Historical Events and Supply Chain Disruption: Chemical, Biological, Radiological and Cyber Events

By

Reshma P. Lensing

B.S. Mechanical Engineering

University of Michigan, 1994

Submitted to the Engineering Systems Division
in Partial Fulfillment of the Requirements for the Degree of

Master of Engineering in Logistics

at the

Massachusetts Institute of Technology

June 2003

Signature of Author.....
Master of Logistics Program, Engineering Systems Division
May 9th, 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 Logistics and Transportation

Historical Events and Supply Chain Disruption: Chemical, Biological, Radiological and Cyber Events

By
Reshma P. Lensing

Submitted to the Engineering Systems Division
on May 9th, 2003 in Partial Fulfillment of the
Requirements for the Degree of Master of Engineering in
Logistics

Abstract

In the wake of the attacks of September 11, 2001, terrorism emerged as a legitimate threat not just to society, but to corporations as well. This new threat has challenged old business rules and prompted companies to rethink their supply chain operations. However, the events of September 11th were not the first or the only disruptions that the business world had experienced. This thesis reviews past historical events that simulate the effects of a terrorist attack and extracts lessons that can be applied by today's corporations to prepare for future attacks or disruptions. The types of events studied include Biological, Chemical, Radiological and Cyber disruptions.

Through the analysis and synthesis of each event's impact, the following generalized recommendations emerged: Prior warnings and events should be acknowledged, studied and utilized. Government intervention may strain operations under disruptive stress. Alternate sourcing should be considered to ease supply issues. Disruptions should be approached in a comprehensive and forthright manner. A security and safety culture should be fostered to prevent disruptions and control their spread. Systems should be prepared to quickly operate in isolation during a disruption. Finally, impact is frequently less severe then initially predicted.

Through the events described and these recommendations, this thesis aims to provide lessons for firms to manage their supply chains through future disruptions.

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

Acknowledgments

I'd like to thank my advisor, Yossi Sheffi, as well as the entire SCRT team, Jim Rice, Jonathan Fleck, Don Lowtan and Deena Disraelly for their guidance, support and interest in my work. I'd especially like to thank my counterpart Chris Pickett for his willingness to listen and his friendship as we muddled through the thesis process together.

I'd also like to thank my Mother, Father and sisters Shilpa and Varsha for always believing in me, most of time more than I did.

Finally, I'd like to thank my husband Brad for his support and the sacrifices that he made to bring me to and help me through MIT. Your love, warmth and acceptance of me at my highest and lowest points are always what keep me going.

Table of Contents

Tables and Figures

1.0 Introduction

On September 11, 2001, terrorism emerged as a genuine threat to the United States. The attacks on the World Trade Center, Pentagon and Shanksville, Pennsylvania brought the notion of terror home to televisions around the globe in horrifying detail. The attacks unnerved society as the assumed foundations of our lives became potential targets. Moreover, it revealed the existence of true and determined enemies that were likely to act again.

The World Trade Center was a symbol of commerce and trade in the US. However, the attacks struck business activity far beyond the limits of Manhattan. Supply Chains experienced not only the direct effects of the attacks, but also the indirect ripple effects from the policies that followed. As more threats or attacks evolve and emerge, businesses will be continually challenged to meet the needs of a dynamic environment.

Organizations require a blueprint for managing their end to end supply chains under these new constraints. This thesis endeavors to understand those needs and provide firms with knowledge that might assist them to operate in a post September 11th environment and to be prepared for what may lie ahead.

In August of 2002, Professor Yossi Sheffi, co-director of the Massachusetts Institute of Technology Center for Transportation and Logistics, launched a research initiative to assist companies to operate their supply chains under the constraints of potential terrorism. The project is titled the MIT Supply Chain Response to Terrorism (SCRT). Its goal is to understand the challenges that manufacturers, retailers and other businesses face in light of future potential disruptions.

For the SCRT project, more specific research goals include:

- Applying lessons of historical events
- Uncovering potential impacts
- Studying public-private partnerships and policies
- Determining risk assessment methods

- Understanding supply chain designs tradeoffs
- Measuring the Costs of Security

One facet of the SCRT initiative is to review past disruptions and understand the impact those events had on firms and their supply chains. This thesis strives to complete this portion of the research as a component of the SCRT project.

Because the method of a future attack cannot be predicted, it is important to focus on the impact. Past events provide useful information and lessons regarding the supply chain effects of a disruption and how companies have successfully and unsuccessfully managed those situations. Historical occurrences also allow the researcher a broader set of circumstances and settings for events, thus providing a more solid foundation of data.

This thesis will select relevant events, analyze their impacts and draw conclusions to provide a foundation for today's enterprises to prepare and operate their businesses and supply chains effectively under the constraints of terrorist threats. It is important to also note that this document is written in conjunction with a related thesis considering a different subset of events, but with similar research goals.

The core research questions that this thesis aims to answer are:

- What was the impact on the supply chain or business operations of affected enterprises following a chemical, biological, radiological, or cyber event?
- How did these enterprises react and what led them to recover or worsen?
- What can be learned from these past events to help current enterprises prepare for future disruptions?

1.1 Scope

This thesis will study past chemical, biological, radiological, and cyber events. The term event is used because some of the disruptions presented are not attacks, but

accidents. Regardless of the intent of the event, its impact can simulate a terrorist attack using the respective means described.

Physical events such as explosions, natural disasters or fires are covered in a related thesis that is also part of the SCRT research initiative. The full set of relevant events was selected based on the insight they provide while the division of coverage was determined from the natural categorical separation of events.

Although a brief description and background is provided, this thesis is not meant to recount the specific sequence of activities surrounding a selected event or attack in great detail. It also does not seek to determine the root cause of a selected case or describe the pursuit and prosecution of its perpetrator.

The following subsections provide a brief description of each type of event that is covered and why the category was chosen. A specific listing of selected events under each category is also provided in table 1.2. Further detail of event types is provided in chapters 4 through 7, the data portion of the thesis.

Biological Events

A biological weapon uses a living organism to enter the human body and provoke disease or death. These agents feed off of their host tissue to multiply, thus requiring a small amount to cause great damage. Their effects are not felt immediately but might slowly and silently wreak havoc on society. Because of this, biological weapons remain a potential threat. Despite medical advances, naturally occurring biological threats such as viruses also exist. With this in mind, the 1918 Influenza, the 2001 Foot and Mouth Outbreak, the 2001 Anthrax attacks, and the current Severe Acute Respiratory System (SARS) virus were selected for study in this category.

Chemical Events

Chemical Agents are non-living compounds created and used with the intent to incapacitate, injure or kill a target. It is widely believed that terrorist or rogue

nations have the capability to produce such weapons. Some weapons can be prepared using readily available household products, while others require ingredients that are more difficult to obtain, but are nonetheless accessible. Given this threat, it is important to understand the effects of chemical exposure. In order to do this, we study the effects of the 1984 chemical leak at the Union Carbide plant in Bhopal, India.

Radiological Events

Populations can be exposed to dangerous radiation via a massive nuclear explosion, or a 'dirty bomb', which uses a more conventional bomb to scatter radioactive materials. Though they are more difficult than conventional weapons for terrorists to obtain and develop, nuclear weapons or radiological explosions nonetheless pose a threat. In order to understand the effects of such an attack, the 1986 core explosion at the Chernobyl Nuclear Power Plant in the former Soviet Union was chosen for study. Two other well known nuclear incidents, Three Mile Island and the bombing of Hiroshima and Nagasaki, are not covered in this thesis as the incident at Chernobyl is more recent and effectively illustrates the effects of a radiological event.

Cyber Events

Advancements in computers, technology and networking have created a new threat, the cyber attack. Attacks on internetworking have become more advanced in recent years as the vulnerability of infrastructure becomes a growing concern. In order to study the effects of cyber attacks on data networks, the following events were selected; directed attacks on top ecommerce sites, a sewage utility infrastructure attack, email viruses such as Melissa and Love Bug, and distributed denial of service attacks Code Red and SQL Slammer.

1.2 Table of Events

The tables below provide a quick overview of the selected events and their effects.

Table 1.2- 1: Overview of Covered EventsError! Not a valid link.

Cyber Attacks Covered

Date	Short Name	Country	Type	Est. Casualties	Est. $ Damage	Short description
February 2000	**Attacks on Yahoo, Amazon, eBay, Buy, CNN**	United States	Cyber Directed Denial of Service	n/a	Estimated $1.2 billion in lost business, market capitalization, and infrastructure and software upgrades	Denial of service attack unleashed on these sites. Sites down or exhibit extreme latency during attack. Internet suffers 25% slowdown.
March and April of 2000	**Attack on Utility Infrastructure**	Maroochy Shire, Australia	Directed Infrastructure Attack	n/a	Aus$190,000	Disgruntled employee gained control of the sewage system. Eventually was successful and released waste into local waterways.
March 1999	**Melissa Virus**	Global	Cyber Email Virus	n/a	$80 million	Virus spreads hidden as attachment in business like email. Sends email to first 50 persons in address book. Cripples mail servers around world. Lost Productivity as servers are downed for emergency maintenance and IT personnel work overtime
May 2000	**Love Bug**	Global	Cyber Email Virus	n/a	$8.7 Billion	Email virus arriving as attachment. Script would propagate to users' entire outlook address book. Also installed malicious files on infected system, and altered certain file types. Most recorded damage.

July 2001	**Code Red Worms**	Global	Cyber Distributed Denial of Service Worm	n/a	$2.6 Billion	Worm spreads to take advantage of IIS server vulnerability. More than 250,000 systems affected in 9 hrs. Variant released less than 1 month later. Microsoft, CNN, ATT, FedEx, Qwest among those hit.
January 2003	**SQL Slammer Worm**	Global	Cyber Distributed Denial of Service Worm	n/a	$750 Million - $1 Billion	Virus spreads as DDoS attack on unpatched SQL Servers. Patch avail for 6 months. Spreads at record rates. Bank America losses ATMS. Other affected companies: SE Asian telecoms, US Gov, American Express.

2.0 Methodology and Literature Review

2.1 Data Sources and Research Methods

The breadth of subject matter contained in this thesis covers a wide area, thus a variety of data sources were utilized. For the more recent incidents journals, newspapers and magazines were used to understand events and business focused impacts. More historical events involved the use of books and prior research. Finally, more technically focused subjects were researched online through internet resources. Research methods included library research, internet based searches, and interviews with industry resources.

The data extracted from the aforementioned resources was organized and studied for consistent presentation. Recommendations were noted as themes emerged. These themes were extrapolated and generalized in a manner that facilitated their application as guidelines for companies to follow with respect to future disruptions. Data was then extracted from each event to support or reject and each potential guideline. The themes that garnered the strongest support were then selected for detailed discussion. The conclusion section of this paper reviews these themes in depth and demonstrates how the past events studied support each concept. Finally, the guidelines are presented as a framework for companies to prepare for and manage future disruptive events.

2.2 Literature Review

This thesis focuses on historical events and attempts to understand them from a supply chain and business perspective. Given that this thesis synthesizes information regarding historical events, the existence of published research covering portions of the subject matter was a forgone conclusion. The available research tends to focus on the general notion of the effect of terrorism on the supply chain, or on the specific events outlined for coverage.

Soon after the September 11 attacks, two works emerged that breathed life into the study of the effects of Terrorism on the Supply Chain. The first work is a paper titled "Supply Chain Management under the Threat of International Terrorism" published in 2001 by Professor Yossi Sheffi, Co-Director of the MIT Center for Transportation and Logistics[1]. This paper outlines the new forces resulting from the attacks and goes on to specify areas for investment and improvement as well as guidelines for public-private partnerships. In fact, Sheffi's work led to the creation of MIT's Supply Chain Response to Terrorism initiative, which seeks to better understand various aspects of terrorism and supply chain including potential threats, scope of impact, corporate response, and supply chain design tradeoffs. These tradeoffs include:

- Efficiency vs. redundancy
- Collaboration vs. secrecy
- Centralization vs. dispersion.
- Lowest bidder vs. known supplier
- Security vs. privacy

In addition to Sheffi's work, other early works considering terrorism and supply chains are "Targeting a Just-in-Case Supply Chain for the Inevitable Next Disaster" by Joseph Martha and Sunil Subbakrishna, in September of 2002 for Supply Chain Management Review, as well as "Creating a Just-in-Case Supply Chain for the Inevitable Next Disaster" by Mr. Martha and Eric Vratimos in 2002 for Marsh and McLennan company's Viewpoints magazine. The former document studies the vulnerabilities of a just-in-time system and makes recommendations to fortify it. The latter reviews a number of case studies resulting from disruptions such as the September 11th attacks, hurricane Mitch and an earthquake in Taiwan. Although this work attempts to understand the effects of terrorism on companies, it limits coverage to natural and physical disasters.

