford and Daimler-Chrysler depended on the frequent replenishment of components and sub-assemblies to maintain a steady rate of production. If the right parts were not in the right place at the right time, the assembly line would come to a screeching halt, costing millions of dollars in idle resources and lost production capacity. For Ford Motor Company, this unfortunately became the case in the days and weeks following September 11<sup>th</sup>. As shipments of engines and drive-train parts became stalled at the Canadian border, Ford quickly exhausted any on-site inventory it may have been carrying and was eventually forced to idle five of its U.S. plants. As a result, Ford produced 13% fewer vehicles than planned for the fourth quarter of 2001 (Martha & Subbakrishna, 2002).

Daimler-Chrysler, however, showed that proper planning and sound execution can go a long way in minimizing the impact of even the most severe of supply chain disruptions. By September 12<sup>th</sup>, the company's Michigan-based logistics staff had conducted a comprehensive analysis of their production flow and identified all parts movements (in-transit shipments, open orders, etc.) that warranted immediate attention. When the team realized that they would be running dangerously low on an updated steering-gear unit for the Ram pickup truck, they team intervened to arrange an alternate means of shipping. Normally, the part is air-shipped from a TRW plant in Virginia to a Chrysler assembly plant in Mexico. To minimize the potential delay, they worked with the supplier and arranged for the parts to be transported via an expedited truck service. In this case, there was not much that either company could do beforehand to anticipate the temporary collapse of the entire U.S. transportation industry. The difference came, however, in how each company reacted to the disruption. Daimler-Chrysler acted immediately to determine their exposure while Ford did not seem to exhibit the same sense of urgency and managerial discipline. And once Daimler-Chrysler made the decision to act, they already had

---



---

the tools in place that provided the supply chain visibility and control that they needed to accurately assess and react to the situation.

#### **5.2.5.4 Toyota/GM NUMMI Plant – 09/29/02 – Port Lockout**

By the time a labor dispute finally closed down the 29 ports that line the coast of the western United States, most businesses had over three months to plan for the disruption and arrange for alternate shipping arrangements; some even longer. According to a story printed in the Honolulu Star-Bulletin, Limited Brands – operators of Limited, Express, and Victoria’s Secret – had been preparing for over nine months. The apparel retailer re-routed several ocean shipments to Miami and secured capacity with air carriers that it was able to quickly transition to when port closures became imminent (Star-Bulletin, 2002). Wal-Mart Stores also took steps to shield its business from disruption. Tom Williams, a company spokesman, stated that “[they] had accelerated deliveries” to build up safety stocks and reduce their dependency on the frequent deliveries that characterizes their steady-state inventory strategy. A Salomon Smith Barney report confirmed this by noting that the world’s largest retailer had three to five weeks of inventory stocked at its store locations and distribution centers in anticipation of the port shutdown (Star-Bulletin, 2002). Some businesses, however, did not heed the warnings and did not take steps to adequately protect their operations as companies like Limited and Wal-Mart had. Fremont, CA-based New United Motor Manufacturing Inc. (NUMMI), a joint venture assembly plant owned by General Motors (GM) and Toyota, was one of those businesses.

At the time, the NUMMI plant was the only major vehicle production line west of the Mississippi where it assembled the Chevrolet Prizm, the Toyota Corolla, and the Toyota Tacoma. Typically, 34 containers of car (8) and truck parts (26) would arrive at the port of Oakland every day where they would be unloaded and trucked the 40 miles to the NUMMI factory for immediate use. When the Port of Oakland was closed on Sunday, September 29<sup>th</sup> 2002 in response to the breakdown in negotiations between the Pacific Maritime Association and the International Longshore & Warehouse, the flow of containers suddenly became anything but typical. Until the ports were re\_opened ten days later, NUMMI’s engines, transmissions, and vehicle frames would sit idle in cargo bays at the Port of Oakland or on ships anchored off the coast of Northern California.

---

As quoted by Sarker in a 2002 article, according to plant spokesman Michael Damer, “NUMMI stopped the truck production line at 11:25 p.m. [the following] Wednesday and stopped assembling General Motors and Toyota cars about an hour later” (Sarker, 2002). Workers were simply unable to finish assembling vehicles together as they waited for out of stock components. Plant operations ground to a halt, idling roughly 5,500 employees with an annual payroll of \$300M. While NUMMI certainly had ample time to anticipate the port closure, their Just-In-Time inventory strategy would not permit them to carry excess inventory and the considerable cost of air-freight made them reluctant to commit to that alternative until they absolutely had to. One freight company told BBC News Online that the difference between shipping and air-freighting cargo averaged \$53,000 per container. And according to a NUMMI spokesman, air-freight “would increase production costs of the cars by \$300 to \$600 each, and the trucks by \$2,000 apiece” (Sarker, 2002). They eventually did opt to charter several 747s to bring parts in from Japan, but only for the car assembly line as the option was viewed as cost prohibitive for truck assembly. Because shipping contracts were not arranged prior to the shutdown, NUMMI was forced to pay inflated rates due to the heavy demand. They also waited until one week after the Port of Oakland closed before air-freighting the much-needed inventory, hoping that the labor dispute would be resolved quickly. It didn’t and they were forced to endure a week of production downtime.

The production lines at NUMMI eventually did come back to life, first with the 40 air-freighted containers of car parts, then with the containers of car and truck parts that began arriving when the port lockout was finally resolved ten days after it started. With overtime and extra shifts, the plant was however able to recover all of the lost production. According to a 2003 NUMMI press release, the joint venture boasted its highest production ever – 369,856 vehicles – in 2002. President Kanji Ishii noted that “it was a record-breaking year despite three major model launches and a port lockout” (NUMMI Press Release, 2003). While it is certainly impressive that they automaker was able to make up the production loss, they incurred significant expense in doing so. While NUMMI did not disclose their financial losses due to the port lockout, the additional shipping costs, costs of production downtime, and overtime costs once the plant reopened, are estimated in the tens of millions of dollars.

---

### **5.2.5.5 Dow Corning Corp. – 03/20/03 – 2003 U.S.–Iraq War**

In the months leading up to the 2003 U.S.-Iraq war, logistics experts at Dow Corning Corp., the U.S. chemical conglomerate, was busy analyzing global supply chain for potential vulnerabilities to disruption. According to the Wall Street Journal, Dow makes over 10,000 deliveries per month to 20,000 customers in 50 countries and depends on a supply base that is just as diverse and far-flung. As the slightest glitch can disrupt the company's complex and streamlined supply chain, Dow understands that "elaborate emergency plans have become an operational necessity (Kahn, 2003). So when the first shots were fired on March 20, 2003, Dow Corning was ready. In the case of the U.S.-Iraq conflict, the Suez Canal was determined to be the likely bottleneck and the biggest potential headache for Dow. In one case, supplies were shipped from Belgium to a finishing plant in Shanghai 12 days early to allow routing around the Cape of Good Hope instead of through the canal. As a general precaution, extra shipping containers were also arranged at ports along the U.S. East Coast to prevent delays in the event of a sudden shortage. Additional inventory was also placed at key storage areas at Dow facilities across the globe to provide insulation from shipping delays.

Dow's team of schedulers and planners began meeting to discuss the potential logistics impact of a prolonged conflict with Iraq months before the threat of war became imminent, and started implementing countermeasures two months before the first shots were fired. Once the conflict began, this proactive approach allowed the team to spend much of their time checking assumptions and updating operating plans based on the rapidly changing global conditions. One condition that the team was especially sensitive to pertained to the potential strain on global shipping that the U.S. military could create by absorbing capacity to re-supply troops in the Middle East; a lesson learned during the 1991 Persian Gulf War. So many commercial container ships were diverted to the Middle East that tracking shipments became difficult and guaranteeing delivery at the proper destination became nearly impossible.

While Dow concedes that advances in information technology have made them much better prepared to deal with the situation this time around, customers have also become much more demanding and less tolerant of delays, regardless of the cause, because their own lean operating strategies have made them all the more dependent on timely deliveries. It is clear that Dow understands the *Efficiency-Resiliency* tradeoff that faces most companies operating today, and are proactive in their efforts to restore the proper balance to their own supply chain operations.

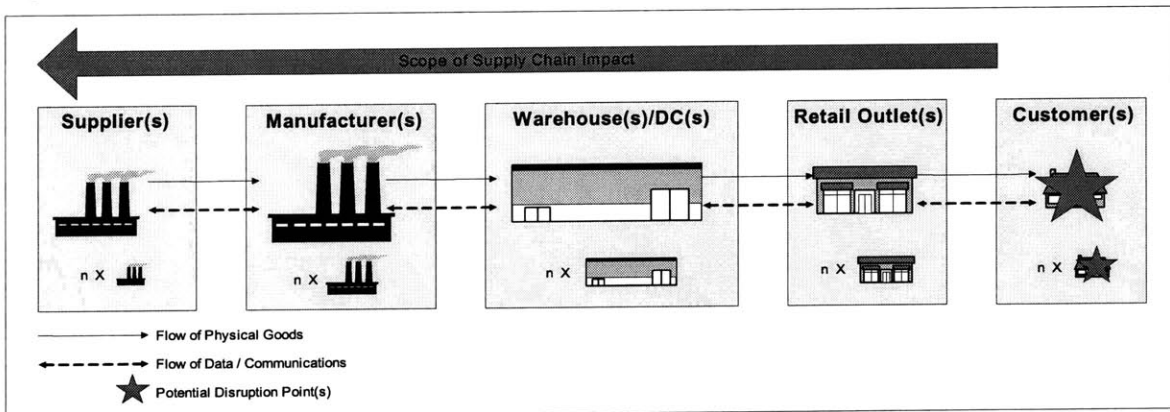
---

---

## 5.2.6 Demand Disruption

And even if firm's ability to manufacture and distribute its products suffers no direct or indirect impact from a disruptive event, it still must rely on its customers' ability to receive and pay for those products. In this scenario, one or more key customers were indeed impacted. This often results in a ripple effect that reaches far back into the supply chain. Figure 34.0 below describes the impact of such a disruption on the flow of physical goods and/or information throughout the generic supply network. In addition, two cases – GHSP and Cantor Fitzgerald – are outlined below to provide accounts of how this type of failure mode can occur, what it means for a firm, and how three such firms responded.

**Figure 34.0 – Potential Impact of Demand Disruption**



### 5.2.6.1 GHSP – 09/11/01 – Terrorist Attack

Founded in 1924 and headquartered in Grand Haven, Michigan, GHSP (formerly known as Grand Haven Stamping Products) is a leading Tier-1 supplier of mechanical and electro-mechanical assemblies to the automotive industry. A vast majority of its business comes from designing and manufacturing floor-mounted shifting mechanisms for large OEMs like Daimler-Chrysler, Ford, GM, Honda, Toyota, and Nissan.

When North American border traffic was ground to a halt following the terrorist attacks on September 11, 2001, several critical parts shipments bound for several Ford manufacturing plants were stopped cold trying to enter the United States from Canada. When Ford's lean Just-In-Time inventory of these critical parts was exhausted, the company was forced to temporarily close six assembly lines, halting production on popular models like the Ford Thunderbird. According to Ericson's 2001 article, the disruption quickly rippled through Ford's supply chain,

---

“creating a chain-reaction train wreck among a host of suppliers who also operate on a zero-inventory basis” (Ericson, 2001). Because Ford no longer accepts any parts deliveries when a line is down, even those suppliers not directly impacted by the event were profoundly affected. Although GHSP delivers by local truck routes, Ford would not accept delivery of its products until shipments from its Mexico and Canada-based suppliers could get through and the assembly line(s) could be re-started.