[1] Prof. Sheffi is also the faculty advisor for this thesis.

A number of less supply chain specific articles and literature were also written specific to September 11th and its impact. However, few mention other historical events as contributions to future planning. There is also a body of literature that focuses on supply chain recommendations in the face of terrorism, but few mention past events while those that do refer to terrorist attacks similar to September 11th.

With respect to Chemical, Biological, and Radiological events, significant research exists. Much of the published information covering events that occurred more than five years ago focuses on a particular disaster, spending a great deal of time detailing the events of the disaster. Economic effects are described in terms of overall effects on the economy rather than specific businesses. Examples of this include America's Forgotten Pandemic: The Influenza of 1918, an account of the Spanish Influenza written by Alfred W. Crosby (1989). This work chronologically follows the spread of the 1918 Influenza throughout the U.S. and Europe and touches on repercussions to industries, without particular detail on specific businesses or firms. Some disruptions are described in the context of Crisis Management. This is true for the Union Carbide chemical leak in Bhopal, India. Here the economic effects are focused on Union Carbide more than other businesses in the outlying area.

However, more recent events provide more information on business repercussions related to disruptions. Sever Acute Respiratory Syndrome, or SARS continues to spread as this thesis is written. Newspapers and magazine initially detailed the nature of the virus, but have slowly moved toward understanding impacts. One disadvantage of an ongoing event is the benefit of perspective that can be gained once the disruption has completed its course. In this respect, information on Foot and Mouth disease (FMD) in the spring of 2001 is more comprehensive. This is partially due to post mortem type reports that were published studying FMD and its effects. Examples of this include The State of the Countryside Report produced by the United Kingdom Countryside Agency in August of 2002 or a report by Iain Andersen written in July of 2002 and titled Foot and Mouth 2001: Lessons to be Learned Inquiry Report. Both of

these works spend some time understanding industry effects and provide specific case studies of particular businesses.

In the Network Security and Cyber Attack arena, there is a vast amount of data available. With each attack or exploitation, published information increases in both breadth and volume. However, at closer inspection, much of the literature available provides the following insights:

- Best Practices in securing networks
  - What to do
  - What not to do
  - Reviews of security products
- Potential Dangers
  - What might happen
  - How it would occur
  - What the worst case effects could be
- An overview of jargon associated with Network Security
- Technical Details regarding the nature of attacks that have occurred
  - Technical Description of nature of attack
  - Potential Technical Damage
  - Technical Treatment of Virus

While these are all important topics, there is less data available on the effect of these attacks or events on businesses. The information that does exist tends to cover impact in broad terms with an aggregate viewpoint and little attention to detail or individual effects. For instance, research describes how many total systems were down, while there is little information on systems and downtime at individual businesses or the associated costs incurred at that location. Carrying this notion a step further, there is even less information noting effects on supply chain partnerships, despite the fact that the information exchange is largely digital.

Though research exists on particular Chemical, Radiological, Biological and Cyber events, there is a void in research that fuses together all of these types of events into one comprehensive document and attempts to learn through their similarities. In addition, there is little research focusing on the business effects of these events together with an eye on supply chain lessons and future terrorist attacks. This thesis attempts to fill these two voids.

2.3 Research Challenges

In conducting research, certain challenges were apparent. As this document attempts to focus on business effects of disruptions, it relies on the willingness of businesses to discuss those effects. When these effects are heavily publicized, the information is readily available, for instance the loss of Bank of America ATMs resulting from the 2003 SQL Slammer cyber attack. However, when the effects are not widely publicized, this information becomes increasingly difficult to obtain. This is because businesses are not incented to discuss difficulties, failures or challenges that they face, given that acknowledging these issues may place the company in a poor light. This is especially true with respect to cyber attacks, as discussion of negative effects becomes an inadvertent confession of poor security practices and a possible lack of technical understanding.

3.0 Results Overview

The next four chapters of this thesis review a number of events in the various categories discussed earlier, Biological, Chemical, Radiological, Infrastructure and Cyber. The details of particular historical events are described followed by a review of the supply chain effects that resulted.

Chapter 4 studies biological events including the 1918 Influenza, Foot and Mouth Disease, Anthrax attacks on the U.S. and the SARS virus. Chapter 5 understands the effects of chemical events by studying the Union Carbide accident in Bhopal, India while chapter 6 reviews the Chernobyl Nuclear Power Plant explosion for the impact of Radiological events. Chapter 7 covers cyber events, with section 7.1 focusing on directed attacks, including those on popular ecommerce sites and government entities. 7.2 Looks at an infrastructure attack on an Australian sewage plant. Section 7.3 studies email viruses Melissa and Love Bug, while 7.4 reviews the Code Red worm, and finally 7.5 focuses on the recent SQL Slammer worm. As these studies are read, the following themes should be considered:

- **Prior Warnings and Events Should be Acknowledged and Utilized**

  Although the victims of disruptions were provided with the benefit of prior experience, this knowledge was frequently disregarded. The events described demonstrate the advantage that results from understanding prior occurrences and giving early warnings significance and attention.

- **Government Intervention May Strain Operations**

  When an event occurs on a large scale, governments often intervene and provide assistance. This intervention may ease one facet of the disaster for an industry while negatively affecting operations for other facets or other industries.

- **Alternate Sourcing can Ameliorate Supply Issues**

  A disruption may strain sources and raw materials along a supply chain. Businesses should prepare for disruptions by creating supply contingency plans and in some cases building relationships with alternate suppliers.

- **Manage Disruptions with a Comprehensive Forthright Approach**

  A disruption should be approached and treated comprehensively in order to get a correct view of the problem, and effectively treat affected areas. This is in contrast to a localized approach that may result in inaccurate statements, unidentified problem areas and fixes that treat one area at the expense of another. Candor and forthrightness should also be employed by those in crisis to facilitate outside assistance and build trust.

- **A Safety and Security Culture are Important Tools Against Attacks and Proliferation of Disruptions**

  A safety or security culture is created when an organization stresses these notions as paramount throughout their business so that they are reflected as the prevailing attitudes of employees. By fostering a safety culture businesses empower employees to make decisions that can save lives, protect against disruptions, and control the spread of harmful effects. Similarly, organizations that place emphasis on security are better safeguarded against breaches and internal attacks.

- **Prepare Systems to Operate in Isolation**

  As nodes in any system become increasingly connected and communicative, their lines of communication are increasingly at risk. This risk requires that connected entities are prepared to operate in an isolated, disconnected environment to ensure continuity of operations.

- **Often, Impact is Not as Dire as Originally Predicted**

  In many cases, while an event is unfolding, forecasts and predictions are made regarding the expected impacts and outcomes. Frequently these predictions

describe extreme scenarios with great negative impacts. However, in retrospect, systems display more resilience than expected and these predictions often prove to be overestimates.

The conclusions portion of this document will revisit these themes, discuss them in greater detail, and provide supporting evidence through the data presented.

4.0 Biological Events

A biological attack uses a living organism that acts on living matter to cause disease or death in others. Biological weapons pose a significant risk as they are hard to identify and even more difficult to detect. Because diseases multiply within their host organism and are contagious, only a small amount of a biological weapon is required to launch an attack. With advanced speed of proliferation, a biological agent can cause significant damage before it is detected. All of this could make this type of weapon attractive to a rogue group or terrorist organization.

In the following section biological events from the past are studied to glean some understanding of their effects. This chapter begins by looking back nearly one hundred years to the Spanish Influenza of 1918, a pandemic that spread toward the end of World War I. This is followed by a review of the outbreak of Foot and Mouth disease that devastated the English countryside in spring of 2001. The chapter then takes a brief look at the Anthrax scare that took hold of the United States Postal system in the fall of 2001. Finally, the recent outbreak of Severe Acute Respiratory Syndrome or SARS in Spring 2003 is considered.

4.1 The Spanish Influenza of 1918

In the latter half of 1918, the final months of World War I, the world celebrated peace and welcomed the end of meaningless death. However, a new killer, more lethal and less forgiving, was establishing a foothold among civilization. This killer would ultimately claim the lives of millions of people around the globe. It was the Spanish Influenza.

Disease Characteristics

The Spanish Influenza initially resembled the flu, but often developed fatal complications. Early symptoms would appear suddenly and were similar to that of common influenza, including fatigue, weakness, coughs, fever, and runny nose. In

some cases, this lasted two to four days followed by recovery. However, this strain differed from the flu in that it often brought with it a secondary infection of pneumonia which was lethal enough to cause death within 48 hours of initial symptoms. Pathologists found afflicted lungs filled with a bloody fluid, dissimilar to common pneumonia where lungs would become merely coarse and hardened. The disease was thought to be airborne and spread by coughing and sneezing (Billings, 1997)

The Spread of the Disease

The Spanish Influenza arrived in two waves. Europe saw the greatest swell in the summer of 1918, while the United States experienced the worst in the fall of the same year. Its earliest effects were noted in the United States in March of 1918. During this early period secondary infections were rarer and thus fatalities were fewer, with most suffering from the shorter two to four day illness. This, in combination with the medical limitations and conditions of the time, diminished concerns. Influenza and even pneumonia were common enough that scattered cases were no cause for alarm.

Since the 1918 Influenza struck in tandem with the war, it was paid less attention, with limited information and reporting given to it. The war also facilitated the disease's spread as troops often shared small enclosed spaces, frequently encountered other troops, and traveled great distances via ships. Indeed a global issue, by August of 1918 the Spanish Influenza had established itself in places as far reaching as the US, Western Europe, Russia, India, China, New Zealand, Cuba, Puerto Rico, and the Philippines.

By late August of 1918, the disease had reached pandemic. Sierra Leone, a West African port commonly used as a coal fueling station was one critical area struck with the disease. This was problematic as ships would not only refuel, but pick up the disease and carry it back to foreign lands. In Sierra Leone Crosby (1989) describes how the disease spread from the port to the industrial center and had affected two-thirds of the population by early September. Brest, France was another location that

fostered the influenza. Housing large American camps and war training grounds for the French, Brest had a transient population of 45,000 (Crosby, 1989), which facilitated the spread of the disease. In the United States, the disease was also spreading quickly. In the span of a week, a Navy Training center near Chicago saw 2,600 hospitalized (Crosby, 1989). Even among civilians, the war facilitated the spread, with rallies and parades held daily to support the armed forces.

On the reporting front, Spanish Influenza found itself in competition with more sensational war headlines. A lack of communication and education "...provided a perfect climate for confusion, panic, and proliferation..." (Crosby, 1989, p49). The Fourth Liberty Loan, issued on October 4th 1918, was billions of dollars in war bonds. In a campaign to promote the bonds, parades were held in cities such as Chicago, Philadelphia and New York, spreading the disease among supportive civilians.

> "Very few health officers and no communities as a whole really appreciated the devastation the pandemic could wreak until experiencing it. Spanish Influenza was just too new, to unprecedented, and it moved faster than the human mind could assimilate news of it," – Crosby (1989, p92).

This theme is found in nearly every city struck by the pandemic. When the Influenza reached the West coast of the United States, the East Coast epidemic was on the wane. Los Angeles, San Francisco and Seattle were aware of the symptoms and severity of the disease. And yet, all of these places acted counter to this information. In San Francisco, war and bond rallies were held just as the Philadelphia epidemic was slowing down. Similarly, Seattle held a gathering of 10,000 civilians at a National Guard Camp despite 173 reported cases of Influenza at the camp.

Direct Impact

The greatest impact of the Spanish Influenza was the loss of life. It is commonly estimated that 20 million people around the globe died at the hands of the deadly virus, though many believe that this is a conservative figure. In the United States, the

number is approximately 675,000, or .66% of the population (Brainerd & Seigler, 2002). As the disease wreaked its havoc, hospitals suffered from overcrowding, and there was a shortage of medical professionals around the globe.

The United States Health Protection Service estimated in 1919 that more than 25 million people in America suffered from Spanish Influenza, whether fatally or not. With so many ill, treating the ill, or avoiding human contact, other services suffered as well. In Philadelphia the phone company lacked operators and was forced to limit calls to emergencies reported with short one-word codes. In San Francisco, garbage collection shut down because of sick workers and absenteeism, causing trash to accumulate around the city. Crosby (1989) contends that other cities also saw police, firefighting, and garbage collection suffer from lack of workers.

Once the Influenza had completed its damage, it left cities with the morbid task of disposing of the afflicted bodies. Philadelphia experienced a shortage of embalmers and grave-diggers and looked to volunteers. There was also a scarcity of coffins, and local government found additional suppliers that could increase production in businesses with wood-working equipment. Similarly, more coffins were produced using cheaper and more available pine. In fact, the city of Buffalo New York ventured into the coffin-making business themselves to alleviate the problem.

Indirect Impact

Once the disease was acknowledged, officials implemented measures to halt its spread. Cities such as Philadelphia closed schools, churches, theaters, and banned public gatherings. In Australia popular horse races were cancelled. Theaters closed as a result of the disease in San Francisco were loosing nearly $400,000 1918 dollars each week. Many cities such as San Diego and San Francisco also implemented a mask ordinance requiring city residents to wear masks outside of their homes. In the first five days of the ordinance, over 100,000 masks were distributed in San Francisco. Subsequently, the Red Cross and other mask distributors experienced shortages.

4.2 Foot and Mouth Disease, Spring 2001

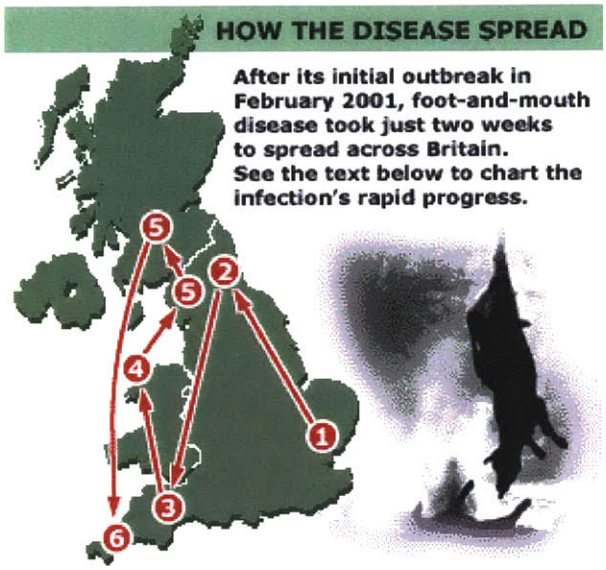
In February of 2001, Foot and Mouth disease swept across rural Great Britain. In a matter of weeks the highly contagious disease infected millions of livestock and threatened the agricultural economy. The Government responded with an order to slaughter potentially affected animals and quarantine the affected areas. These actions impacted agriculture, its customers and suppliers, and devastated the British tourism industry.

Disease Characteristics

Foot and Mouth disease, also referred to as FMD, is a virus affecting animals such as cattle, pigs, and sheep, as well as more rare livestock like goats and llamas. It is a highly infectious airborne virus producing a weakening pain and lameness as well as lesions in the mouth and on the body of infected animals. Animal secretions such as milk, breathe, saliva, and excrements are all contagious, which facilitates the spread within a farm or enclosed rural area. Quarantine is used to prevent the spread of the disease to unaffected areas. Culling, the separation of affected animals for slaughter and burning, is used to halt the spread within an affected area. Vaccination is also an available option to control an outbreak.

Spread of the Disease

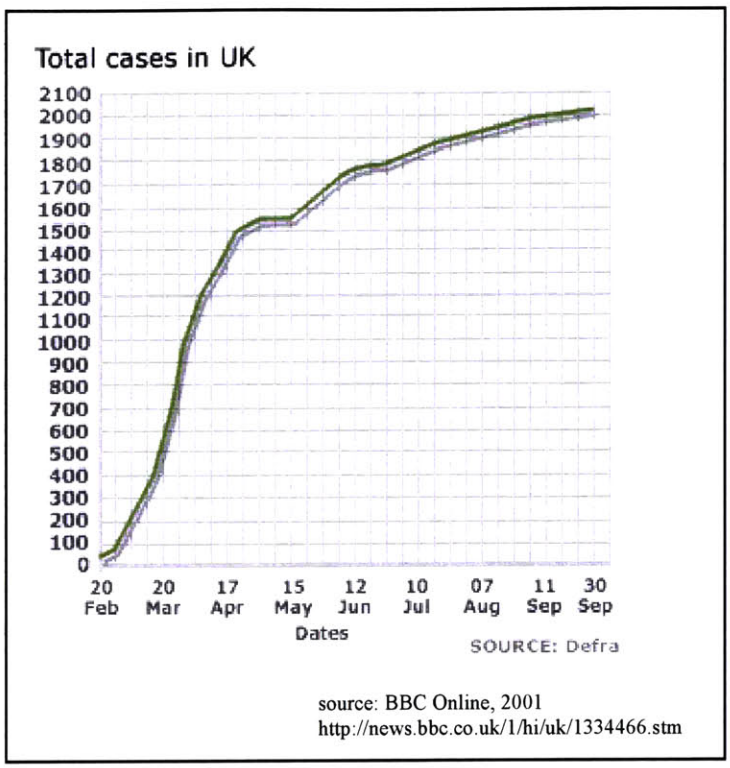
Foot and Mouth disease was initially detected on February 19, 2001 at a slaughterhouse in Essex, an area northeast of London. Once outbreak was confirmed, the disease continued to spread while its origins and potentially affected areas were identified. Figure 4.2-1 below gives a high level view and timeline of the disease's path across England. The proliferation of Foot and Mouth around the countryside was rapid and the nation quickly faced a crisis. Figure 4.2-2 depicts the growth in confirmed cases over the spring and summer of 2001. The outbreak lasted for 221 days and was considered "...one of the worst peacetime disaster since 1945," ("Learning the Hard way", 2002).



1. 19 February 2001:
Outbreak begins at Little Warley in Essex
2. 23 February 2001:
After more cases erupt in Essex the disease makes its first major leap and arrives at the other side of the country in Heddon-on-the-Wall in Tyne and Wear
3. 24 February 2001:
A day later the disease moves back south to Highampton in Devon
4. 27 February 2001:
As the number of cases rises across England foot-and-mouth makes its first appearance in Wales in Gaerwen, Gwynedd
5. 1 March 2001:
In under two weeks the epidemic reaches Cumbria and Scotland
6. 3 March 2001:
Cornwall is also hit, as foot-and-mouth covers the length and breadth of Britain

source: BBC Online, 2001
http://news.bbc.co.uk/1/hi/uk/1334466.stm

Figure 4.2- 1: The Path of Foot and Mouth around the English Countryside



source: BBC Online, 2001
http://news.bbc.co.uk/1/hi/uk/1334466.stm

Figure 4.2- 2: The speed of contamination is apparent in the growth of total cases of Foot and Mouth disease from February through September of 2001

Foot and Mouth Disease is difficult to identify and easy to overlook. Because of this, it is thought that a number of infected animals were carrying the disease and spreading it prior to detection of an outbreak. In his inquiry report, Foot and Mouth 2001: Lessons to be Learned, Iain Anderson (2002) said, "at least 57 farms in 16 counties were infected before the first case was confirmed." In the livestock trade, animals were formally moved from farm to farm via markets, but often through informal handshake agreements as well. This contributed to the initial spread of the disease between farms even after markets were temporarily closed. Once the disease arrived on a farm, it spread quickly among the animals until it was detected and infected animals could be separated. Since many farms were in close proximity to each other, the airborne disease also spread this way, although the disease did not travel great distances.

Response

Initially, local governments responded to the crisis by closing markets and imposing restrictions on cattle movement and transportation. Farmers and their families living on infected farms were also more or less quarantined until instructions were provided. Locally, slaughter and burning of livestock was initiated to eradicate the disease. On February 27, 2001, as the apparent severity of the outbreak had increased, livestock movement was restricted at the national level. This was followed by restrictions on public footpaths, the closing of parks and the postponement of public events in rural areas to prevent the spread via humans. Livestock exports were also banned from the United Kingdom by the European Union and British Parliament. As cases appeared in Ireland, Scotland, the Netherlands, France and Germany, transportation and export restrictions were imposed in these countries as well. On March 15, 2001, the British Government implemented a measure that ordered all livestock within a three kilometer radius of infected livestock to be slaughtered and burned. All of these responses would ultimately have harmful repercussions on some of Britain's most important industries.

Agriculture Industry

The agriculture industry in England suffered the brunt of the direct affects of Foot and Mouth disease. An estimated 6.5 million cattle, pigs and sheep were slaughtered and burned. According to Cameron's 2002 Foot and Mouth Disease: State of the Countryside Report, sponsored by the Countryside Agency[2], the agricultural cost of Foot and Mouth disease was close to £2.4 billion (US$3.9 million). Among the British rural community, it was widely believed that the high cost could have been avoided. Indeed the government's indiscriminate three kilometer slaughter radius rule resulted in the loss of countless unaffected livestock. Because slaughter was delayed in some areas, farmers also lost income continuing to feed the animals slated for culling. In the southwest peninsula region of Devon alone, every million pounds of lost livestock output meant £400,000 (US$648,000) lost from the area's gross

[2] The Countryside Agency is a national body in England responsible for conservation of the countryside. http://www.countryside.gov.uk/index.htm

domestic product. Unemployment was also prevalent among those in rural industries, where employment switching costs are high.

Agricultural suppliers including livestock markets, livestock transporters, and feed providers suffered an estimated £85 million (US$138 million) loss. The State of the Countryside Report (2002) estimated the demand slowdown for feed and veterinary products at about 10-15%, while the closing of markets affected an estimated 3,000 related employees. The report went on to say that livestock transporters were severely affected as their business was halted by movement restrictions, and their contaminated vehicles could not be redeployed for fear of further spreading infection.

Downstream, agriculture producers and the food industry suffered £575 million (US$931 million) from lost business, withholding, and pricing depression (Anderson, 2002). Figure 4.2-3 below illustrates the ripple affects throughout the agriculture industry.

14.1.1 Sectoral Economic Effect of FMD (Agriculture, Food Chain and Tourism) 2001- 2005

Sector –		£ million
Agricultural producers		-355
of which:	Market prices[1]	-50
	Export loss[2]	-130
	Withholding costs[3]	-175
	Consequential costs[4]	-35
	Sheep Annual Premium[5]	-120
	Agrimoney aid	+155
Food Industry		-170
of which:	Auction Markets	-95
	Abattoirs	-40
	Processors/hauliers	-35
Tourism[6] (range)		-2700 to -3205
Indirect effects		
Agriculture/food chain[7]		-85
Tourism[8] (range)		-1835 to -2180

[1] Market prices represents a loss of revenue associated with price changes consequent upon the changed pattern of marketings.

[2] Export loss is an additional effect associated with lower quality domestic uses (e.g. pet food) for supplies diverted from export.

[3] Withholding costs are the extra costs and deterioration in quality associated with holding animals on farm beyond optimum marketing dates.

[4] Consequential losses are those associated with the loss of production whilst farms are prevented from re-stocking.

[5] Sheep Annual Premium/Over Thirty Months Scheme/Agrimoney are associated subsidy changes, some of which are co-funded by the EU budget.

[6] Losses of gross value added.

[7] Additional (indirect) costs.

[8] Estimates from input-output multipliers to all industries linked to tourism.

Source: DEFRA and the Department of Culture, Media and Sport

source: Foot and Mouth 2001: Lessons to be Learned Inquiry Report. (2002)

Figure 4.2- 3: Ripple effects of Foot and Mouth Disease

Over the long term, the farming industry was expected to face difficulties in restocking their herds and rebuilding their breeds. These difficulties included raising capital to restock (well exceeding Government crisis coverage), government approval to restock, and favorable restock prices (Cameron, 2002).

Tourism Industry

News site Ananova (2001) reported that Foot and Mouth related losses to the tourism industry from March through October 2001 reached £3.3 billion (US$5.3 billion), thus exceeding the price tag to the agriculture industry. Tourism experienced the greatest loss as a result of reduced travelers to the United Kingdom. Although the disease is harmless to humans, some believe that international travel declined as a result of confusion over this point (Cameron 2002). As of April of 2001, Heathrow Airport had experienced a 2.3% decline in traveler numbers. Similarly, Eurotunnel, which serves the channel tunnel rail linking England and France, saw its passenger numbers drop 10% in the first four months of 2001 ("Travel Firms Hit," 2001). In April 2001, foreign tourists spent £885 million in England, compared to £1.06 billion the previous April ("Farm Crisis 'body blow'..." 2001). Depression of the tourism industry was expected to lead to the loss of 20,000 to 30,000 jobs according to BBC ("FMD: Economic Impact," 2001).

The American Hospitality Association estimated that 80% of hotels, inns and accommodation providers were impacted by the outbreak, affecting small independent companies and bed and breakfast houses most severely. This may also be the result of widespread closing of public attractions in the area. The State of the Countryside Report (Cameron, 2001) estimated that as of April 30, 2001, over 1000 attractions were closed as a result of Foot and Mouth. Shops in affected areas that relied on tourists saw steep declines, while retail sales in town centers increased as people were hesitant to enter the countryside. In the Southwest of England, considered to be the hardest hit, it was estimated that restaurants and cafes lost £8 million (US$13 million) in revenue (Cameron, 2001).