Well into October, 2001, floor shifters for the new Ford Thunderbirds remained stacked up on GHSP’s shop floor. When Ford shut down, the shifters that they were scheduled to ship that day just got put off to the side, taking up precious floor space. There was not much that they could do except to notify its own suppliers, as Ford would not take delivery. Most of their customers will notify GHSP to inform them to hold shipments when disruptions occur, but that is not always the case. Their large OEM customers exert the power in the supply chain and the various Tier-1 and Tier-2 suppliers must be flexible enough to react accordingly. “Jeffrey McCauley, Manager of Information Systems at GHSP, also points out that it doesn’t take as much as a terrorist attack to knock Ford offline. GHSP recently waited for weeks for a fix to a cooling fan fault by another supplier that had idled a Ford assembly line. Since GHSP operates three plants for various customers, the best it can do is re-allocate resources while the supply chain gets back in order” (Ericson, 2001). In the modern JIT-based extended supply chain, prevalent in technology-intensive industries like automotive and consumer electronics, a disruption for one is a disruption for all.

#### **5.2.6.2 Cantor Fitzgerald – 09/11/01 – Terrorist Attack**

When terrorist attacks brought about the collapse of New York City’s World Trade Center on September 11<sup>th</sup>, the many financial services firms that called the twin towers home suffered numerous casualties and massive property damage. Cantor Fitzgerald, a leading U.S. Treasury bond broker, was the hardest hit of them all. In total, the firm lost 680 of its 1,000 New York-based employees; every one of Cantor’s traders in the international, Nasdaq, and program trading groups died. The firm was however, left with 1,450 employees, including several key players in the firm's large London office and a cadre of New York staff who survived. To mobilize resources and prepare the firm for a recovery, Howard Lutnick, Cantor’s long-time CEO, closed offices in Paris and Frankfurt, and transferred staff to London. Said Lutnick in a 2001 New York Metro News article, "We played with the cards the terrorists left us" (Gordon,

---

---

2001). But most importantly, and to the awe of Wall Street and most government regulators, they were able to restore their U.S. eSpeed operations – a crucial link in the Treasury markets – within two days after the attack. Against all odds, the firm was mounting a comeback.

Cantor Fitzgerald's primary business was trading United States treasury bonds and provided a critical service to many large banks and insurance companies. That service was anonymity. It provided financial institutions with the ability to execute large trades without letting competing firms know what they were up to. The following example was presented by Shawn Tully in a 2001 Fortune article: "When a bank asks Merrill Lynch to unload \$1 billion of Treasury bonds, Merrill uses Cantor to break the order into pieces. That keeps other customers or dealers, like Salomon, from knowing that a big block of bonds is hitting the market. If Merrill called Salomon directly, Salomon might dump its own bonds first, pushing down the price when Merrill sold. Cantor dominates the business because it serves so many clients; it can quickly find buyers, at low cost, for even \$3 billion sell orders. It's practically an exchange itself: The world's bond traders use Cantor's quotes to establish the price of Treasuries. And investors use Cantor's screen to make sure dealers aren't ripping them off" (Tully, 2001).

With many billions of dollars at stake on any given trade, the relationship between a customer and his broker was historically very important. In fact, Cantor Fitzgerald had built its business on the ability of its brokers to build and sustain such relationships with its customers, especially the large institutional investors that literally moved the markets on a daily basis. In Mark Kahn's 2001 NetRisk.com article, they were characterized as a "20<sup>th</sup> century equivalent of the craftsman of Old England – and its workforce, composed of family and friends, mimicked that of any guild. While [their] brokers were employed in a brokerage "factory," each developed a relationship with his or her accounts based on his or her personality and ability to execute trades in the chaos of Cantor's trading rooms" (Kahn, 2001). In a business like Cantor's, the brokers and the personal relationships that they maintained with their customers were critical to the firm's ability to earn generate revenue. That said, the human loss that Cantor Fitzgerald suffered on the morning of September 11<sup>th</sup>, 2001, should, for all intents and purposes, have put the firm out of business. Due to several factors however, most the result of efforts made long before September 11<sup>th</sup>, Cantor has managed to defy the odds and remains a viable competitor in the global bond markets.

---

Cantor's greatest stroke of luck had been its recent transition away from the broker-based, high-touch relationship investing that it had built its business on and towards a more automated operating model. Throughout the 1990's, Cantor, like other brokerage firms, started to shift to an electronic platform for brokering – an internal electronic trading arm that the firm called eSpeed. Instead of a static computer screen and a direct phone line to a broker, a trader executed his or her trades directly from a computer keyboard without the assistance or advice of a personal broker. In 1999, the firm began offering its clients a discount to switch from traditional, over-the-phone broker-based trading to the eSpeed system. By September 10<sup>th</sup>, eSpeed accounted for 80% of the firm's bond business (Tully, 2001). While many, including Mark Kahn in his 2001 NetRisk.com article, argue that this transition runs exactly counter to Cantor's historical competitive advantage and could ultimately undo its leadership position, it is precisely what has allowed the firm, at least initially, to back from the destruction of its headquarters and the death of so many of its traders and support staff (Tully, 2001). Because the firm was able to restore its eSpeed operations so quickly – within just two days – they were able to serve its customers when the U.S. markets re-opened on September 17<sup>th</sup>. And because they had already successfully transitioned such a large proportion of its bond business (80%) to eSpeed, Cantor had a critical mass of initial transaction volume that could sustain them as they aggressively marketed their online services to their broker-based clients in an attempt to woo them back or keep them from taking business elsewhere. It is important to note, however, that the strength of their pre-September 11<sup>th</sup> broker relationships is playing a critical role in the recovery as well. According to Kahn, “the anecdotal stories told in various articles and heard on trading floors argue that Cantor might just survive based on the personal relationships its clients had with those same brokers that Cantor was trying to eliminate. Traders, out of a loyalty to their deceased brokers/friends and their families want to see Cantor survive” (Kahn, 2001).

The Cantor Fitzgerald case provides an interesting perspective on the devastating impact that a demand-side supply chain disruption can have. While Cantor certainly had many obstacles to overcome in term of general property damage, destruction of IT assets/infrastructure assets, and loss of life, it is the disruption of the communication links between the firm and its customers that this was focused on here. The lesson is twofold. First, relying completely on personal relationships for recurring sales can be hazardous to a firm's health in the event of a disaster like September 11<sup>th</sup>. Had Cantor not begun the transition to an online trading platform prior to the attack, they firm would most likely not have been able to mount a comeback. This does not

---

---

mean however, that a firm should rely completely on technology. For some commodity industries, this may make sense. But for a financial services firm like Cantor Fitzgerald, personal relationships between a company and its customers can be very important. Without both of these elements working in their favor, Cantor Fitzgerald would not be in business today.



---

## Chapter 6: Supply Chain Resilience Strategies

### 6.1 General Observations and Conclusions

A primary theme of this thesis has been the importance of focusing not on the nature of any specific disruption, but on how business operations are likely to be generally impacted. That is to say, organizations should focus on the failure modes, not the failures themselves. Firms cannot foresee every potential threat, let alone the probability of it occurring at each point in a complex and rapidly expanding supply network. It simply isn't feasible, nor would it be practical. Fortunately, firms should not have to. As the numerous events and case studies discussed in Chapters 4 and 5 showed, a wide variety of disruptions tend to have very similar effects on a company's supply chain. Therefore, a single all-encompassing supply chain resilience strategy can be used to prepare for myriad future disruptions, whether natural or man-made. This was the first of two major insights made clear by the research data.

The second major insight pertains to how firms approach resilience or business continuity investments. When crafting an enterprise supply chain resilience strategy, it may be useful to frame investment decisions as a question of risk vs. reward, terms that are very familiar to most business managers. Using this framework, an organization would temper every risk management investment decision with the expected reward of mitigating that risk, much like hedging an investment portfolio. This ensures that managers take into account both sides of the risk-reward equation. It also grounds the process with a common framework that is familiar to most decision-makers, thus reducing the uncertainty and discomfort that topics like global terrorism, killer earthquakes, or devastating hurricanes may stir.

In addition to these two insights, ten recurring themes became evident throughout the analysis of the data presented in Chapters 4 and 5. These themes highlight lessons that companies like Toyota, Unilever, Dow, Nokia, and Daimler-Chrysler had to learn the hard way. Each theme is discussed in detail throughout the rest of Chapter 6.

---

## 6.2 Lessons Learned: 10 Steps to a More Resilient Supply Chain

### 6.2.1 Build a Resilient Culture!

One of the most effective ways to enhance overall resiliency is to build it into the culture of the organization. Just as quality or safety can be embedded into the cultural fabric, the notion of resiliency can be made integral to the identity of an organization in much the same way. By bringing resiliency to the forefront and aligning the organization to a common strategy, managers can dramatically improve their chances of overcoming disruptions, regardless of the root cause. This is the single most powerful tool to maximize supply chain resiliency and can pay enormous dividends over time. As shown in the Nokia Vs. Ericsson case, it can even be the edge that allows one firm to weather the same storm that forces ones of its largest competitors out of the market.

The first step in building a resilient culture is learning to be constantly watchful for potential disruptions. This notion pertains to security threats and supply chain anomalies in the same manner. Recall that it was Nokia's quick recognition of a blip in the supply of chips from Philips that allowed them to get a jump on Ericsson, capturing all excess supply capacity before Ericsson even realized there was a problem. Timely detection of the disruption is the first step to a successful recovery. And once a potential problem is detected, employees should be encouraged and rewarded for communicating bad news quickly. This notion of information velocity was a key success factor in several cases including Land Rover and Continental-Teves.

And once a disruption is detected, all parties in the supply chain must be notified to allow a holistic response, be it identifying alternate sources for a key component, as in Nokia Vs. Ericsson, stocking shelves with alternative product, or modifying promotional practices so that in the worst case, the company is not promoting what it does not have and in the best case, it is directing customers to the products that it does have, as in the Dell vs. Apple case. It is also important to understand that this type of open, holistic, and uninterrupted communication can have enormous collateral benefits as well. By breaking down the silos that tend to divide the functional nodes of a supply chain and encouraging open and free-flowing collaboration, enterprises will be much better positioned to operate as a globally-optimizing whole rather than a scattered array of locally-optimizing nodes.

---

### **6.2.2 Expect to Fail**

For many of the cases profiled in Chapter 5, a prudent and comprehensive disaster plan, more than anything else, made the difference between success and failure. For companies like the Merrill Lynch, Oklahoma Federal Employee Credit Union (FECU), the New York Board of Trade (NYBOT), and Nokia, operational disruptions are a foregone conclusion. In terms of disaster planning, the question was never whether or not a disruption would occur, but when. And it was exactly because these firms expected to fail that they were able to respond so well when disaster struck.