Gloustershire, a rural area in southwest England, suffered a difficult tourism blow during the Foot and Mouth epidemic. The Cheltenham National Hunt festival, an annual three day equestrian event normally held in the countryside in mid-March was first postponed, and then cancelled due to nearby cases of Foot and Mouth Disease. Each year the event was expected to fuel the area tourist economy directly through ticket sales as well as indirectly through gambling, hotels, restaurants, pubs and shops. Though lost ticket income was covered via insurance, BBC reported that the event set the local economy back by £30 million (US$48 million) ("Cheltenham's £30m Blow", 2001). Hospitality businesses including hotels, caterers and restaurants were among the victims, as the meeting was expected to bring 200,000 visitors to the area. The damage to the gambling industry was equally harmful as bookmakers estimated losses reaching £100 million (US$162 million) (Fleetwood-Jones, 2001). Figure 4.2-4 illustrates the consumption that usually takes place during the festival in Cheltenham.

Figure 4.2- 4: The consumption that was foregone as a result of the Foot and Mouth related cancellation of the Cheltenham Equestrian Festival in Gloustershire, England.

Leather Industry

With the mass culling and burning of livestock, the number of hides processed was cut in half and a hide supply crisis ensued. The loss of this vital raw material translated to a 50-75% increase in prices for the leather industry ("Hiding to Nothing," 2001). Although British hides accounted for a small portion of hides globally, the hide market was rather sensitive to supply and demand fluctuations.

Because of this, the effects were felt globally. For instance, Lear Corporation of Southfield Michigan, who supplies leather seats to high-end car manufacturers, saw prices rise 20% (Kaufman, 2001). This demonstrates the power of global trade and the connected world. Though Foot and Mouth disease occurred within a relatively small area of the world, its repercussions were felt all over the globe.

The Malungs Garveri tannery in southern Sweden, addressed the problem by sourcing elk hides, although in many applications this was not possible. Products like sheepskin cannot be substituted and forced companies to source outside of Europe in places such as Australia and the United States.

In the aftermath of Foot and Mouth, the reduced demand for beef continued to place downward pressure on the leather hide supply as fewer animals were slaughtered for meat. Pittards PLC, a Somerset England specialty leather supplier who provides leather for Louis Vuitton Luggage, Adidas, Puma and Clarks footwear, gloves, apparel and other products, warned of lower profits in mid-2001 as a result of the hide shortage and alternate sourcing. Pittards was in the habit of purchasing about 10,000 hides each week, half of which came from Britain ("Foot-and-Mouth Disease Spreads," 2001). Another profit warning due to rising leather costs came from Portland, Oregon's Nike as late as the first quarter of 2002.

Crisis Management

Though Foot and Mouth disease shook the British economy, many questioned the government's handling of the crisis along the way. One criticism was that the government was too slow in halting the movement of animals ("Learning the Hard Way," 2001). BBC interpreted Anderson's Lessons Learned Inquiry Report (2002) to say that better knowledge of farming practices and information specific to the nature and spread of the disease would have brought swifter action, which is necessary in fighting a fast moving infectious disease such as Foot and Mouth ("Q&A," 2002).

Once the outbreak was widespread, government communication was found to be fragmented and inconsistent. In fact at one point, Nick Brown, the Agriculture Minister, misstated that the disease was under control. Indeed the Anderson Report (2002) suggests that government face future challenges more comprehensively, creating a "National Strategy" and slowly building public trust through training, information, and communication to better understand the impact of its decisions. In the same way, there were also groups who felt that the Ministry of Agriculture Fishing and Food's method was too indiscriminate in selecting animals to be culled and could have avoided the slaughter of millions of unaffected animals ("Learning the Hard Way," 2002).

Another frequent area of criticism was the delayed decision by the British government to deploy the army to assist with the culling and disposal of the animals. Close to one month after the outbreak the army was called for logistics assistance in moving carcasses to mass 'pyres' along small rural roads. Army Brigadier Alex Birtwhistle noted that carcasses had piled up and begun to rot before the army arrived ("A Hell of a Mess," 2002). The delayed decision especially came under fire as a 1967 Foot and Mouth outbreak report recommended swift army deployment in future outbreaks. Thus it was revealed that the British Government, particularly the Ministry of Agriculture Fish and Food (MAFF) had neglected the 1967 report. This was compounded by Anderson's 2002 inquiry report stating that the ministry had also neglected a 1999 report which warned that the MAFF would be overwhelmed by an outbreak ("County Verdict," 2002).

Epilogue

Retrospective looks at Foot and Mouth found that the damage was not as extensive as predicted. In Cumbria, only two of the farms in the area were out of business. The Economist ("Disaster that Never Was", 2002) explains that though the Cumbria region of England was heavily impacted, "...the county seems to have come through the epidemic much better than expected." It goes on to say that although the economy of the area was expected to fall, the unemployment rate actually fell 8%. Ananova

notes that exporters had experienced minimal disruptions as of June 2001 ("Most Exporters," 2001). Though the tourism industry reported a swift downturn in the summer of 2001, reports became much direr from that industry following September 11, 2001. By 2002, tourism in the Cumbria region was returning to normal levels according the Economist, though that industry had suffered more damage ("The Disaster That Never Was," 2002).

Another development is that the Ministry of Agriculture Fish and Food has changed its name to Department for Environment, Food and Rural Affairs, or DEFRA. DEFRA currently hosts an informative website dedicated to Foot and Mouth information, prevention, protocol, crisis management and contingency planning[3].

4.3 Anthrax Attacks, Fall 2001

In October and November 2001, on the heels of the September 11th attacks, deadly Anthrax contaminated the United States mail system. A series of Anthrax laden letters circulated through the U.S. Postal Service finding their way to media outlets, government entities, and businesses. Table 4.3-1 below lists some specific targets. The attacks also caused significant delays within the postal system in the affected regions.

Table 4.3- 1 Specific Anthrax Targets

Target	Type	Location
New York Times	Media Outlet	New York, NY
NBC	Media Outlet	New York, NY
American Media Inc.	Media Outlet	Florida
Supreme Court	Government Entity	Washington, DC
Department of Agriculture	Government Entity	Washington, DC
Senate Offices	Government Entity	Washington, DC
Microsoft	Businesses	Phoenix, Arizona

[3]DEFRA's foot and mouth website can be found at http://www.defra.gov.uk/footandmouth/

Disease Characteristics

Anthrax is a man-made biological agent. There are three ways for Anthrax to enter the body; through the nose (inhaled), through a cut or wound (cutaneously), or via the stomach (ingested). Once Anthrax spores enter the body, they begin to multiply, although multiplication can be delayed for up to two weeks. Cutaneous exposure first appears as a lesion on the skin. Symptoms of inhaled exposure include cough, fever, muscle aches, vomiting and fatigue, which can give way to breathing problems and meningitis. Once advanced symptoms appear, the victim usually dies within 36 hours. There are three available antibiotics which are effective against Anthrax, although the inhaled form must be treated at an early stage, while the cutaneous form cannot be treated until lesions appear. The effectiveness of inhaled Anthrax depends on the weight of the spores, as lighter spores can travel further in the air than larger ones. Though the disease is not contagious, very fine airborne spores could infect multiple people at once.

Direct Effects

The effects of the Anthrax attacks were immediately felt by the US Postal Service. Following the attacks, postal workers "expressed fear, confusion or frustration," (Janofsky & Chen, 2001). Post Offices or service centers that were exposed to Anthrax were closed for investigation and decontamination. Many post offices adopted gloves for mail handling as well as increased inspections to isolate suspicious packages. Though this created a safer environment, it caused a backup in mail delivery. Indeed, when a sorting center in the Washington DC area was closed because of contamination, businesses suffered as some zip codes did not receive mail for up to a week.

The mail delays had ripple effects throughout industry. Mortgage, credit card lenders and utilities such as Potomac Electric Power Company (PEPCO) were forced to waive late fees as paid bills remained stuck in the mail system. Likewise, commercial Real Estate broker Julien J. Studley saw commission checks delayed for days and as a result advised employees to mail from their residences (Irwin, 2001). Similarly,

Princeton University waived penalties for late applications as their mail was heavily delayed by Anthrax exposure at a nearby Hamilton New Jersey mail processing center.

In addition to the slowdown within the post office, mail rooms across U.S. were affected. As businesses attempted to implement more detailed inspections, they felt the effects in both costs and delays. DuPont, for instance, spent over $200,000 on portable x-ray machines and explosive detection systems for explosives and agents (Foust & Khermouch, 2001). At New York real estate firm Cushman and Wakefield, similar increased scrutiny in the mail room resulted in four hour delivery delays. Rerouting also caused problems. In the Washington DC area, Covad Communications saw courier fees rise from $10 to $50 as the Federal Communications Commission (their document destination) diverted mail to Capitol Heights (Irwin, 2001). Similarly, Microsoft, who received contaminated mail in a Nevada office, centralized all mail opening in its Redmond, Washington office, causing increased delays.

Direct Mail Industry

Beyond the businesses that rely on mail to support functions such as accounts payable, accounts receivable, or document sharing, lie the firms whose business is the mail, Direct Mail companies. The Anthrax scare of 2001 prompted these businesses to rethink the use of their primary distribution and promotion channel, the mail system. In 2000, about $44 million was spent to sell $528 billion of goods through direct mail (Elliot, 2001). Companies such as Publishers Clearing House increased security at printing facilities, while Nextel wireless altered their direct mail campaign to use postcards in lieu of envelopes. Prior to the Anthrax scare, one strategy to get recipients to open direct mailings was to not print a return address or vendor name on the envelope. In the wake of the attacks, this type of envelope was avoided by recipients, prompting the direct mail association to recommend that return addresses and vendor names appear clearly on envelopes. Although some ignored the advisory hoping that the situation would pass, others like democratic party direct mailer Hal Machow chose to follow the advisory and steer clear of handwritten-looking letters

(Mayer & Stern, 2001). Nissan North America was forced to discontinue an ill-conceived promotional mailing marked "Rx" and containing a prescription bottle. A number of recipients complained about the mailing, whose purpose was mean to promote their new car model Altima as the "cure for the common car." The campaign was stopped with over 52,000 pieces unsent (Maynard, 2001).

Epilogue

In all of this we are reminded of a supply chain design tradeoff, security versus efficiency. The anthrax scare brought about the need for greater security in the mail system design. However, this security came at the price of the speed, ease and competence of the system. Further, the direct mail example illustrates that design changes may be motivated by renewed public opinion or concern. This means that supply chains should remain flexible enough to absorb shifting requirements.

The perpetrator(s) behind the 2001 Anthrax attacks remain at large as the government continues its investigation. In total, 20 people would suffer from Anthrax exposure in the U.S. from September through November of 2001, and the agent would claim the lives of five people.

4.4 Severe Acute Respiratory Syndrome (SARS), Spring 2003

In the course of producing this document, a highly contagious and fatal respiratory disease has slowly crept up on the world population. Severe Acute Respiratory Syndrome (SARS) was identified by the World Health Organization on March 15, 2003. It bears an eerie resemblance to the Spanish Flu in that it has struck during the U.S. war with Iraq, thus initially taking a secondary position to war headlines. Although the disease is currently being investigated, and thus information is incomplete, the effects of SARS are already rippling through global trade and tourism.

Disease Characteristics

SARS' primary symptoms are high fever, coughing and shortness of breath. Though these symptoms are also associated with cold and flu, SARS leads to an 'atypical' pneumonia, which occupies the lower lobes of the lung. Secondary symptoms that may appear include headache, muscular stiffness, loss of appetite, confusion, rash and diarrhea. Within a week, the majority of patients recover, while the rest deteriorate. These people often require intensive care or mechanical respirators. The ability of a patient to recover is determined by his or her immune system's ability to fight off the infection. Doctors have determined that SARS is a coronavirus, commonly linked with the less deadly cold. There is currently not a cure for SARS, and its cause is unknown. As of April 30, 2003 there more than 5600 confirmed cases and 372 deaths resulting from SARS around the globe. Table 4.4-1 breaks down the cases by country.