Recall that when terrorists brought down the twin towers of the World Trade Center on September 11<sup>th</sup>, 2001, Merrill Lynch suddenly found itself without its world headquarters. But general preparedness, sound contingency planning, and disciplined testing allowed the firm to absorb the shock and return to normal operations while barely skipping a beat. According to Paul Honey, Director of Global Contingency Planning, “the financial firm was able to successfully evacuate their headquarters and resume critical management functions within minutes of the terrorist attack”(Ballman, 2002). Almost immediately after the first plane struck, the company’s emergency management jumped into action and initiated the evacuation process. And “within just a few minutes of the evacuation, Merrill Lynch was able to switch its critical management functions to their command center in New Jersey, explained Honey. Since the command center had been pre-designated in corporate-wide contingency plans, all personnel immediately knew where to dial into and transfer information. This allowed transactions throughout the company’s global offices to continue as usual” (Ballman, 2002). There was never any question as to how the firm should respond, despite the tragic and horrific nature of the disruption. They simply executed the failure plan.

Merrill Lynch was successful because they planned appropriately and executed brilliantly. It cannot be stressed enough how important execution is in these situations. A sound recovery plan is useless if not implemented properly. For example, in Texas City, dockworkers and rescue personnel were ignorant to the danger of the situation and did not react appropriately. There was a plan in place at the time that called for dangerously burning ships to be towed from harbor, but that plan was not initiated until it was too late. The tugboat never arrived.

---

When crafting a plan, a firm should try to be as “destructively creative” as possible when brainstorming potential disaster scenarios. This means that they should consider the absolute worst-case. While the 1993 World Trade Center bombing and the Y2K scare motivated many New York City companies to invest in a sound disaster recovery strategy, most were not prepared for the breadth of the September 11<sup>th</sup> disaster. For example, when telecommunications networks were suddenly crippled, a spike in mobile telephone traffic from concerned loved ones coincided with the loss of a major telephone-switching station operated by Verizon. Communication via these networks was significantly compromised. Most plans assumed that a telecommunications infrastructure would be available to facilitate the execution of the recovery plan.

On the same day, many firms also realized the folly of locating their backup data far from their central operating locations. Having an alternate site with the backup data that is far enough away to not be affected by the disaster is critical. However, some of the organizations affected by the collapse of the twin towers had their backup data stored hundreds of miles away. Unfortunately, the massive transportation problems following the attacks prevented the data from being physically transported to where it could be put to use in a timely way. When air traffic was halted in the days following the disaster, back-up data tapes and other equipment had to be shipped via ground transportation, severely slowing the IT recovery process. Conversely, several firms that had back-up locations in another building in the World Trade Center complex realized the folly in locating sites too close together. Both primary and secondary sites were destroyed (Wright, 2002).

While the process of disaster planning can be cumbersome and time-consuming, the payoff will more than justify the expense when disaster strikes. And as every resilient enterprise knows, disaster will strike. The question is not if, but when. As Merrill Lynch, NYBOT, and Nokia will attest to, planning to fail is a winning strategy.

### **6.2.3 Centralize at your Own Risk**

To reduce organizational complexity and achieve economies of scale, many firms have pursued a strategy of asset centralization when designing and building out their supply chains. While this practice often does lead to lower total costs, it also exposes the enterprise to a significant amount of risk. For example, if a firm operates only one production facility and that facility is rendered

---

inoperable by any number of potentially disruptive events, the firm suddenly loses all ability to manufacture its products. In some highly competitive industries, a disruption of this nature could put a company out of business. On the other hand, if that same firm operated out of multiple facilities, or even maintained some sort of contingency relationship with a contract manufacturer, production volumes at the alternate location(s) could be ramped up to balance the load until the damaged facility could be brought back online.

This notion of “centralization risk” is prevalent in many of the case studies presented in Chapter 5. Unilever experienced first-hand how risky it can be to operate out of a single manufacturing location when Hurricane Mitch destroyed their Q-Tip plant in Puerto Rico. The idea also applies to sourcing and procurement. In both the Land Rover and Avon Rubber cases for example, several firms learned a painful lesson in the dangers of “putting all of their eggs in one basket” by sourcing critical parts from a single supplier. While centralizing assets and consolidating procurement contracts often makes perfect economic sense, these decisions must be made with a full understanding of the risks involved. This means that firms should always temper the cost savings from centralization with the estimated impact and recovery expense of a major disruption. It is interesting to note that after the September 11<sup>th</sup> terrorist attacks, several New York City firms are doing just that and de-centralizing their operations so that losing one office building or one factory will not cause an interruption in their service to their customers. A 2002 Insurance Day article lists the following organizations as moving towards a more de-centralized logistics strategy by re-locating operations that were originally centralized at the World Trade Center:

- Morgan Stanley plans to move 2,000 of 16,000 employees to Westchester County.
- Goldman Sachs is moving equity trading to the New Jersey waterfront.
- Marsch & McLennan is relocating 1,100 employees to Hoboken, New Jersey.

While it may often be difficult to derive the optimal balance between a centralized and de-centralized logistics strategy, the most important thing for organizations to remember is that there is now an important tradeoff between cost and risk that must be included in the analysis.

---

#### **6.2.4 Understand the Risks Inherent to Sole-Sourcing**

As discussed in the previous section, the notion of “centralization risk” also applies to sourcing. While single-sourcing components can be advantageous in many circumstances, it also introduces a significant level of operational risk. Suppliers can go out of business, lose key employees, or get acquired by another company – all very dangerous situations if that supplier provides one or more key components that can bring production to a screeching halt if supply is interrupted. In the situations where it does indeed makes sense for a firm to sole-source a key component, contingency planning can be used to hedge its risk. A comprehensive supplier risk management plan will require that a firm:

- 1. Identify all critical suppliers or service providers (carriers, contract mfrs., etc.)**
- 2. Estimate the probability/frequency of a business failure or supply disruption**
  - Formal data collection: published financial data, SEC filings, etc.
  - Informal data collection: own contacts with the company, frequent re-organizations?, etc.
- 3. Estimate the potential impact of a supply disruption**
- 4. Evaluate current business relationship with supplier**
  - Are you making it difficult for the supplier to stay in business?
  - Review the contract for disruption clauses, etc.
- 5. Monitor all critical suppliers on a regular basis**
- 6. Contract with back-up suppliers to hedge risk where feasible and practical**
  - Compensate via either retainer fees or a minority percentage of regular volume
  - Arrange for spikes in supply volumes in the event of disruption in primary supply
  - Ensure that all operating links are in place to facilitate a rapid change-over if needed

Land Rover, Ericsson, and Avon’s ill-fated OEM customer all learned painful lessons in the dangers of consolidating supply to a single source. In all cases, significant supply crises arose not only because these companies sole-source critical components, but also because they lacked the visibility into their supplier’s operations that may have allowed them to anticipate the both the impact and the likelihood of such a disruption and develop an appropriate response plan before they needed it. They simply were not prepared. It is also important to note that the contingency planning process outlined in the six steps above can, and should, also be used to evaluate sole-source relationships that may exist with transportation providers, contract manufacturers, or other 3<sup>rd</sup>-party service providers.

---

### **6.2.5 Know your Supply Chain!**

While the importance of keeping a watchful eye on key suppliers was discussed in the previous section, this idea also applies to other partners in the supply chain. It is not enough to ensure that proper risk management strategies are implemented at your firm, you must also ensure that your suppliers and partners are resilient. Enterprises should become intimately familiar with both the capabilities and vulnerabilities of their partners. According to Chase Kushak, Senior Supply Chain Product Manager at Covisint, “business processes and physical supply chains are different elements that have to work in concert. Building plants right next to your supply base would be a bit of a knee jerk. Just because your tier-one supplier is next to you, he still may be sourcing parts from Mexico. The bottleneck just moves” (Ericson, 2001).

In Chapter 5, Nokia, Ericsson, Land-Rover, and Toyota all learned first-hand how vulnerable their operations really were to disruptions suffered by supply partners. In each case, the situation could have been prevented by proactively working with partners to understand their respective risk profiles and implement contingency measures to protect themselves. While this certainly assumes a high level of cooperation and trust between supply chain partners, that is what is necessary to achieve true supply chain resiliency. For enterprises can no longer afford to keep their proverbial heads in the sand, depending solely on negotiated supply contracts and blind optimism.

### **6.2.6 Hedge Disruption Risk with Inventory Buffers**

Inventory buffers, or safety stocks, can be a very effective tool for firms to use as a hedge for various disruption risks. Extra inventory held at strategic locations throughout the supply chain can dramatically improve a company’s ability to weather events like supply shortages or a sudden decrease in manufacturing capacity for instance. It basically provides a safety net that will ensure that the supply chain can continue to function in the event that one of its critical nodes is somehow impaired.

Examples of using inventory buffers as a risk management tool can be found in several of the cases discussed in Chapter 5. When Unilever chose to continue to centralize manufacturing at a single facility even after that facility was destroyed by Hurricane Mitch, they increased inventory levels across their North American supply chain by 10%. This step was taken to reduce their exposure to manufacturing disruption risk should disaster strike twice. So while the

---

---

perceived risk did not drive them to de-centralize manufacturing, it did enter the logistics analysis and drove them to take other steps to mitigate that risk. Another example can be found in Dow Corning's preparations for the 2003 U.S.-Iraq War. When the threat of war became imminent, Dow's logistics managers placed additional inventory at key storage areas at Dow facilities across the globe to provide insulation from potential shipping delays.

Martha & Vratimos (2002) estimate that Just-In-Time (JIT) techniques have saved the auto industry more than \$1B a year in inventory carrying costs alone over the past decade. While this thesis certainly does not suggest a full retreat from JIT manufacturing and logistics principles, it does recommend that the tradeoff between the cost of downtime or stock-outs and the cost of carrying excess inventory be re-visited and analyzed in the context of the myriad supply chain disruption risks that enterprises now face on a daily basis. The challenge then is to strike the proper balance between Just-In-Time and Just-In-Case. This is certainly no trivial task as decades of inventory optimization theory must now be modified to account for this loosely-defined notion of disruption risk. And until the appropriate risk assessment techniques are developed and the requisite optimization algorithms are improved, this tradeoff will likely have to be managed with equal parts art and science. But just because a firm cannot quantify the risk does not mean that it can afford to ignore it. The planning tools will eventually evolve, but leading firms like Dow and Unilever are not waiting around. They recognize today's increasingly risky operating environment and are using inventory buffers to protect themselves.

#### **6.2.7 Develop Backup & Recovery Processes for All Data/IT Infrastructure...and Practice!**

According to Meta Group, "companies deprived of key computer systems for 10 days cannot recoup the financial damage, and 50% of them will go out of business within five years" (Meta, February, 2002). In the new information economy, technology is king. Information technology increasingly drives virtually every corporate function, from planning to manufacturing to sales. And in industries like financial services and e-commerce, technology is the lifeblood of the organization. If the computers go down, business ceases.

For this reason, it should not be a surprise to learn that in formation technology leads all other corporate functions, by far, in terms of business continuity and disaster recovery planning, information technology. After the Year 2000 (Y2K) frenzy and the 1993 and September 11<sup>th</sup> terrorist attacks, it is now common practice to have comprehensive back-up and recovery plans

---



---

in place for mission-critical corporate IT infrastructure. These are the plans that allowed Merrill Lynch, Cantor Fitzgerald, and Sidley Austin Brown & Wood (SABW), for example, to absorb and respond so brilliantly to the September 11<sup>th</sup> terrorist attacks. These firms had sound recovery strategies in place and were prepared to implement them when it came time to do so. And the best way to maximize preparedness, as all can attest to, is through testing.