Table 4.4- 1: Worldwide Confirmed SARS Cases as of April 30, 2003

Country	Cumulative number of case(s)[2]	Final status/ Number of deaths	Final status/ Number recovered[3]	Date of last report
Australia	4	0	3	30/Apr/2003
Brazil	2	0	2	24/Apr/2003
Bulgaria	1	0	0	24/Apr/2003
Canada	148	20	87	30/Apr/2003
China	3460	159	1332	30/Apr/2003
China, Hong Kong Special Administrative Region[5]	1589	157	791	30/Apr/2003
China, Macao Special Administrative Region	1	0	0	30/Apr/2003
China, Taiwan	78	1	25	30/Apr/2003
France	5	0	1	21/Apr/2003
Germany	7	0	7	30/Apr/2003
Indonesia	2	0	1	30/Apr/2003
Italy	9	0	4	30/Apr/2003
Japan	2	0	0	30/Apr/2003

Kuwait	1	0	1	20/Apr/2003
Malaysia	6	2	3	30/Apr/2003
Mongolia	6	0	3	30/Apr/2003
Philippines	4	2	1	28/Apr/2003
Republic of Ireland	1	0	1	24/Apr/2003
Republic of Korea	1	0	0	30/Apr/2003
Romania	1	0	1	22/Apr/2003
Singapore	201	24	139	30/Apr/2003
South Africa	1	0	0	9/Apr/2003
Spain	1	0	1	24/Apr/2003
Sweden	3	0	2	23/Apr/2003
Switzerland	1	0	1	21/Apr/2003
Thailand	7	2	5	30/Apr/2003
United Kingdom	6	0	6	30/Apr/2003
United States	52	0	not available	29/Apr/2003
Viet Nam	63	5	53	28/Apr/2003
Total	**5663**	**372**	**2470**	

Notes: Cumulative number of cases includes number of deaths.
As SARS is a diagnosis of exclusion, the status of a reported case may change over time. This means that previously reported cases may be discarded after further investigation and follow-up.

1. The start of the period of surveillance has been changed to 1 November 2002 to capture cases of atypical pneumonia in China that are now recognized as being cases of SARS.

2. A decrease in the number of cumulative cases and discrepancies in the difference between cumulative number of cases of the last and the current WHO update are attributed to the discarding of cases.

3. Includes cases who are "discharged" or "recovered" as reported by the national public health authorities.

4. National public health authorities report to WHO on the areas in which local chain(s) of transmission is/are occurring. These areas are provided on the list of Affected Areas .

5. One death attributed to Hong Kong Special Administrative Region of China occurred in a case medically transferred from Viet Nam.

Source: World Health Organization; April 30, 2003
http://www.who.int/csr/sarscountry/2003_04_30/en/

Spread of the Disease

Initial Cases of SARS were identified in China, Hong Kong, Indonesia, Philippines, Singapore, Thailand and Vietnam. The current global economy requires travel by air, especially in Southeast Asia, characterized by island nations. Airplanes assist in the spread of the disease as they are tightly enclosed spaces with recirculated air. In addition to spreading via airplanes, SARS spread within hospitals and among hospital workers where the disease arrived prior to identification. While some strains of SARS can only be contracted through close physical contact, other strains are believed to be airborne and highly infectious. These strains can contaminate an object possibly for hours and thus spread the disease through elevators, handsets, keyboards. "This disease is more infectious than we thought," said Singapore Health Minister Lim Hong Kiang, warning that each "superinfector" with SARS could infect 20 to 40 people. (Richardson, Borsuk, &Chang, 2003).

Crisis Management

The first cases of SARS were detected in China as early as November of 2002. However China was reluctant in reporting the outbreak and its details until March of 2003. Only recently has China agreed to allow health officials to enter the country and study its cases. This suppression of information facilitated spread of the disease through unsuspecting carriers and ultimately lead to a greater panic. Although Hong Kong was forthright with its information, it remained relaxed about restrictions and concentrated on downplaying issue to safeguard its economy. For instance, Hong Kong only closed schools where SARS appeared. These actions have created mistrust of government according to the Wall Street Journal ("The Singapore Model," 2003). Singapore in contrast closed all schools and imposed quarantine with the threat of a fine on those who come in contact with potential victims. Also, Singapore set up specific SARS hospitals where the disease is treated, in order to limit spread in hospitals. According to Asian Market Research ("SARS, Thailand, Business", 2003), when the World Heath Organization declared Singapore 'SARS Free' this message was not echoed by leaders in the country for fear of relaxed attitudes among its citizens.

The World Health Organization has issued travel warnings specifically warning against travel to Hong Kong and Guangdong provinces of China and briefly travel to Toronto Canada. The WHO has also worked with airlines on in transit procedures.

New York City is counting on its early detection system to allow them to identify a SARS outbreak quickly. Formally called the New York Syndromic Surveillance System, it performs advanced statistical analysis on various data from the city including 911 calls, pharmacy prescriptions, over the counter drug purchases, emergency room visits and attendance at government agencies and schools. The system concludes whether there are any patterns or abnormalities that are statistically unexpected. In 2002, the system successfully detected early signs of the Norwalk-type virus similar to the one that plagued cruise ships, thereby preparing medical professionals to treat the affliction (Perez-Pena, 2003). In October of 2002, the first National Syndromic Surveillance Conference was hosted by the New York Academy of Medicine, the New York City Department of Health, and the Center for Disease Control and Prevention to discuss creating a national system similar to New York's.

Mask Culture

Since the onset of the disease, the SARS outbreak has already had a detrimental impact on people, businesses and the tourism industry in the affected regions. In Southeast Asia, a mask culture has already taken effect. There has been a burst in demand for regular masks and N95 masks, which block smaller particles. Masks are also becoming accessorized as they meld into daily life in China and Hong Kong.

High Technology and Manufacturing

In March 2003, when the disease was first detected by the World Health Organization, many predicted the devastation of manufacturing in South East Asia and high tech companies, many of which source operations in that region. The New York Times (Bradsher, 2003) estimated that nearly 1000 multinational companies have created regional headquarters in Hong Kong alone while Forbes (Flannery,

2003) named China as the number two producer of computer hardware in 2002. Fear of the disease wreaking havoc is based on the small enclosed dormitories that serve as housing for many factory workers,. For instance, according the Wall Street Journal on April 3 2003, digital consumer technology analysts warned that "the illness could cause serious manufacturing disruptions, schedule slippages, and transportation delays that could derail the global tech industry." Similarly, on April 7, 2003 Boston based Aberdeen Group research expressed fears of a "nuclear winter" for the semiconductor and electronics industries, though it stated that these industries were currently in a "cautionary stage" (Murray, 2003). Though these fears are well founded, and operations have been affected by the outbreak, the expected 'serious disruptions' have yet to pass. In fact, Business Week (Einhorn, Engardio & Shari, 2003) contends that there have been "virtually no reports of factory slowdowns or delayed shipments in the five months since the SARS outbreak began." Further, a survey conducted by the Singapore Confederation of Industries showed that the effects on that country's manufacturing sector have been mild in comparison to travel and tourism (Khalid, 2003). In addition, Computerworld (Roberts & Evers, 2003) report that IBM and Home Depot, both of whom have offices in the region, have not witnessed any supply chain disruptions or effects.

For most, the actual impact has been changes in operational procedures to contain the spread of the disease, and travel restrictions to isolate the problem in the regions where SARS been detected. Below are some examples that demonstrate the effects that manufacturing companies and the high tech sector have felt.

When a Motorola factory worker was diagnosed with SARS in Singapore, the government ordered the 305 factory employees into quarantine. This halted production for at least one shift there, but operations were back on line the following day (Murray, 2003).

Intel Corporation cancelled two major conferences scheduled to be held in Taipei and Beijing. The shows were expected to draw 1500 attendees to discuss innovations in

chip design. Further the company closed an entire floor of its Hong Kong Sales and Marketing office when a worker appeared to have symptoms of SARS. However, this closure lasted only one day, and operations returned to normal. Business 2.0 (Hellweg, 2003) spoke to a local spokesperson at the semiconductor manufacturer who attributed its resilience to "strong supply chains and business-continuity plans."

Travel restrictions by US companies with operations in South East Asia have become common. Companies such as Home Depot, IBM, and Nokia have restricted travel to that region. Since orders are often made up to three months in advance of production, some manufacturers fear that the effect will present itself in the form of fewer orders in the next production cycle, despite the lack of difficulties delivering orders in this cycle. The Wall Street Journal (Buckman, 2003) describes a small Hong Kong toy manufacturer, Color Rich Ltd., that has seen very few orders because their buyers are no longer traveling to the region. Buckman describes how small toy retailers ordinarily place Christmas orders during the spring, but have not because of SARS. Tom Conley, President of the 250 member Toy Industry Association, describes that the toy industry relies on in person buying to ensure correct colors and parts, and that travel restrictions could have a harmful effect on retailers who do not make the trip (Buckman, 2003). For larger toy companies and their suppliers this is less of an issue as companies like KB Toys, Wal-Mart Inc. and Toys 'R' Us placed holiday orders well before the outbreak. These companies have also begun to rely on overnight deliveries to exchange samples and prototypes. All of these large retailers describe smooth operations since the outbreak and expect to meet holiday deadlines.

In the banking industry, quarantine programs were implemented. Swiss Bank UBS is requiring its employees in Asia to return and remain at home for 10 days to ensure that the disease is not incubating and potentially affecting the European office. JP Morgan has implemented a similar program requesting that those in Asian offices alternate weeks in the office and at home, staggered among offices.

Similarly, Hong Kong & Shanghai Banking Corp. (HSBC), a high end bank and lender, was forced to temporarily close its doors when a teller was diagnosed with SARS. In the following days, four more employees were diagnosed, prompting HSBC to reduce operations and send employees in contact with those affected home for diagnosis. The company also sent 50 bond traders home to wait out the incubation period as a precaution. With a clean bill of health, these workers will operate a back up facility, which can provide ongoing operations if the main facility requires closure.

Tourism and Entertainment

As noted above, SARS prompted travel restrictions to Asia by many multinationals with operations there. This, coupled with quarantines and fear of contracting the disease, has greatly affected the travel, tourism and entertainment industries in Southeast Asia.

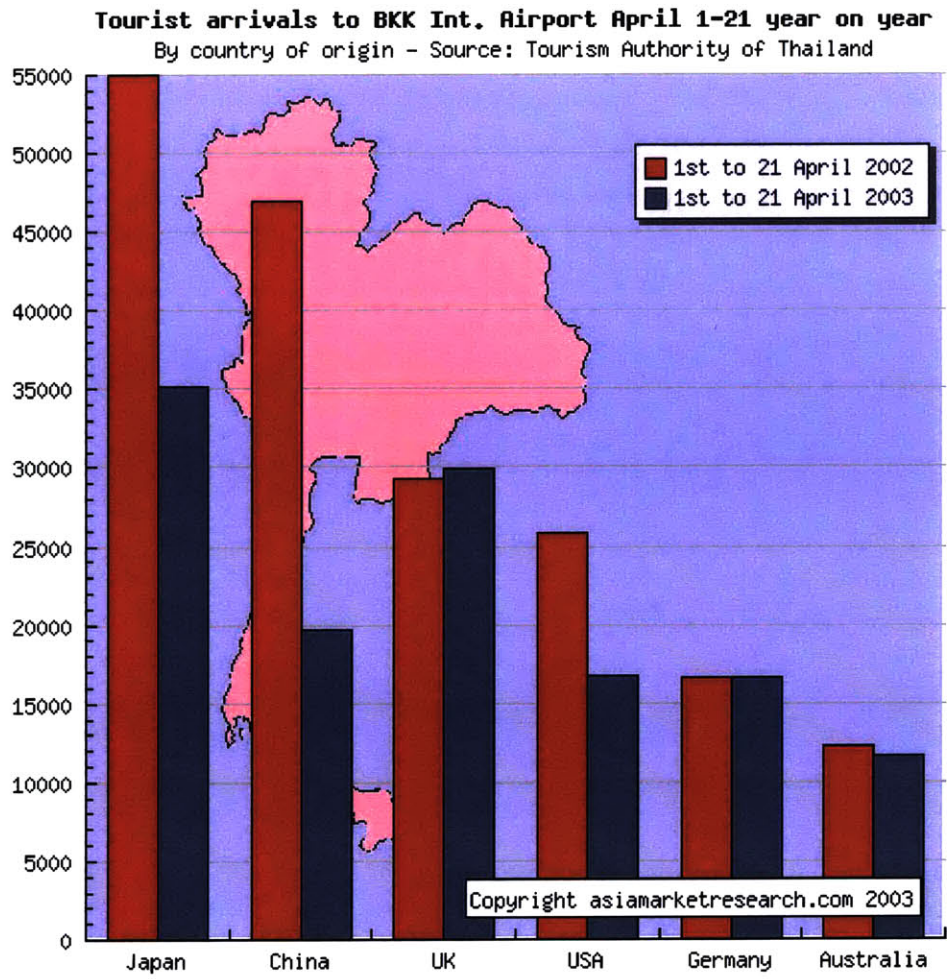
A number of airlines have cut routes and service to Southeast Asia since SARS struck. In the U.S. airlines have reduced service to Asia. Continental Airlines has resorted to extremes and cut all flights to Hong Kong due to lack of demand (Einhorn, et. al., 2003). Asian airlines were hit especially hard including Quantas, Singapore Airlines, Malaysian Airlines, Korean Air, Japan Airlines and Cathay Pacific. The Australian (Korporaal, 2003) reports that together, these airlines have "suspended more than 300 services in the region." Korporaal also discusses a memo leaked at Cathay Pacific airlines noting that passengers had fallen from 39,000 to 7000 per day, an 82% decline, and that the airline was considering grounding its fleet. On April 10, Cathay declared that it would cut 40% of its flights indefinitely and issued a profit warning along with it.