For example, when a severe ice storm interrupted power at ING Property & Casualty's Saint-Hyacinthe data center, a well-tested recovery plan allowed them to stay in business without suffering any downtime whatsoever. As Rothstein (1998) observed in his review of the case, testing was absolutely critical. "While everyone pays that lip service, where it becomes very critical is in [disaster] situations like [the ice storm] where you build the relationship and rapport between the organizations so that when the disaster happens, the supplier can provide useful support. Exercising pays a lot of dividends" (Rothstein, 1998). Building strong relationships and rapport through mutual exercises is the best way to ensure suppliers can provide useful support when needed. Even the best IT recovery plan is useless if it cannot be implemented properly and in a timely manner.

Again, we see that planning and execution are equally critical when responding to a disruptive event. And one of the best ways to ensure proper execution when the time comes is through comprehensive testing. As painful as testing can be for an organization, it is nothing compared to the disastrous effects that prolonged downtime can have.

### **6.2.8 Implement Enterprise Standards**

Implementing an enterprise standard for hardware, software, and processes makes a lot of sense, especially in terms of disaster preparedness. If employees are all working on a standard computing platform, the process of backing up critical systems and restoring those systems after a disruptive event becomes much less painful. Enterprise standards also improve a firm's ability to re-configure their operations quickly and efficiently if needed. For example, it becomes much easier to transfer employees to alternate manufacturing locations in response to a disaster at a primary plant if all plants are running on the same Enterprise Resource Planning (ERP) system. Employees don't have to spend precious time trying to learn a system that they may not be familiar with. This concept also applies to business processes like procurement, payroll, or quality control.

---

For Compaq, a consolidated product data management platform allows them to quickly transition production from one plant to the other by ensuring that everyone is working off of a single product specifications package (bill of materials, design drawings, etc.). In a second example, when Dow Corning's team of planners and schedulers began meeting to determine the impact of the pending 2003 U.S.-Iraq war, it was crucial that all team members were conducting analyses and making decisions based on the same information. Because the company's entire delivery, warehousing, and transportation network is run by a single SAP AG software platform, this never became a problem. The process would have been very difficult, if not completely infeasible, if each factory ran its own ERP system. A company-wide software standard also facilitated SABW's recovery process following the destruction of their World Trade Center data center and office locations on September 11<sup>th</sup>, 2001. The entire system was recovered in a matter of days with the same operating environment and applications that were present on September 10<sup>th</sup>.

#### **6.2.9 A Flexible Supply Chain is a More Resilient Supply Chain**

Several of the cases presented in Chapter 5 also illustrate the benefits of a flexible supply chain. Once a disruption was detected, managers were able to quickly and effectively take corrective action within the supply chain to minimize the overall impact to operations. The first key to this is detection, which is made possible with supply chain visibility. Visibility is facilitated both by attentive and skilled employees and supply chain management tools. In the Nokia Vs. Ericsson case, Nokia's ability to quickly detect the supply disruption allowed them to capture all of Philips' alternate production capacity before Ericsson could, which put them in a much better competitive position. And once visibility is achieved, it is supply chain control that allows management to respond when disaster strikes. When a major earthquake disrupted the supply of computer chips for both Apple and Dell in 1999, superior supply chain control gave Dell the edge. Although their famously lean build-to-order operating strategy meant that they held only five days of inventory, their "sell-what-you-have" sales model allowed them to direct customers to products for which they could build with available components. The inherent nature of their

---

build-to-order system also prevented them from experiencing the same “hard-configuration” issues that hurt Apple. So in summary, when it comes to supply chain management:

**Visibility + Control = Resilience**

### **6.2.10 Insure Wisely**

As supply chains grow both in term of complexity and geography, it is crucial that firms subject their existing insurance policies to a periodic review. As the global operating environment evolves, risk profiles change and organizations can quickly become more or less vulnerable to disruption. As a supplement to the property and casualty insurance commonly used by firms to protect their assets from physical damage under a variety of circumstances, business continuity insurance can be used to protect a firm in the event that a disruption occurs because of an event outside the proverbial four walls of the company. While a firm may suffer no direct physical damage to its asset base, a disruption elsewhere in the extended supply chain – perhaps at a key supplier or contract manufacturer – could significantly impact operations. As one might expect, the terrorist attacks of September 11<sup>th</sup> highlighted the need for comprehensive insurance coverage. They also dramatically changed the face of an insurance industry that is still struggling to incorporate the “new threat” of terrorist attacks into policies available to companies operating on U.S. soil.

Before September 11<sup>th</sup>, “*all risk*” insurance was commonly used to insure policyholders against business interruption when unforeseen events – hurricanes, earthquakes, industrial accidents, terrorist attacks, etc. – disrupted either the inbound shipment of raw materials or the outbound shipment of finished goods. September 11<sup>th</sup>, however, introduced a new sense of magnitude to the potential loss calculations used by insurance companies to derive appropriate policy premiums. It also introduced a new sense of uncertainty regarding the likelihood of future attacks; the historical data commonly used to predict the future simply doesn’t exist yet. The major insurance providers have generally responded by stripping acts of terrorism from *all-risk* policies, just as acts of war are commonly excluded. In November 2002, the U.S. government passed legislation requiring major insurance companies to offer some form of terrorism insurance to its business customers.

Terrorism insurance is now offered as a separate policy with much higher premiums derived

using geographic location as the primary indicator of risk, or the probability of suffering damage due to a future terrorist attack. Risk modelers have concluded that, despite terrorist organizations like al Qaeda’s fluid nature, high-profile cities like New York and Washington D.C. are more likely than others to be struck, which means companies in those areas should pay times more for coverage. In fact, Newark-based Risk Management Solutions Inc. estimates that only 2% of U.S. Zip Codes face more than 90% of the risk (Brady, 2003). Applying this thinking, AIR Worldwide Corp., a subsidiary of Insurance Services Office Inc. (ISO) – the company that sets rate guidelines for the industry – has helped ISO establish three tiers of risk. As Figure 35.0 illustrates, the price points at each tier vary dramatically.

**Figure 35.0 – Recommended 3-Tier Cost Structure of Terror Insurance**

<b>The Price of Risk</b>		
Recommended cost of terror insurance* in city centers per \$100,000 of coverage		
<b>TIER 1</b> New York, Chicago, Washington D.C., San Francisco <b>\$30</b>	<b>TIER 2</b> Houston, Seattle, Los Angeles, Philadelphia, Boston <b>\$18</b>	<b>TIER 3</b> Rest of the Country <b>\$1</b>
<small>* Annual charge based on estimated cost of losses, excluding insurers' costs or added            Data: Insurance Services Office, Inc.</small>		
<small>Source: Brady, 2003</small>		

As of April 2003, most companies are declining such insurance; either because they deem it unnecessary, others because it’s too expensive. “Insurers say that some companies are simply counting on the government to bail them out if another attack occurs” (Brady, 2003). While there was a slight spike in firms seeking supplemental terrorism coverage in the days leading up to the U.S.-Iraq war, the data still indicates that the overwhelming response has been negative; the extra costs remain far too high in proportion to the perceived risk for most companies.

For those companies that do choose to purchase supplemental terrorism coverage, it is crucial that they review the policy terms in detail and understand precisely the terms of the contract, as most insurers offer only coverage specifically mandated by the government’s terrorism-coverage bill. For example, federal coverage is limited only to terrorism perpetrated by foreign perpetrators or groups. While this obviously leaves policyholders vulnerable to domestic terrorism, it also introduces some uncertainty in the event that the government might not be able to determine the nationality of a terrorist killed in an attack. In response, several insurers –

---

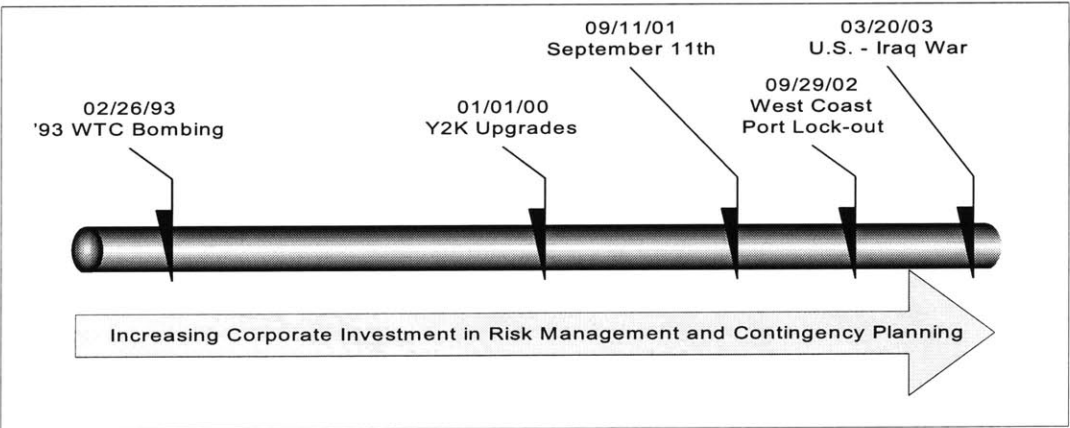
including Ace, American Insurance Group Inc., and Lloyd's of London – offer coverage that includes acts of domestic terrorism as well (Oster, 2003).

For those firms that were fortunate enough to have some form of business continuity insurance in place prior to September 11<sup>th</sup>, many found their coverage was inadequate. This coverage typically is triggered only if there is physical damage to a company's property. As widely discussed, many businesses were shut down or lost money not because their properties were damaged, but because air traffic was grounded, closing some airports for several days and canceling moneymaking events like conventions and trade shows. Most of those companies took learned this lesson the hard way and have since purchased broader business interruption insurance policies that provide coverage beyond direct physical damage (Oster, 2003).

**6.3 Summary of Lessons Learned**

Terrorist attacks, natural disasters, political upheaval, and industrial accidents are nothing new – most as old as commerce itself. But events like the Year 2000 (Y2K) computer upgrade frenzy, the 9/11 terrorist attacks, and even the West Coast port lock-out in the summer of 2002 have brought the risks to the forefront of global consciousness. As described in Figure 36.0 below, the rate of corporate investment in risk management and business continuity planning has increased with the relative frequency of these significantly disruptive events.

**Figure 36.0 – Milestones for Corporate Awareness of Supply Chain Vulnerabilities**



---

It is not that disruptive events are necessarily occurring with any greater frequency or magnitude, but that enterprises now find themselves increasingly vulnerable to their effects. For the past two decades, there have been two major trends at work – Just-in-Time (JIT) manufacturing and rapid globalization – that have led to this new reality. Organizations must now take decisive action to address these new vulnerabilities and improve general supply chain resiliency. The goal of this thesis project was to identify steps that firms can take to do just that. By studying a wide range of past disruptions, several significant insights were gleaned.

***Primary Insights:***

- Organizations should focus on the failure modes, not the failures themselves. Firms cannot foresee every potential threat, let alone the probability of it occurring at each point in a complex and rapidly expanding supply network. It simply isn't feasible, nor would it be practical. A single all-encompassing supply chain resilience strategy can be used to prepare for myriad future disruptions, whether natural or man-made.
  
- When crafting an enterprise supply chain resilience strategy, it may be useful to frame investment decisions as a question of risk vs. reward, terms that are very familiar to most business managers. This ensures that managers take into account both sides of the risk-reward equation. It also grounds the process with a common framework that is familiar to most decision-makers, thus reducing the uncertainty and discomfort that topics like global terrorism, killer earthquakes, or devastating hurricanes may stir.

***Lessons Learned:***

- 6.2.1 Build a Resilient Culture!
- 6.2.2 Expect to Fail
- 6.2.3 Centralize at your Own Risk
- 6.2.4 Understand the Risks Inherent to Sole-Sourcing
- 6.2.5 Know your Supply Chain!
- 6.2.6 Hedge Disruption Risk with Inventory Buffers
- 6.2.7 Develop Backup & Recovery Processes for All Data/IT Infrastructure...and Practice!
- 6.2.8 Implement Enterprise Standards
- 6.2.9 A Flexible Supply Chain is a More Resilient Supply Chain
- 6.2.10 Insure Wisely

---

#### **6.4 Opportunities for Further Study**

While significant research has been initiated on the subject of supply chain resiliency and disaster recovery, there is still much to be done. Much of the data collected at this point, including the contents of this thesis, covers only a small subset of potentially available data. It would be useful to somehow capture a larger sample size, which would allow more statistically significant results. There is also much work to be done in the field of risk assessment and the derivation of appropriate inventory levels for various levels of hedging. This pertains to Section 6.2.6 where the notion of using inventory buffers as a hedge for disruption risk was discussed. Traditional inventory optimization algorithms should be modified to account for variable levels of disruption risk. This would allow firms to craft inventory policies that incorporate a specified level of risk that the firm is comfortable taking on. This would be similar to how the risk of stocking out is incorporated into most traditional inventory models. Another subject that warrants additional study is that of collateral benefits of supply chain resiliency and/or security investments. Many firms underestimate the probability of a major disruption impacting their operations. For these firms, it may be difficult to persuade management to make the appropriate investments unless alternative benefits, such as decreased lead times or increased service levels, can be identified.

Finally, the likelihood of future government mandates would be a useful area for many companies to understand, particularly those in critical infrastructure industries or those representing especially attractive targets for terrorist attacks. It remains uncertain as to what role the U.S. government will eventually play in motivating organizations to address known vulnerabilities, but the trend is certainly beginning to take shape. As described in the Wall Street Journal (Schlesinger, 2003), the “Chemical Facilities Security Act” will impose a \$250,000 fine, and possibly an additional \$50,000 per day, on any chemical production facility that is found to be too relaxed in protecting itself against a terrorist attack. The bill would also permit the Department of Homeland Security to sue any chemical plant and request a court order to close the facility until the security threat is appropriately addressed. According the current draft of the bill, all chemical plants would be required to draft a comprehensive security plan. While it is still somewhat unclear as to how such legislation will be policed, it shows that both Democratic and Republican lawmakers are willing to use government mandate to force the U.S. chemical industry to close perceived security gaps, as opposed to leaving the issue for industry to address on a voluntary basis. “This is a trend that is expected to continue for those commercial sectors

---

---

deemed strategically important and/or likely targets of terrorist attack – power generation, telecommunications infrastructure, oil refineries, etc.” (Schlesinger, 2003).

## **6.5 General Conclusions**

One of the things that this thesis hopes to make is that the world is becoming a much riskier place for modern supply chain managers. Terrorist attacks, natural disasters, political upheaval, and industrial accidents are disrupting operations on an unprecedented scale and frequency. Trends like lean/JIT manufacturing and rapid globalization have exposed supply chains to myriad new risks and rendered them highly susceptible to many types of disruptive events. What this thesis also hopes to make clear is that no supply chain strategy can eliminate all of these risks. And even if it could, it would be far too expensive for any firm to implement. Organizations should instead focus on the general failure modes, rather than the failures themselves. This approach allows for a single all-encompassing supply chain resilience strategy that can be used to prepare for myriad future disruptions, whether natural or man-made.

The subject of insurance was also discussed in considerable detail. While the insurance industry wrestles with the new problem of quantifying many of these new disruption risks, especially those related to terrorist attacks, one thing is clear. Enterprises simply cannot rely on insurance alone to protect themselves. In many cases, coverage may prove to be prohibitively expensive or it may not be available at all. This makes the use of operational supply chain resilience strategies all the more important.

Outside of insurance, there is much that the modern supply chain manager can do to mitigate his or her organization’s exposure to disruption risk. The key lies in acquiring the awareness and the capability to detect, quantify, and prepare for future disruptions. This leads to the various resilience lessons outlined in Section 6.2. By identifying these lessons and presenting them here, the goal is to provide managers with a body of work that enables them to learn from the collective experiences of the firms profiled, and apply these lessons without first having to endure the painful learning process. In other words, there is much to learn much from the past that can help many firms prepare for the uncertain future. Because, as so appropriately stated by American philosopher George Santayana, “those who cannot remember the past are condemned to repeat it.”



---

## References

### General

- Cuneo, E. (2003, April). Safe At Sea. InformationWeek.com.  
<http://www.informationweek.com/story/IWK20030606S0001>.
- Firms spread offices over several states and NY city. (2002, March 6). Insurance Day. Informa Publishing Group Ltd.
- Helferich, O. & Cook, R. (2002). Securing the Supply Chain. Council of Logistics Management Research Report.
- Lensing, R. (2003). Historical Events and Supply Chain Disruption: Chemical, Biological, Radiological and Cyber Events. (Masters Thesis, Massachusetts Institute of Technology, 2003).
- Martha, J. & Subbakrishna, S. (2002, September 1). Targeting a Just-in-Case Strategy for the Next Inevitable Disaster. Supply Chain Management Review.
- Martha J. & Vratimos E. (2002). Creating a Just-in-Case Supply Chain for the Inevitable Next Disaster. Viewpoint Magazine, no.2. Marsh & McLennan Companies, Inc.
- McCarthy, A. (1993). No Plan, No Site, No Business. Disaster Recovery Journal, v.12, no. 2.  
[http://www.drj.com/special/wtc/w2\\_033.htm](http://www.drj.com/special/wtc/w2_033.htm).
- Perkins, B. (2002, December 9). Develop a Supplier Contingency Plan. Computerworld.com.  
<http://www.computerworld.com/printthis/2002/0,4814,76489,00.html>.
- Sheffi, Y. (2001). Supply Chain Management under the Threat of International Terrorism. International Journal of Logistics Management, v.12, no. 2
- Wright, H. (2002, March 18). Disaster Recovery Lessons Learnt. NZ Infotech Weekly (Wellington).

### 1999 Taiwan Earthquake

- An EQE Briefing: Chi-Chi, Taiwan Earthquake of September 21, 1999. (2000). EQE International, Inc. <http://www.eqe.com/revamp/taipei/pdf/taiwan.pdf>
- Chi-chi (Taiwan) Earthquake Information Website (Retrieved 2003, January 30)  
<http://www2.rcep.dpri.kyoto-u.ac.jp/~sato/taiwan/>.
- Weiman, D. (2000). Event Report: Chi-Chi, Taiwan Earthquake. Risk Management Solutions, Inc. (RMS). [http://www.rms.com/Publications/Taiwan\\_Event.pdf](http://www.rms.com/Publications/Taiwan_Event.pdf).

---

## **1995 Kobe Earthquake**

Arnold, R. (Retrieved 2003, January 15). Special Report: The Kobe Quake. Disaster Recovery Journal Online. <http://www.drj.com/special/quake95.html>.

Geography Resources for Teachers and Students Website (Retrieved 2003, January 15).  
<http://www.zephyrus.demon.co.uk/education/geog/tectonics/kobe.html>.

Kobe Earthquake Summary Website (Retrieved 2003, January 25).  
<http://www.cowswithfluff.freeserve.co.uk/meg/impacts.htm>.

BBC News Website: Full Coverage of the Taiwan Earthquake (Retrieved 2003, January 25).  
<http://news.bbc.co.uk/1/hi/world/asia-pacific/453441.stm>.

## **Hurricane Andrew**

Disasters of the Last Decade Website (Retrieved 2003, February 11).  
[http://long.linux-dude.net/~cyrille/disaster/main.php?menu\\_choice=6](http://long.linux-dude.net/~cyrille/disaster/main.php?menu_choice=6).

National Weather Service Website (Retrieved 2003, February 10).  
<http://www.ns.ec.gc.ca/weather/hurricane/storm92.html#andrew>.

## **Hurricane Mitch**

Mitch: The Deadliest Atlantic Hurricane Since 1780 (2002, December 20). National Climatic Data Center Website. <http://lwf.ncdc.noaa.gov/oa/reports/mitch/mitch.html>.

National Weather Service Website (Retrieved 2003, February 10)  
<http://www.ns.ec.gc.ca/weather/hurricane/storm98.html#mitch>

## **1998 Quebec Ice Storm**

1998 Ice Storm Homepage. (Accessed 2003, December 26).  
<http://hometown.aol.com/badice98/icestorm.html>.

Bueckert, D. (1998, December 15). Ice Storm Damage Tallied. Associated Press/CNews.com.  
<http://www.canoe.ca/CNEWSIceStorm/home.html>.

The Ice Storm (1999). CBC Newsworld.ca. <http://www.newsworld.cbc.ca/flashback/1998/>.

Verglas Montreal Ice Storm 98 Website. (Accessed 2003, January 10).  
<http://www.imiuru.com/icestormdiary/icestormtext.html>.

---

## **1993 Mississippi River Flood**

- McConnell, D. (1998). Mississippi River Flood: 1993. (Course notes, University of Akron, 1998).  
[http://enterprise.cc.uakron.edu/geology/natscigeo/Lectures/streams/Miss\\_Flood.pdf](http://enterprise.cc.uakron.edu/geology/natscigeo/Lectures/streams/Miss_Flood.pdf)
- Ramsey, M. (2002). Case Study – 1993 Mississippi Flood (Course notes, University of Pittsburgh, 2002). <http://ivis.eps.pitt.edu/courses/hazards/lectures/11b.pdf>
- The Mississippi River Flood of 1993. Weather.com (The Weather Channel) Storm Encyclopedia (2003). <http://www.weather.com/encyclopedia/flood/miss93.html>

## **2002 Central European Floods**

- Central Europe Flooding, August 2002 (Event Report). (2003). Risk Management Solutions.
- Chemical Leaks Threaten Prague as Floods Hit Dresden. (2002, August 15). The Guardian.  
<http://www.guardian.co.uk/Print/0,3858,4482032,00.html>
- Green, P. & Pohl, O. (2002, August 15). Floods Rise in Dresden; Czechs Deal With Chemical Threat. The New York Times. <http://www.mindfully.org/Water/Chlorine-Dresden-Floods15aug02.htm>
- Hanna, M. (2002, August 8). Prague Cleans Up as Threat Continues. CNN.com.  
<http://www.cnn.com/2002/WORLD/europe/08/16/czech.floods/index.html>
- Toothill, J. (2003). Central European Flooding – August 2002 (An EQE Technical Report). ABS Consulting. [http://www.absconsulting.com/eqecat%20flood/flood\\_rept.pdf](http://www.absconsulting.com/eqecat%20flood/flood_rept.pdf)

## **2002 Seven Building Flood**

- Bernard, J. (2003, February 10). The Value of Business Continuity Management. The Business Continuity Institute Website. <http://www.thebci.org/BCAWCS15.htm>

## **Philips Plant Fire: Nokia Vs. Ericsson**

- Latour, A. (2001, January 29). Trial by Fire: A Blaze in Albuquerque Sets Off Major Crisis For Cell-Phone Giants. Wall Street Journal, p. A1.