In Hong Kong, for example, tourists contributed more than HK$64 billion (US$8.2 billion) to the economy in 2001. "In Hong Kong, the SoHo restaurant district, usually crowded with breakfasting expatriates and tourists on Sunday mornings, was thinly populated," (Richardson, et al, 2003) Entertainment was also affected as scheduled

concerts by the Rolling Stones, Moby and Santana have been cancelled or postponed. Similarly, four first-round soccer qualifying matches for the 2004 Olympics scheduled in Taiwan, Singapore, Hong Kong, and Sri Lanka were postponed.

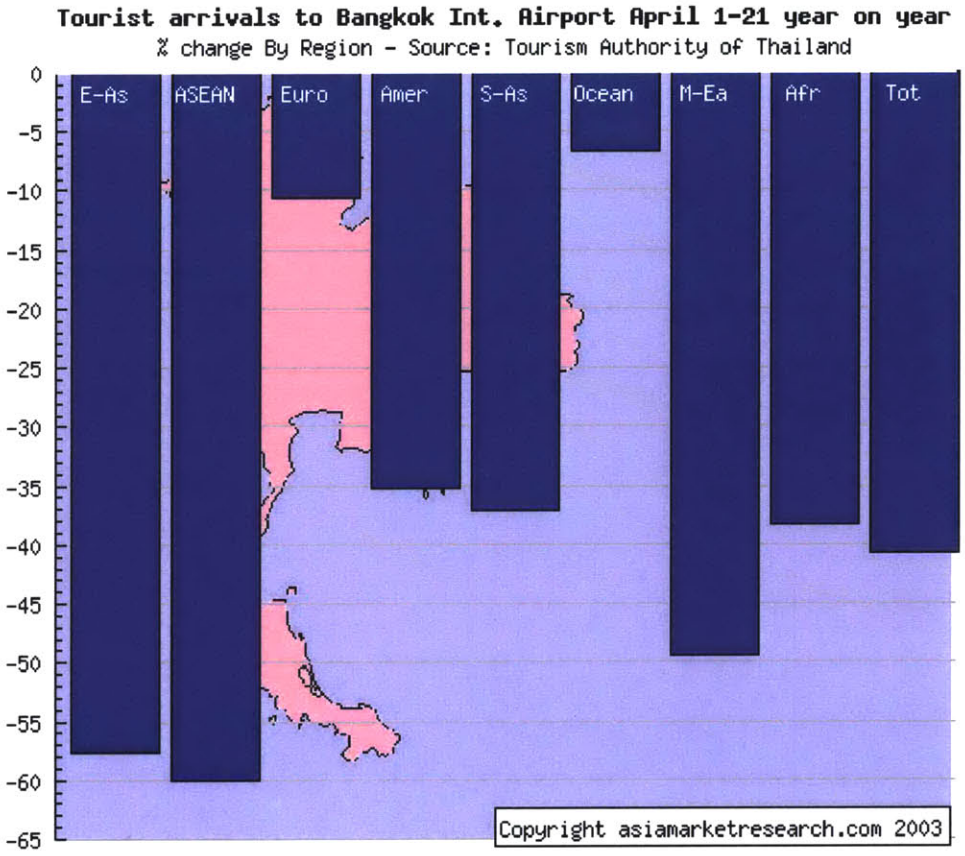
Thailand, who relies heavily on its tourism industry, has seen a significant drop in its visitors. Asian Market Research performed a study on travel to Don Muang International Airport in Bangkok for the first three weeks in April, which includes the Songkran holiday that usually sparks an influx of visitors. They compared visitor arrivals in 2003 during the SARS outbreak, to arrivals in 2002. Figures 4.4-1 and 4.4.-2 below depict their findings, that there has been a precipitous drop in travel to Bangkok. compared to the previous year.

Figure 4.4-1: Drop in arrivals to Bangkok in April 2003 compared to April 2002.



source: Asian Market Research, May 13, 2003
http://www.asiamarketresearch.com/news/000305.htm

Figure 4.4-2: Drop in arrivals to Bangkok by country during SARS outbreak



source: Asian Market News
http://www.asiamarketresearch.com/news/000305.htm
E-As = Japan, Taiwan, South Korea; ASEAN = 10 states in Association of South East Asian Nations including Singapore, Malaysia, Phillipines and Indonesia; S-As = India, Pakistan, Sri Lanka region; Amer = N. and S. America including US; M- Ea = Middle East; Afr = African Continent

Starbucks Inc, operating 953 coffee shops throughout Asia, closed one shop located in an infected hospital in Singapore. The company is also experiencing a decline in sales in Hong Kong and Singapore, though not in China.

Toronto Canada cancelled the annual meeting for the American Association for Cancer Research, turning back 16,000 worldwide attendees. A local tourism group

estimated the tourism loss as a result of SARS to be from C$15 million to C$20 million (Curren, 2003).

5.0 Chemical Events

Chemical Weapons are not a new concept. Indeed, Chlorine based gases were employed in World War I, Mustard gas was used in World War II, and a variety of chemical agents were used by Iraq in the Iran-Iraq war of the early eighties. Chemicals have also been used as weapons off of the battlefield. In March of 1995, a Japanese cult terrorist group attacked the Tokyo subway with deadly Sarin gas causing 19 casualties and thousands of hospitalized injuries. Soon after, the group responsible for the attack, Aum Shinri Kyo was discovered with an arsenal of Sarin and plans to attack Disneyland in Los Angeles, California.

Chemical attacks pose a considerable threat since crude poisons such as Sarin can be made with common household items such as cleaners. This level of accessibility means that even the most fragmented of criminal and terrorist groups have the capability to produce and use a weapon of this sort.

Chemical weapons are commonly divided into two categories, harassing weapons and casualty weapons. Harassing chemicals are not fatal, but bothersome enough to prompt the victim to remove a gas mask. These could be tear, sneeze or vomit gases. Casualty gases cause severe trauma and possible death. They include choking gases, blistering gases, blood gases, and nerve gases. Persistent agents will linger for a long period, while a Non-persistent agent will dissipate quickly.

In recent times, nations have considered the use of chemical weapons a viable threat. In fact, at the time of this thesis, the United States is currently engaged in a war with Iraq, to rid the latter of its purported chemical and biological weapons of mass destruction. Although this war is on the wane, the US forces continue to search for chemical and biological arsenals.

In the following section, this thesis considers not a gas attack, but an accidental gas leak. The events that took place in Bhopal India in December of 1984 provide useful insight into preparing for and reacting to a disruption of this sort.

5.1 Union Carbide Chemical Leak Bhopal, India, December 1984

On December 3 1984, a Union Carbide plant in Bhopal, India leaked a poisonous gas throughout the town and surrounding areas. It would come to be known as the worst industrial accident to date, injuring 200,000 and claiming the lives of 2000 (Diamond, "Workers Recall Horror", 1985).

Background

The Union Carbide India Ltd plant in Bhopal, India produced the pesticide Savin and was 50.9% owned by U.S. parent company Union Carbide. Just after midnight on December 3, 1984, water entered a tank of poisonous liquid Methyl Isocyanate (MIC) causing the temperature and pressure of the tank to rise. At this point some safety systems failed to operate, and liquid chemical began to vaporize and escape through an improperly shut vent, creating a deadly cloud of gas. The plant attempted to contain the gas by burning it off with a flare, but the flare also malfunctioned. An alternate containment measure was to direct the gas into an empty tank, however no tank was available. The cloud began to drift away from the plant and toward the nearby neighborhoods.

The chemical Methyl Isocyanate is more toxic than cyanide and caused violent and horrifying deaths in the people it killed. The agent simulates drowning in the lungs and causes severe nerve damage. Because of the late hour, many died in their sleep, but others were killed in their tracks amidst the chaos outside the plant as people were running in all directions. Lerbinger (1986) suggests that Union Carbide failed to educate the area regarding the dangers of the plant and how to react in an emergency situation. Indeed, the knowledge to apply a simple wet cloth over the mouth or run in the opposite direction to the wind would have saved hundreds from death and injury.

Following the disaster, investigations were initiated to understand the underlying causes of the incident. As concerns were revealed, Union Carbide and its Indian subsidiary began to point fingers. One issue that was raised was training. Workers admitted to noticing an issue, but deciding to address it after a tea break. Further, many of the workers on duty that night did not meet the required training level for their posts. In addition, many workers felt that they were not aware of the toxicity of MIC or the potential hazards of a leak. There is speculation (Lerbinger, 1986, p13) that two on duty technicians fled the scene instead of hosing down the tank, which could have ameliorated the problem. Another issue raised regarded safety equipment and measures in the plant. As stated above, some equipment integral in handling Methyl Isocyanate was faulty or broken. Likewise, the detection system for monitoring MIC temperature was set too high and thus found the problem too late. Finally, the plant did not have a computerized leak monitoring system that was available in similar Union Carbide plants. As these factors emerged, the parent company began to distance itself from its Indian subsidiary, claiming that "noncompliance with safety issues is a local issue," (Fink, 1986, p178).

Union Carbide's actions following the Bhopal crisis are considered text book examples of how not to manage a crisis. Their reaction was characterized by denial, finger pointing, and misinformation. Indeed, Fortune magazine (Kirkland, 1985) reported that UC lacked a comprehensive plan to manage a "catastrophe of this magnitude,".

Prior Warnings

During the investigations into the 1984 accident, a report was revealed that was filed in 1982 by the parent company and found critical safety issues in the Bhopal plant warning of "a serious accident or more serious consequences," (Diamond, "How it Happened", 1985). The report made recommendations to replace old or broken systems including a central safety device that could have assisted in controlling the

1984 incident. The report also was the result of a cursory inspection which was never followed up by a more comprehensive assessment, despite the alarming findings.

The Bhopal plant was also the sister plant to a Union Carbide plant located in Institute, West Virginia. As the Bhopal safety issues emerged, the Institute plant was temporarily shut down for a five month $5 million safety retrofit. Indeed, the chairman of Union Carbide testified before congress that a similar accident at the West Virginia plant was unthinkable, while the UC director of Safety, Health and Environmental affairs, Jackson Browning, called the Institute plant "absolutely safe," (Fink, 1986, p181).

To the disbelief of many, the Union Carbide Institute, West Virginia plant experienced a toxic gas leak on August 11, 1985, just eight months after Bhopal. 135 residents in the surrounding area were treated for exposure. The newly installed multi-million dollar detection system was not programmed to detect Methyl Chloride, the toxic gas that was released. An investigation into the cause conducted by Union Carbide found that plant had ignored computer, temperature and pressure alarms and had failed to fix broken equipment.

Human Effects

As stated above, 2000 people died from the leak at Bhopal. However, those that survived continued to suffer the effects of exposure including breathing, sleeping, vision, and digestion problems. The number affected varies from Government reports of 5,000 to 10,000 to health groups reporting 50,000 affected (Weisman, 1985, "Disabling and Incurable"). Indeed, counts of deaths and injuries vary greatly due to the impoverished conditions of the area and the likelihood of diminished reporting of occurrences.

Epilogue

In 1985, one year after the fatal gas leak, Union Carbide had been devalued by $900 million. At that point, over 4000 jobs had been eliminated and UC had taken a $1B

write-off. In February of 1985, Stuart Diamond completed his award winning four part series in the New York Times with a description of lessons learned from the tragedy. Diamond discussed the cultural challenges related to technical and potentially hazardous operations in a third world country. He cited the need for special training, public education, a sense of urgency regarding safety, regard to cultural differences, and an emphasis on preventative maintenance ("Lessons for the Future," 1985).

Ultimately, Union Carbide paid a settlement of $470 Million to the Indian Government in 1989. In September of 1994, parent Union Carbide sold its stake in the Indian subsidiary. In 1999, Union Carbide merged with Dow Chemical taking the latter's name. The Wall Street Journal reported on May 8, 2003 that Bhopal survivors continued to pursue Dow Chemical regarding proper compensation for survivors and their families.