## **Avon Injected Rubber & Plastics Plant Fire**

- Avon Rubber – Devastated! (2001). MJ Mechanical Services: A Company Case Study.  
<http://www.mjmechanical.com/work>

---

### **Aisin Seiki Co. (Toyota P-Valve Supplier) Plant Fire**

Reitman, V. (1997, May 8). Toyota Motor Shows Its Mettle After Fire Destroys Parts Plant. *Wall Street Journal*, p. A1.

Wilding, R. (2002, January). All Together Now. *Continuity & Insurance Risk*. The Business Continuity Institute. <http://www.corporateinsurance-risk.com/FEATURES/Dec-Jan%2002/eps/42-43.pdf>

### **Halifax Port Explosion**

2002 HRM Tourism Culture and Heritage Website (Accessed 2003, February 20).  
<http://www.halifaxexplosion.org>

Maritime Museum of the Atlantic Website (Accessed 2003, February 13).  
<http://museum.gov.ns.ca/mma/AtoZ/HalExpl.html>.

Tourism/Metro Guide Website (Accessed 2003, February 20).  
<http://www.region.halifax.ns.ca/community/explode.html>

### **Texas City Disaster**

Stephens, H. (1997). *The Texas City Disaster, 1947*. Texas: University of Texas Press.  
<http://205.172.60.10/comm/virtual/readingroom/books/blast.htm>

The Texas City Disaster (2003). *The Handbook of Texas Online*.  
<http://www.tsha.utexas.edu/handbook/online/articles/view/TT/lyt1.html>

### **1993 World Trade Center Bombing**

Devlin, E. (1993, Spring). A Top Consultant Discusses the Bombing of the World Trade Center. *Disaster Recovery Journal*, v.6, no.2.  
[http://www.drj.com/special/wtc/w2\\_036.htm](http://www.drj.com/special/wtc/w2_036.htm)

### **1995 Oklahoma City Disaster**

Arnold, R. (1999, Fall). Special Report: Oklahoma City. *Disaster Recovery Journal*.  
[http://www.drj.com/special/wtc/w3\\_070.htm](http://www.drj.com/special/wtc/w3_070.htm)

---

## **September 11<sup>th</sup> Terrorist Attacks**

HowStuffWorks.com Website (Accessed 2003, January 15). September 11 Terrorist Attacks. <http://people.howstuffworks.com/sept-eleven4.htm>

U.S. Department of State (2002). Patterns of Global Terrorism: 2001. [www.state.gov/s/ct/rls/pgtrpt/2002/pdf](http://www.state.gov/s/ct/rls/pgtrpt/2002/pdf)

## **1997 UPS Strike**

Festa, P. (1997, August 15). Net Vendors Feel UPS Strike Pinch. CNET News.com. <http://news.com.com/2100-1017-202122.html?tag=bplst>

UPS strike: Talking but no talks (1997, August 13). CNN Online. <http://www.cnn.com/US/9708/13/ups.early/index.html>

Voorhis, V. (1997, August 8). UPS Strike Delivers Work to Area Couriers. Boston Business Journal. <http://boston.bizjournals.com/boston/stories/1997/08/11/story5.html>

## **1998 General Motors Strike**

Coon, K. (1999). The Ripple Effect of Union Strikes: A Case Study of the Micro and Macroeconomic Effects of the General Motors Strike of 1998. The Park Place Economist, v. VII, p. 33.

Nauss, D. (1998, June 18). GM, UAW amplify war of words. Los Angeles Times. Business Section, D3.

Other Companies (1998, October 23). The Washington Post, p. A1.

Turner, M. (1998, October 13). GM Press Release. <http://media.gm.com/corpcom/98news/g981013a.htm>

USX-U.S. Steel stock expected to rise – Business Week. (1998, October 22). Reuters-New York, Yahoo Finance. <http://biz.yahoo.com/rf/981023/s9.html>

## **2002 West Coast Port Lockout**

Japan Firms Start Airlifting Due to Port Closures. (2002, October 3). Automotive News. <http://www.autonews.com/news.cms?newsId=3522>

Larsen, M. (2002, October 14). Rush is on to beef up inventories. Sacramento Business Journal. <http://www.msnbc.com/news/821078.asp?0cb=-318111251>

---

National Retailers Prepare Backups in Case of Strike. (2002, July 9). Honolulu Star Bulletin.  
<http://starbulletin.com/2002/07/09/business/story2.html>

Schoen, J. (2002, October 7). Port Closures Will Hurt Holiday Sales. MSNBC.com.  
<http://www.msnbc.com/news/818319.asp?0cb=-818111251>

Wolk, M. (2002, October 8). Behind the West Coast Port Lockout. MSNBC.com.  
<http://www.msnbc.com/news/816688.asp?cp1=1>

### **Land Rover/UPF-Thompson Bankruptcy Case**

Rechtin, M. (2002, January 28). Discovery Production in Jeopardy. Automotive News Europe,  
p. 6.

Rechtin, M. (2002, February 11). Supplier Failure Hurts Land Rover. Automotive News Europe, p. 22.

Lester, T. (2002, April 1). Making it Safe to Rely on a Single Partner. Supply Chain Management Inside Track, p.7.

Duckers, J. (2002, February 12). Auto Supplier Failure a Source of Mutual Grief, Warns Recovery Expert. Birmingham Post, Business Section, p. 24.

Hoult, P. (2002, September 12). Land Rover's Rough Ride. Legal Week.

### **Oklahoma FECU Case**

Towler, G. (1999, Fall). A Survivor's Tale: The Rebirth of the Federal Employees Credit Union in Oklahoma City. Disaster Recovery Journal.  
[http://www.drj.com/special/wtc/w3\\_066a.htm](http://www.drj.com/special/wtc/w3_066a.htm)

### **New York Board of Trade Case**

Sliwa, C. (2001, September 24). New York Board of Trade Gets Back to Business. Computerworld Magazine.  
<http://www.computerworld.com/securitytopics/security/recovery/story/0,10801,64128,00.html>.

### **ING Property & Casualty Case**

Rothstein, P. (1998, March). A Chilling Experience. Information Security Magazine.  
<http://www.rothstein.com/articles/chilling.html>

---

### **Merrill Lynch Case**

Ballman, J. (2001, Summer). Merrill Lynch Resumes Business Critical Functions Within Minutes of Attack. *Disaster Recovery Journal*, v. 14, issue 4.  
<http://www.drj.com/special/wtc/1404-04.html>

### **Sidley Austin Brown & Wood, LLP Case**

Heath-Porter, J. (2002, August 21). 9/11 – Respond and Recover: A Case Study. Sidley Austin Brown & Wood LLP. As presented at LawNet 2002.

### **Rocket USA Inc. Case**

Rusberry, B. (1999, November). When Bad Things Happen to Good Entrepreneurs: What Every Small-Business Owner Needs to Know About Crisis Management. *Entrepreneur Magazine*.  
[http://www.entrepreneur.com/Your\\_Business/YB\\_SegArticle/0,4621,229495,00.html](http://www.entrepreneur.com/Your_Business/YB_SegArticle/0,4621,229495,00.html)

### **Toyota/GM NUMMI Case**

2002 Is NUMMI's Best Production Year Ever. (2003, January 3). NUMMI Press Release: Company Website. [http://www.nummi.com/doc\\_record\\_production\\_02.html](http://www.nummi.com/doc_record_production_02.html).

Armstrong, D., Hua, V., & Sarker, P. (2002, October 3). Idling Time: The West Coast Shutdown is Beginning to Hurt Workers and Industries Dependent on Imports. *San Francisco Chronicle*. <http://lists.iww.org/pipermail/iww-news/2002-October/000351.html>.

Dickerson, M. & Iritani, E. (2002, November 25). Tallying Port Dispute's Costs. *Los Angeles Times*.  
[http://216.239.33.100/search?q=cache:xCLUhYMkEpwC:www.andersoneconomicgroup.com/Publications/Press\\_Clips/98\\_02/TallyingPortDisputeCosts\\_LATimes\\_112502.pdf+NUMMI,+port+lockout&hl=en&ie=UTF-8](http://216.239.33.100/search?q=cache:xCLUhYMkEpwC:www.andersoneconomicgroup.com/Publications/Press_Clips/98_02/TallyingPortDisputeCosts_LATimes_112502.pdf+NUMMI,+port+lockout&hl=en&ie=UTF-8).

Shiels, M. (2002, October 9). US Industry Counts Cost of Port Dispute. *BBC News Online*.  
<http://news.bbc.co.uk/1/hi/business/2312175.stm>.

### **Dow Corning Corp. Case**

Kahn, G. (2003, March 24). Dow Corning Put Logistics To Work to Cut Disruption. *Wall Street Journal*, p. A2.

---

## **GHSP Case**

Ericson, J. (2001, October 4). Addressing Supply-Chain Disruptions. Line56.com.  
<http://www.line56.com/print/default.asp?ArticleID=3015>

Ericson, J. (2001, November 28). Supply Chain Interrupted. Line56.com.  
<http://www.line56.com/print/default.asp?ArticleID=3207>

## **Cantor-Fitzgerald Case**

Gordon, M. (2001, December 10). Howard Lutnick's Second Life. New York Magazine.  
<http://www.newyorkmetro.com/nymetro/news/sept11/features/5486/index.html>

Kahn, M. (2001, October 31). Commentary - Cantor Fitzgerald, A Risky Tale Of Substituting Technology For People. RiskCenter.com.  
[http://www.netrisk.com/news/dailynews/2001\\_10\\_31\\_3900.htm](http://www.netrisk.com/news/dailynews/2001_10_31_3900.htm)

Tully, Shawn (2001, September 17). Special Report: Rebuilding Wall Street. Fortune.com.  
<http://www.fortune.com/fortune/print/0,15935,370058,00.html>

## **Terrorism Insurance**

Brady, D. (2003, April 14). Terrorism: Put The Money Where The Danger Is. Business Week, p. 40.

Oster, C. (2003, March 20). Many U.S. Firms Have Sought Terror Insurance in Recent Weeks. Wall Street Journal, p. A2.

Oster, C. (2003, March 25). Many Businesses Decline to Buy Terror Insurance. Wall Street Journal, p. B3.

## **Government Mandates**

Schlesinger, J. (2003, April 24). Bill Would Fine Chemical Plants That Don't Obey Antiterror Rules. Wall Street Journal, p. B2.



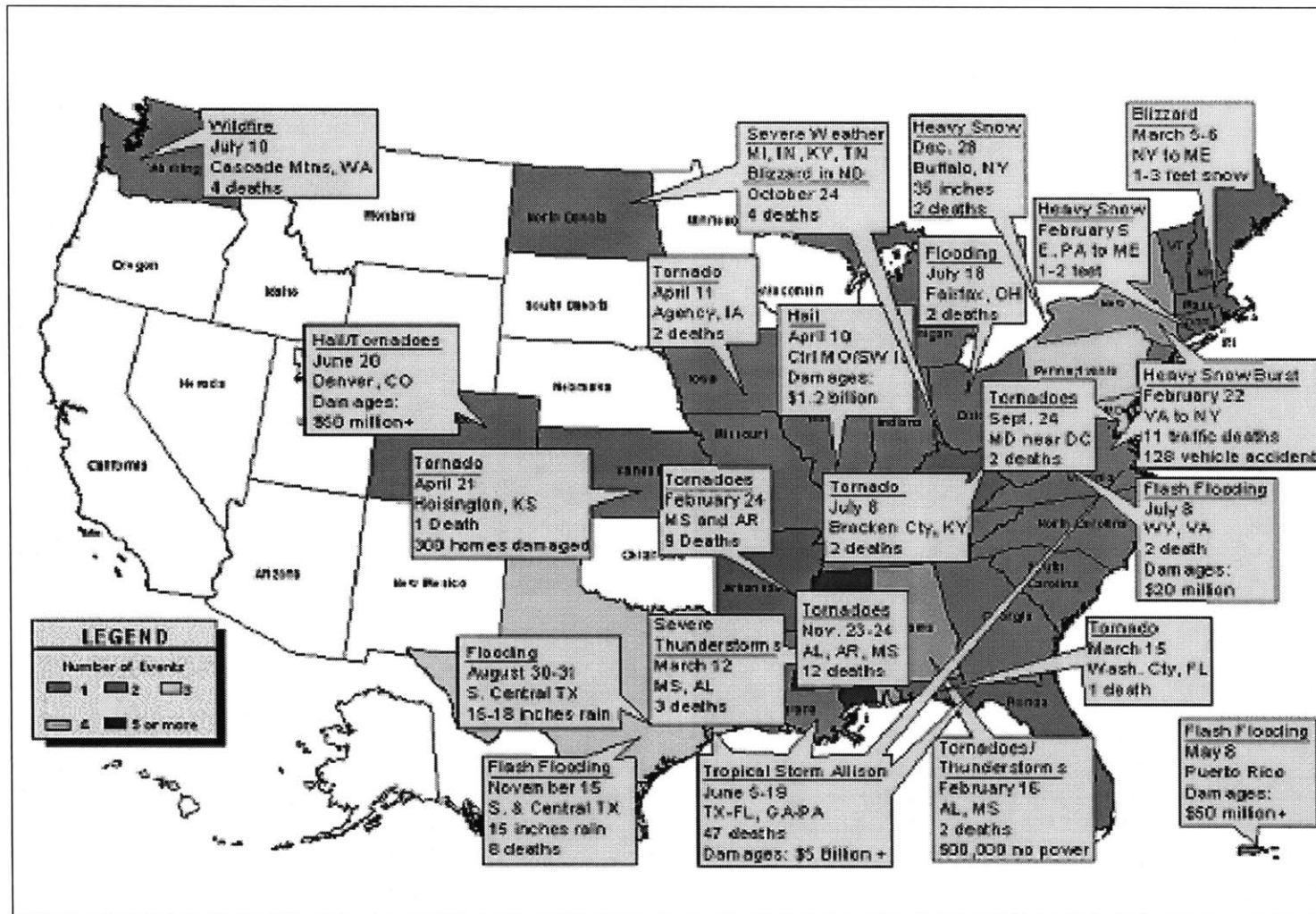
## Appendix Items

Figure 37.0 – Severe Weather Fatalities & Damage Costs: 1940 - 2001

Year	Lightning Fatalities	Tornado Fatalities	Flood Fatalities	Hurricane Fatalities	Heat Fatalities	Cold Fatalities	Winter Fatalities	All Hazard Damage Costs (\$)
1940	340	66	60	51				
1941	338	53	47	10				
1942	372	384	68	8				
1943	432	59	107	19				
1944	419	275	33	64				
1945	268	210	91	7				
1946	231	78	28	0				
1947	308	313	55	53				
1948	256	140	82	3				
1949	289	212	46	4				
1950	210	70	93	19				
1951	248	34	51	0				
1952	212	230	54	3				
1953	145	515	40	2				
1954	230	36	55	103				
1955	181	126	302	218				
1956	149	83	42	21				
1957	180	191	82	305				
1958	104	66	47	2				
1959	183	59	25	24				
1960	129	47	169	65				
1961	149	51	93	48				
1962	153	28	53	4				
1963	165	21	41	11				
1964	129	73	142	49				
1965	149	296	188	75				
1966	110	98	56	54				
1967	88	114	53	18				
1968	129	131	57	9				
1969	131	66	445	256				
1970	122	72	131	11				
1971	122	156	68	8				
1972	94	27	565	121				
1973	124	87	178	5				
1974	102	381	111	1				
1975	91	60	127	4				
1976	74	44	183	9				
1977	98	43	210	0				
1978	88	53	125	36				
1979	63	83	121	22				
1980	74	29	92	4				
1981	66	24	94	0				
1982	77	64	155	0				
1983	77	34	204	22				
1984	67	122	126	4				
1985	74	93	166	30				
1986	68	15	94	11	48		60	
1987	88	59	70	0	38		30	
1988	68	32	31	0	41	17	55	\$6,151.5
1989	67	50	95	38	6	121	63	\$13,816.1
1990	74	53	142	0	32	13	48	\$6,021.9
1991	72	39	61	19	36	13	45	\$6,203.4
1992	41	20	62	27	6	14	50	\$38,305.4
1993	42	33	103	2	20	19	66	\$28,431.3
1994	69	60	91	9	20	52	20	\$4,441.0
1995	95	93	90	17	1,021	22	17	\$11,383.1
1996	53	26	131	37	36	62	86	\$7,575.4
1997	42	67	118	1	81	51	90	\$10,785.6
1998	44	130	136	9	173	11	68	\$18,110.5
1999	46	64	68	19	502	7	41	\$12,253.3
2000	51	41	38	0	158	26	41	\$,050.1
2001	44	40	48	24	186	4	18	11,830.2
TOTAL	8841	6300	6791	2179	2387	421	825	\$182,757.7
30-Yr. Average (1972-2001):	71	65	127	18				
10-Yr. Average (1992-2001):	52	57	88	15	219	27	52	\$15,056.5

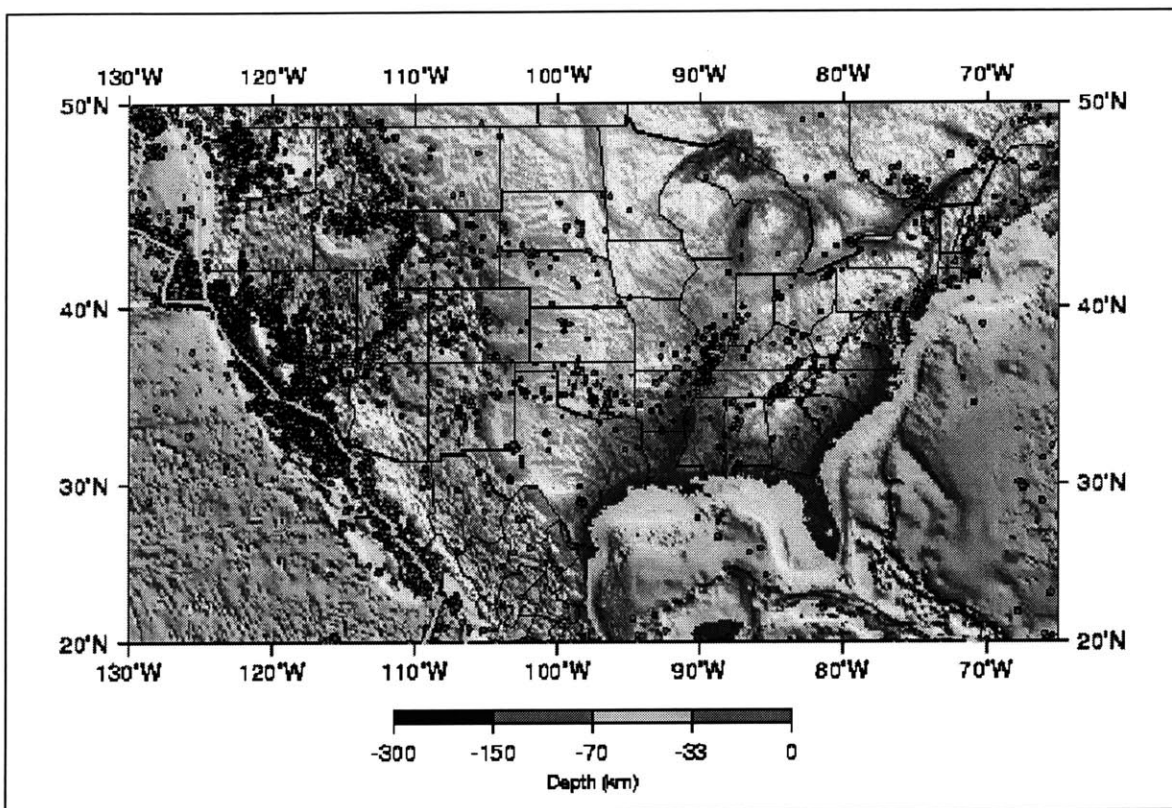
Source: National Weather Service

Figure 38.0 – Significant Weather Events: 2001



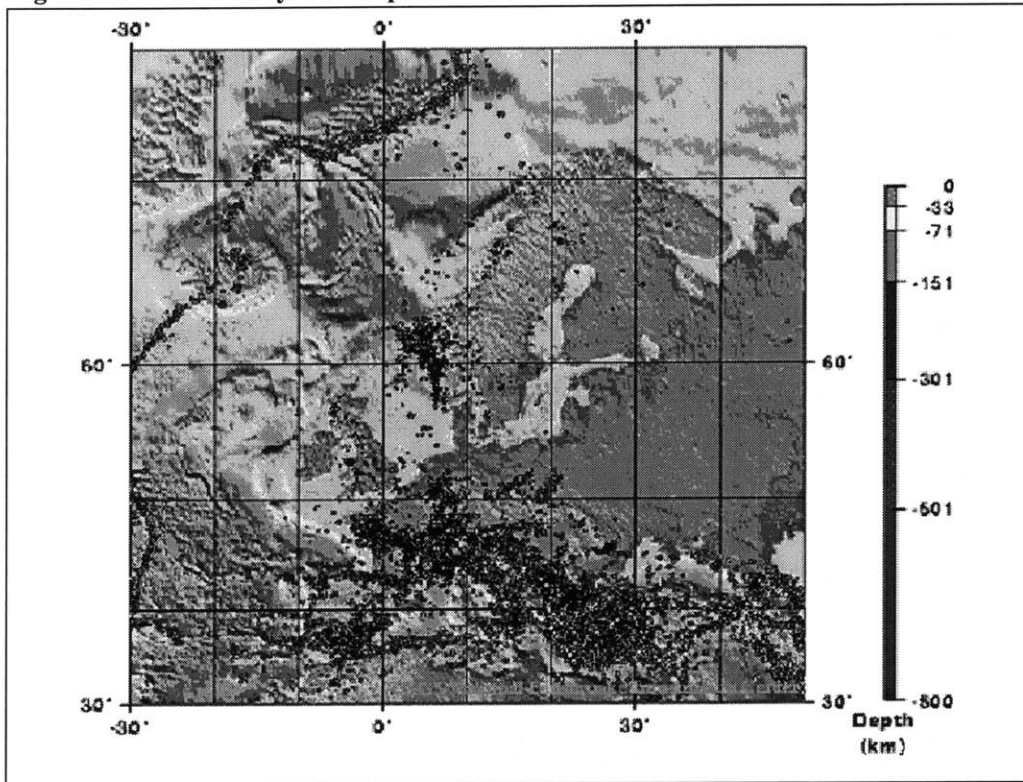
Source: National Weather Service  
<http://www.nws.noaa.gov/om/sigwx.shtml>