6.0 Radiological Events

Although the Cold War is over, the threat of nuclear attack remains. In 1998, Pakistan and India made their nuclear power known as they tested their weapons to a world audience. In late 2002 and early 2003, North Korea also raised concerns as it restarted its nuclear program. However the threat lies beyond countries with nuclear weapons programs, as these nations participate in world politics and also have a substantial amount to lose by launching such an attack. A new type of hazard exists in the release of radioactive material through what have been coined dirty bombs.

A dirty bomb is an explosion set off by traditional explosive materials, but that contains radioactive material which can spread over and affect the targeted area. This is in contrast to a nuclear weapon in which the explosion is caused by a nuclear reaction and can cause a greater blast and much more damage. Time Magazine (Karon and Thompson, 2002) asserts that a nuclear bomb would require nearly a decade and considerable infrastructure to develop. A terrorist group that relies on its fragmentation is thus unlikely to develop a nuclear weapons program. Radioactive materials are also widely used in medical, agriculture and industrial applications, while weapon grade plutonium or uranium is again difficult to obtain. With this in mind, a dirty bomb becomes a more manageable situation. Though a dirty bomb's destruction remains dependant on the extent of its blast, the fear incited by the threat of radiation to the public effectively accomplishes a terrorist's goals. Thompson (2002) asserts "It's ultimately a pure terror weapon." In May of 2002, a suspected Al-Qaeda terrorist in the United States was charged with plotting to build and set off a dirty bomb (Council on Foreign Relations, 2003).

The blast and heat from a nuclear weapon are the initial direct effects of a nuclear explosion. The blast itself causes air shockwave injuries while the intense heat causing first and second degree burns in up to a 25 mile radius. Flash Blindness can also occur as a result of the intense flash of light or permanent blindness from thermal radiation. Great exposure to radiation can cause a myriad of health issues, including accelerated cancer.

In the following section we study one area devastated in recent years by a nuclear accident. This allows us to understand the effects of a nuclear or radiological incident to the supply chain.

6.1 Nuclear Accident at Chernobyl, Ukraine, April 1986

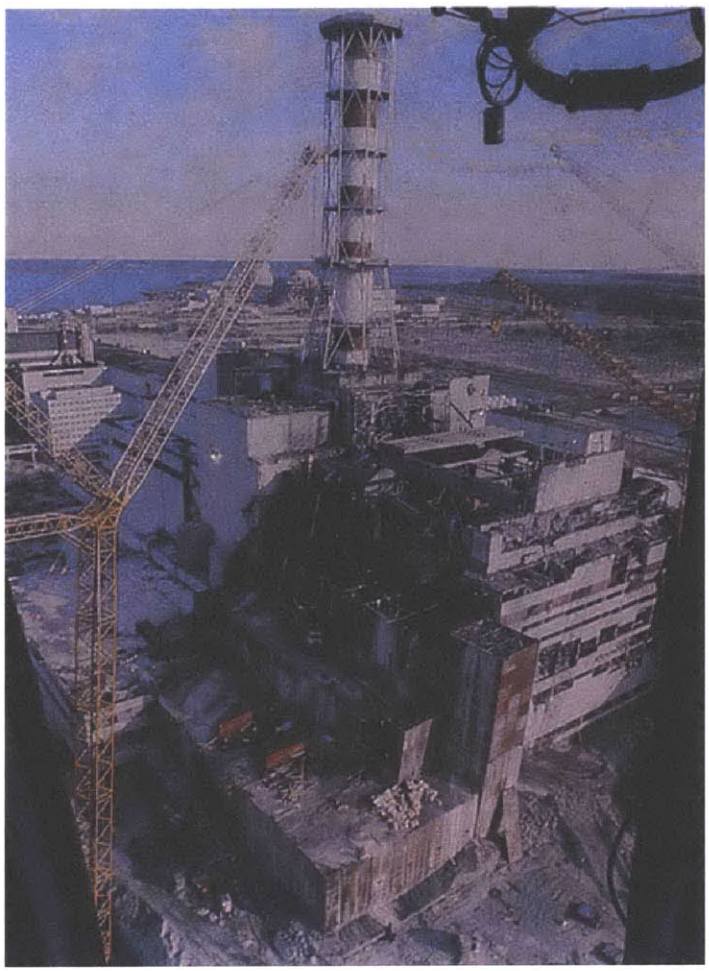
On April 26, 1986 the Chernobyl Nuclear Power Plant suffered the worst nuclear accident in history. Reactor 4 experienced a chain reaction causing two great explosions followed by a graphite fire that would direct radioactive winds as far reaching as Western Europe. The Chernobyl accident directly resulted in loss of life and the devastation of the area, and indirectly damaged the agriculture and energy supply chains.

Sequence of Events

Late in the evening on Friday April 25, 1986, the Chernobyl Nuclear Plant (NPP) located in Chernobyl, Ukraine shut down Reactor 4 for maintenance and plant testing. During this maintenance power was reduced to a lower but operational level of 700 megawatts in order to conduct tests.

Instead, the power level suffered a precipitous drop to 30 megawatts, which set off a sequence of steps to stabilize and maintain power, some of which endangered the protection system of the reactor. Eventually, these steps caused power to increase by a factor of 30. This increased the temperature and caused steam and pressure to accumulate. Eventually the steam forced an explosion destroying the core and blowing off its shield, weighing in at 1000 metric tons. Figure 6.1-1 depicts reactor 4 after the explosion.

Figure 6.1- 1: Exposed Chernobyl NPP Reactor 4 after the explosion.



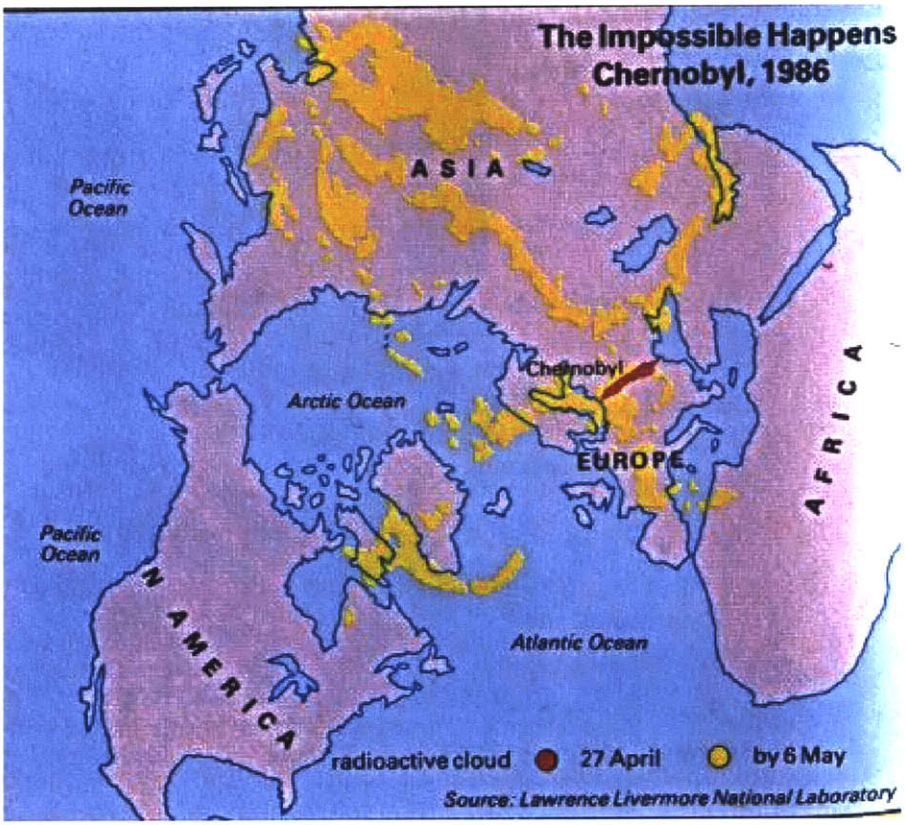
source: Chernobyl.com
http://www.chernobyl.com/chernobylreactorcolor.jpg

"The explosion exposed the core directly to the atmosphere and sent a plume of hot and highly radioactive particles, smoke, and building debris into the air," (Bar'yakhtar, Poyarkov, Kholosha, & Shteinberg, 2000, p13). The explosion also set off a number of fires, including a dangerous fire fueled by highly pure graphite, which firefighting teams had great difficulty controlling. Bar'yakhtar et. al (2000) contend that "There is very little experience—anywhere in the world—fighting graphite fires involving high radiation and radioactive contamination." Indeed, the graphite fire burned for 14 days and was finally extinguished on May 9, 1986.

The radioactive plume of smoke emitted from the fire traveled Northwest across Ukraine, Belaros and Russian territories. It reached great distances and radiation was

detected throughout the world. Figure 6.1–2 depicts the affected areas. In fact for many countries, this is how they came to know of the accident. Sweden's radiation detector noted levels 100 times the norm, initiating an investigation that would garner world attention. It was Monday April 28, two days after the incident had occurred. Initially, news from the Soviet Union was sparse and guarded, delivered in curt press releases (Barnathan, Strasser, Barry & Cook, 1986).

Figure 6.1- 2: Global Radiation Disbursement from after Chernobyl

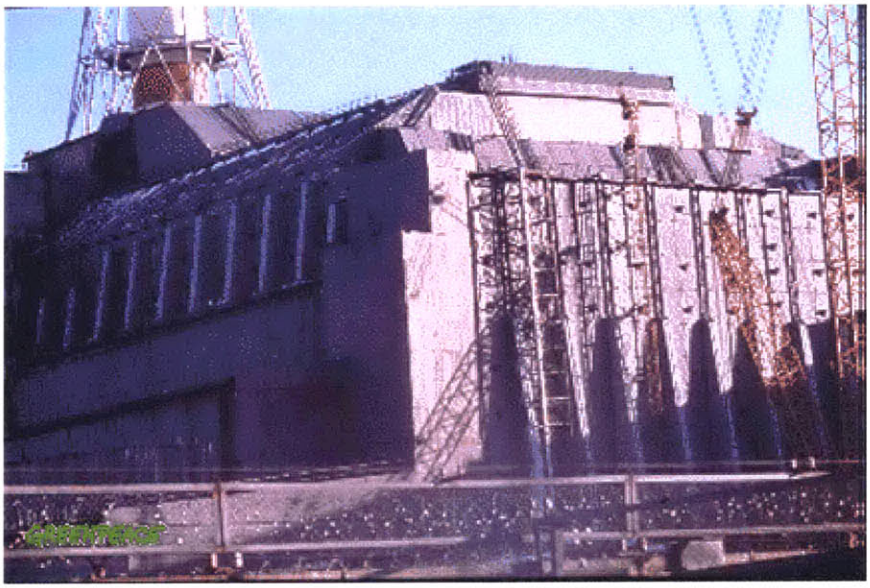


source: Brama.com
http://www.brama.com/ukraine/pics/chrnbyl3.jpg

The graphite fire reached temperatures of 5000°F and burned for thirteen days before firefighting teams could control and extinguish it on May 9, 1986. The fire released nearly 4% of reactive material from the core into the environment. Eventually, a large concrete enclosure was built around the damaged reactor in an attempt to contain radiation. This was coined 'The Sarcophagus' or 'The Shelter' and was sponsored by the Committee of the Soviet Union Communist Party and USSR Council of

Ministers. The 117 construction workers who built the shelter did so despite the heavy exposure to radiation that it required. The shelter began construction in mid-May 1986 and was completed six months later in November of the same year. Figure 6.1-3 shows the reactor after the shelter was built.