Figure 39.0 – Seismicity of the United States: 1977 - 1997



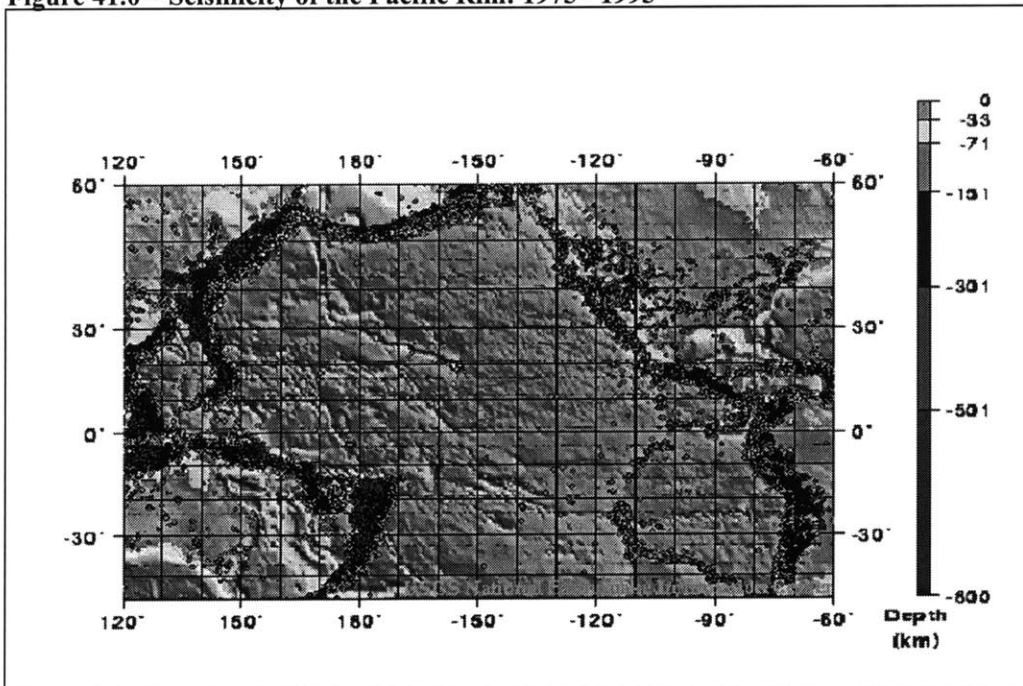
Source: USGS National Earthquake Information Center

**Figure 40.0 – Seismicity of Europe: 1975 - 1995**



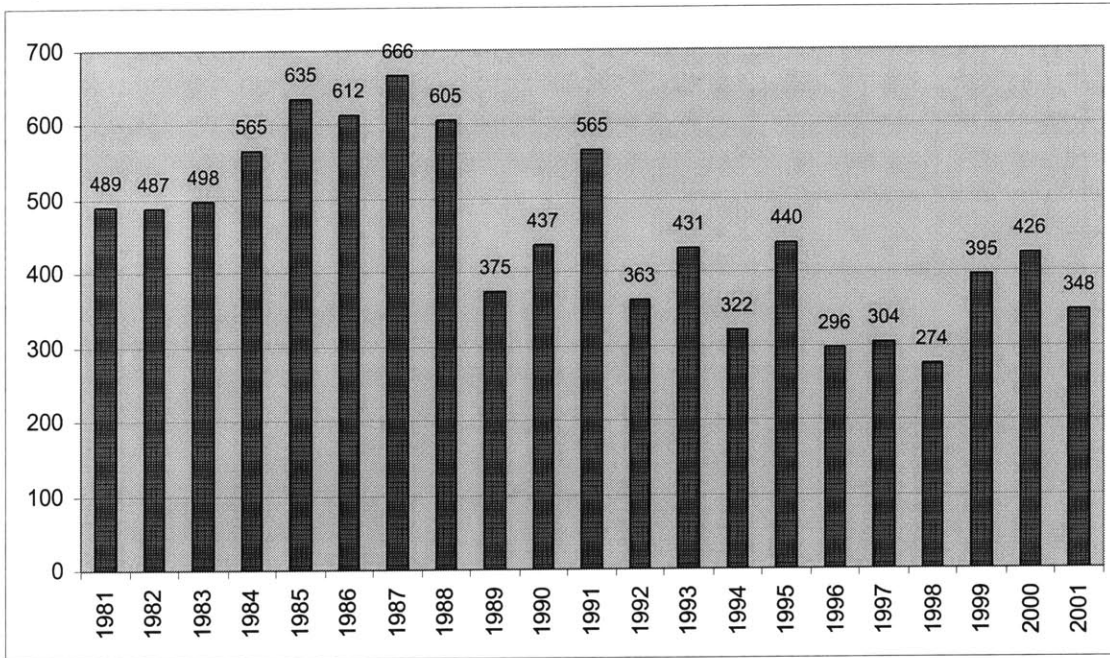
Source: USGS National Earthquake Information Center

**Figure 41.0 – Seismicity of the Pacific Rim: 1975 - 1995**



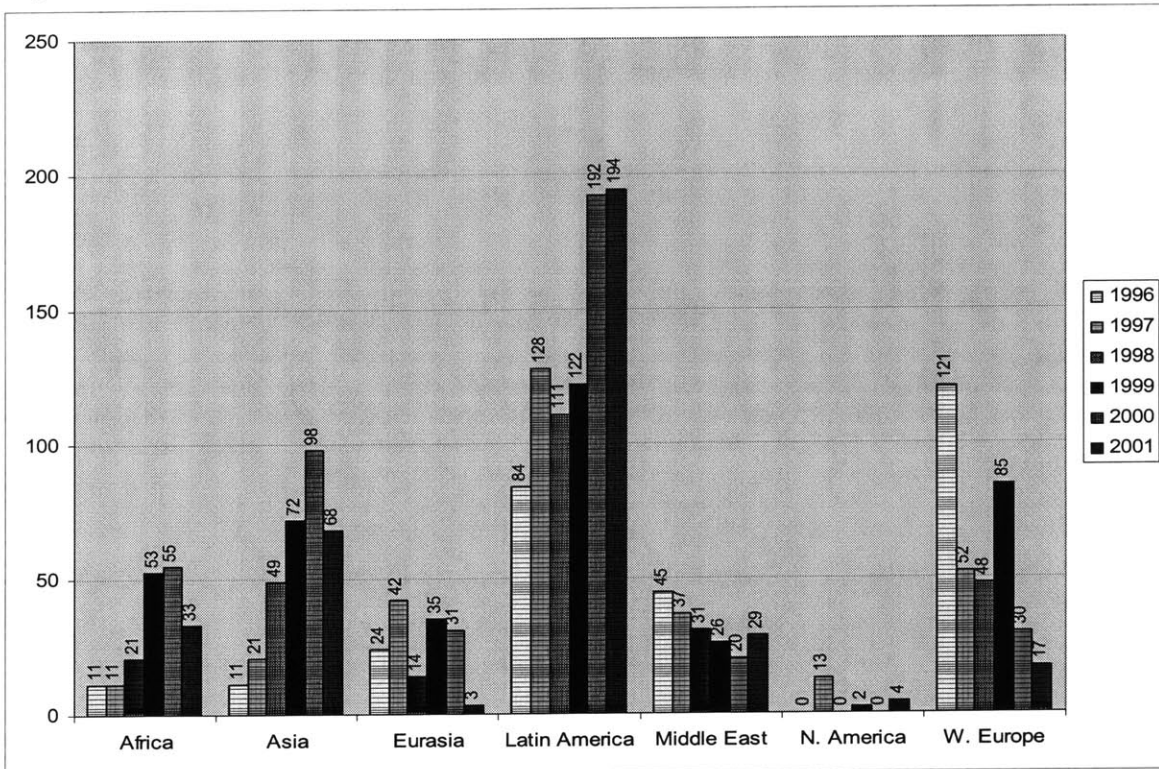
Source: USGS National Earthquake Information Center

**Figure 42.0 – Total International Terrorist Attacks: 1981 - 2001**



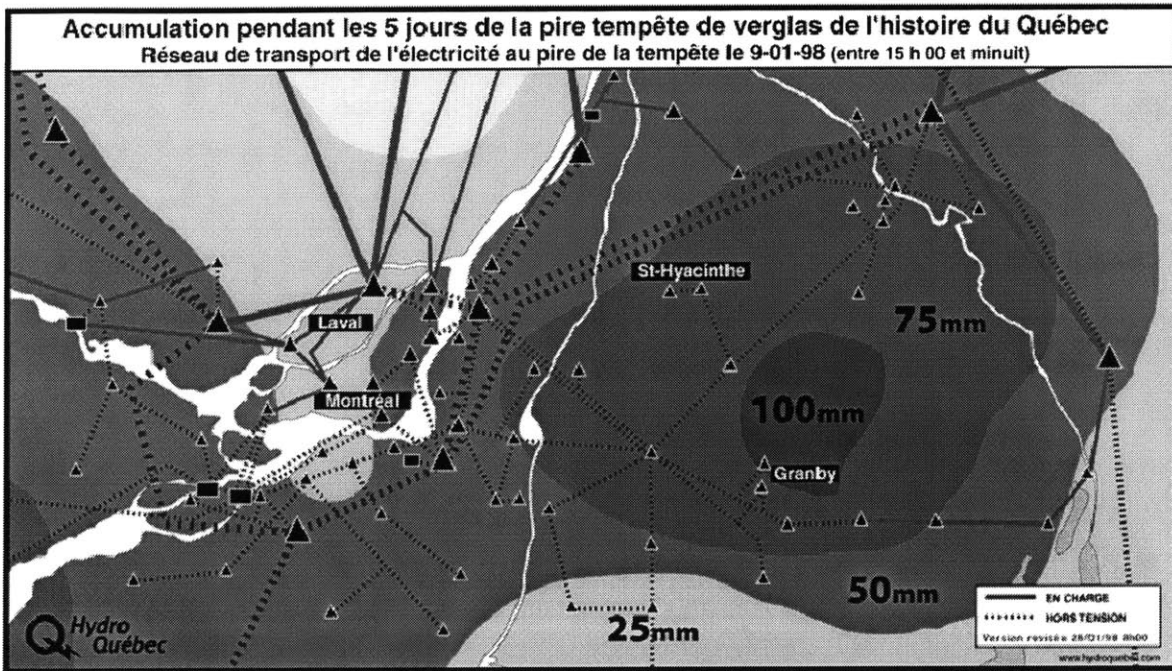
Source: U.S. Department of State, "Patterns of Global Terrorism: 2001"  
[www.state.gov/s/ct/r/s/pgtrpt/2001/pdf](http://www.state.gov/s/ct/r/s/pgtrpt/2001/pdf)

**Figure 43.0 – Total Terrorist Attacks by Region: 1996 - 2001**



Source: U.S. Department of State, "Patterns of Global Terrorism: 2001"  
[www.state.gov/s/ct/r/s/pgtrpt/2001/pdf](http://www.state.gov/s/ct/r/s/pgtrpt/2001/pdf)

Figure 44.0 – HydroQuebec Electrical Grid at Peak Ice Storm Conditions



Source: HydroQuebec  
[www.hydroquebec.com](http://www.hydroquebec.com)

Note: Map shows the Quebec electrical grid on 01/09/98 between 3pm and midnight, when the storm was at its peak. The solid green lines represent functioning lines while the dotted red lines represent non-functioning lines. The black triangles are main transformer stations and the blue areas indicate average accumulated ice (mm).