Figure 6.1-3: Reactor 4 after the shelter was built



Reactor 4 Chernobyl NPS. Covered with Sarcophagus since accident in 1986.
0.96.07.02.17 DEC 1995
CHERNOBYL UKRAINE D
© Greenpeace/Shirley

source: Greenpeace.org Chernobyl Ten Years After
http://archive.greenpeace.org/~comms/pics/0217.gif

Human Impact

The Chernobyl accident killed about 30 people within five days of the accident, and the Ukraine Radiological ("Chernobyl: Assessment, 2002) institute estimates a total of 2500 deaths. However, the greater human impact was that caused by the radioactive release and resulting exposure to the public. Kholosha and Poyarkov (2000) estimate 200,000 people were exposed to radiation. The plant was located between the towns of Chernobyl and Pripyat on the Pripyat river. The populations of those areas were 25,000 and 10,000 respectively. Perhaps more alarming was the proximity of the city of Kiev, populated with nearly 2 million people and located a

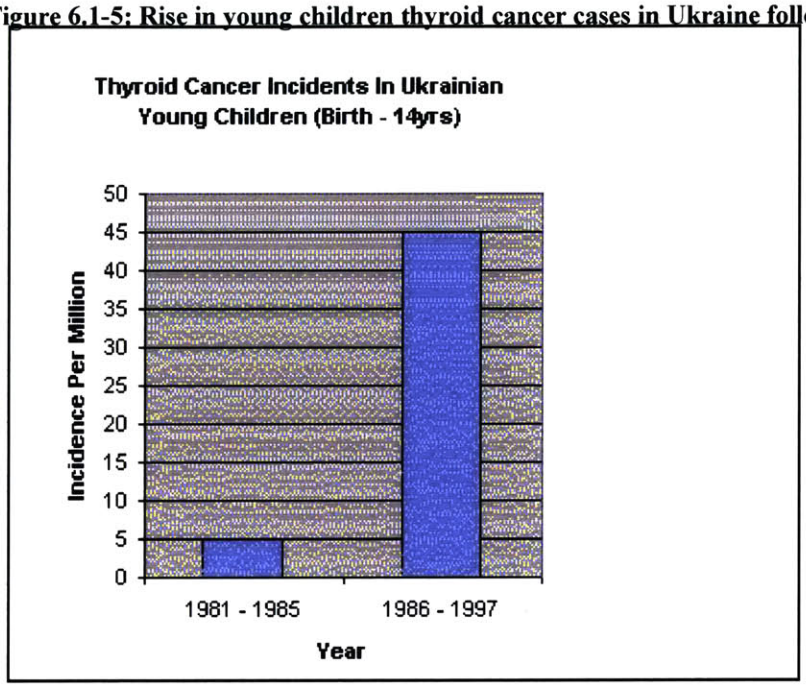
mere 80 miles away. In total, approximately 116,000 people were evacuated and 210,000 people relocated from the area (Visscher). Figure 6.1-4 below depicts the affected areas.

Figure 6.1-4: Local radiation hotspots resulting from the Chernobyl accident

source: brama.com
http://www.brama.com/ukraine/pics/chrnbyl1.jpg

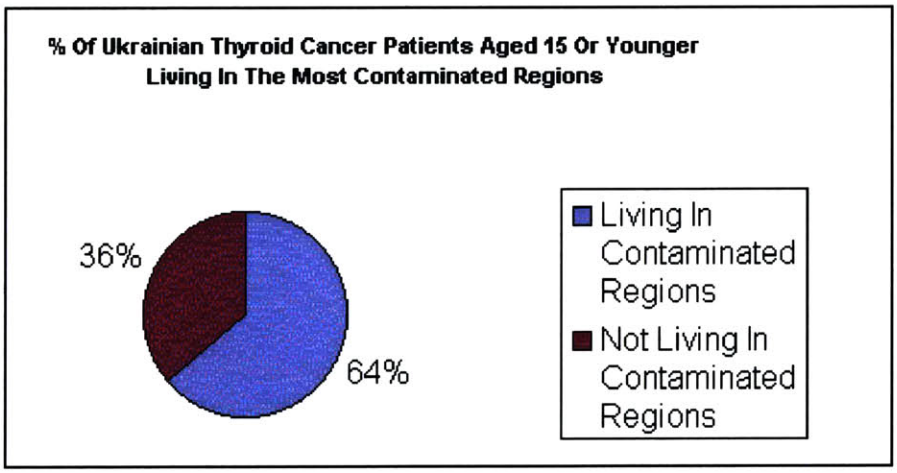
In the long term, the human effects are more disturbing. The area remains a cancer hotbed. Thyroid cancer among Ukrainian children saw a great increase. Indeed according to a study in 1999, 64% of the Ukrainian children suffering from Thyroid cancer lived in the most contaminated regions (Visscher). Figures 6.1-5 and 6.1-6 depict these statistics.

Figure 6.1-5: Rise in young children thyroid cancer cases in Ukraine following Chernobyl accident



Source: Chernobyl.com Health and Psychological Consequences
http://www.chernobyl.co.uk/health.html

Figure 6.1-6: Locations of young thyroid cancer patients in Ukraine regions.



Source: Chernobyl.com Health and Psychological Consequences
http://www.chernobyl.co.uk/health.html

Economic Effects

The direct losses as a result of the accident are estimated by Kholosha and Poyarkov (2000, p210) to be about 9.2 billion rubles (translating to $12.9 million) which was about 30% of the Soviet Economy at the time. Businesses directly affected include a Fleet repair and Operations facility, an Iron Foundry, a cheese plant and a vegetable drying plant in the area.

One difficult disruption was the loss of equipment following the disaster. Thousands of trucks along with a number of bulldozers and helicopters, cars, buses and other vehicles were deemed contaminated and required disposal. The equipment was subsequently moved to nearby waste sites in the area. Figure 6.1-7 depicts a contaminated truck and helicopter storage site in Rozsohka.

Figure 6.1-7: Rozsohka, a site for contaminated trucks and helicopters deemed unfit for use due to radiation exposure.

Rassohka, the biggest storage point for contaminated trucks and helicopters, from Chernobyl.
0.96.07.02.24 DEC 1995
CHERNOBYL UKRAINE D
© Greenpeace/Shirley

source: Greenpeace.org Chernobyl Ten Years After
http://archive.greenpeace.org/~comms/pics/0224.gif

Losses also included those from losing agriculture and forest resources that were deemed unusable from excessive contamination. These were estimated (Kholosha and Poyarkov, 2000, p216) to reach 8.6-8.9 billion rubles ($276-$286 million) from 1986-1991. An estimated ("Chernobyl: Assessment", 2002) 52,000 km^2 of agricultural land was contaminated by the accident. In addition, nearly 15,000 cows were slaughtered in the Ukraine although many were not contaminated to untreatable levels.

Of the 5000 km^2 of forest withdrawn from use, the woodworking industry lost almost 2 billion rubles ($64 million US). These forest lands produced nearly 50% of Soviet resin as well as 6000 tons of sawdust each year. One area of pine trees was nicknamed the 'red forest' after the trees turned a red color from increased exposure to radiation. In 1987 contaminated soil and dead trees were removed in attempt halt the spread of radiation through forest fires.

Another important loss was the reduction in energy production resulting from the downtime of the plant. Kholosha and Poyarkov (2000) estimate that this to be a 20 billion ruble ($643 million US) hit to soviet industry from increased prices due to power shortages.

Crisis Management

As mentioned above, the Soviet Government was slow in releasing information about the crisis at Chernobyl. As the initial radiation was detected by global entities, Moscow remained close-lipped about the incident. Some of this can be attributed to the political setting at the time, deep in the midst of the cold war with Soviet press controlled by its government. Statements were brief and generally downplayed the severity of the blast. This led to confusion for the people in the area. Newsweek's 1986 special report titled Chernobyl Meltdown reported that the though the Soviet Union desperately searched for assistance in controlling the graphite fire, little could be offered given their unwillingness to divulge details of the incident (Barnathan, et al, 2000). The article went on to say that foreign visitors were frustrated that reports

from their home countries presented a direr situation than that described within the Soviet Union.

Epilogue

A thirty mile exclusion zone was created around the Chernobyl Nuclear Power Plant which included Chernobyl and Pripyat. Residents of these areas were evacuated in 1986 and most no longer plan to return. As a result, those cities remain effectively deserted today, save the crews that remain assisting with cleanup. Figure 6.1-8 depicts the town of Pripyat in 1995.

Figure 6.1-8: Pripyat, an evacuated city, ten years after the Chernobyl accident.

The deserted city of Pripyat, Chernobyl nuclear power plant in the background. Ukraine.
0.96.07.01.04 DEC 1995
CHERNOBYL UKRAINE D
© Greenpeace/Shirley

source: Greenpeace.org Chernobyl Ten Years After
http://archive.greenpeace.org/~comms/nukes/chernob/cher01.gif

According to BBC ("Chernobyl 'not so deadly') in 2000, a statement was issued by the International Atomic Energy Agency admitting that the accident was responsible for the rate of thyroid cancer in children in the area but going on to say, "with this

exception, there is no scientific evidence of increases in overall cancer incidence or mortality or in non-malignant disorders that could be related to radiation disorder."

In 2002, 16 years after the disaster, investigations were undertaken to look at long term effects. The sarcophagus remained, although heavily cracked and posing a risk of falling apart. There remained a number of trade restrictions on the agricultural products produced in the region as contamination remained above acceptable levels. Nearly 55,000 hectares are part of the exclusion zone and are forbidden from agricultural farming. (NEA 104).

The Chernobyl Nuclear Power Plant is no longer in use as reactors 1, 2 and 3 were shutdown in 1997, 1999 and 2000 respectively. Plans to dismantle the reactors, including reactor 4 within the sarcophagus, remain under discussion. In April of 2003, Russian and Ukrainian officials agreed that the shelter surrounding the reactor was weak and in danger of collapsing. Ukrainian officials intend to stabilize the current shelter by September 2003, and later in the year begin a project to construct a new shelter to be complete by 2007.

7.0 Cyber Events

Recent advances in supply chain systems such as Just in Time, MRP, Quick Response and ERP all rely on data. Information availability, accuracy and reliability are therefore essential to the effectiveness of today's lean operational environments. Consequently, if data is compromised, so are critical supply chain activities.

The Internet has become vital tool for most businesses to exchange this critical data and connect with partners and suppliers. Information flows from business to business to consumer along a vast network. However, as more information is shared, more information is made available. The rise of technology has unfortunately given way to the rise of crimes which identify and magnify vulnerabilities along that network. Vulnerabilities can exist within a company or along the shared networks that data move across. These crimes are sometimes referred to as cyber attacks.

It is widely believed that one way terrorists will enforce disruption is by attacking our infrastructure in concert with data networking capabilities. By studying cyber attacks and disruptions, we can learn from experiences of affected organizations.

The following sections study recent instances of digital attacks on data networking and infrastructure systems. Section 7.1 considers directed attacks at specific entities such as Yahoo, CNN, the White House and Al-Jazeera. This is followed by section 7.2, which reviews a cyber attack on infrastructure involving a disgruntled water system employee who succeeded in attacking a utility with the computer. Section 7.3 covers email attacks such as Melissa and Love Bug. The final section reviews some computer viruses and worms that spread their dangerous tentacles across the internet and brought digital communication to its knees. These include Code Red and SQL Slammer.

7.1 Directed Attacks on Ecommerce Sites, February 2000

In the world of Cyber Crime and Vandalism, there are many methods and motivations. Some attacks are designed to affect a large number of non-specific

targets and slow down overall communications. These are usually viruses or worms which are considered in section 7.3 through 7.5. Conversely, a directed attack is constructed with a specific target in mind. These attacks are meant to cause problems only for their intended victim(s) and are not built to spread indiscriminately. In this section, we will examine vandalism and denial of service attacks on the US Government, Foreign Media sources, and ecommerce web sites.

Vandalism

The nature of a vandalism cyber attack is meant to deface a web property. It is the equivalent of graffiti on a building. Often times these attacks are initiated with political motivations, and thus their targets are frequently government or media organizations. For instance the White House website, whitehouse.gov, has been attacked on numerous occasions. In May of 1999 for example, the site was shut down for 24 hours following attempts to hack into their system. This was apparently in retaliation for a NATO accidental bombing of the Chinese Embassy in Belgrade. That same weekend, the Department of the Interior, Department of Energy, and the US Embassy in China homepages were all replaced with anti-US sentiments and photographs. Though the public websites of these entities are more or less marketing channels, the attacks highlight the weakness of their networks and the potential for more material damage. As this extrapolates to media companies, the concern is not merely publicity, but advertising revenue as well. In May of 2002, Chinese separatists group Falun Gong hacked into and gained control of television and radio signals in China's Anhui province. The group caused a thirty minute interruption and replaced normal broadcasts with Falun Gong propaganda during that period. Similarly, during the US campaign against Iraq in the March of 2003, Arab Satellite Television network Al Jazeera's English version website was defaced with an American flag.

Denial of Service

A Denial of Service attack is one that seeks to cripple a network by essentially flooding it with messages. The concept is to send many requests to a server or

network and prompt a response from it. This response-acknowledgement system is how typical web based communications are initiated. Though the response is not acknowledged during a denial of service attack, the network becomes bogged down in its attempts to respond. The Washington Post (Shwartz, Cha, & Vise, 2000) explains that a denial of service attack "resembles piling up trash in front of the door so that others can't get in." A distributed denial of service attack (DDoS) goes one step further and unwittingly uses a large number of 'distributed' servers as launch pads for the attack. Essentially, these distributed machines are hacked as well, thus concealing the actual attacker's location. There are many different types of DDoS attack scripts, and most are available on the Internet. Though there are some methods to react quickly to a DDoS attack, or mitigate its effects, it is difficult to entirely eliminate their threat without barring access to your site.

Beyond cyber attacks that affect government and media sites the potential for damage to the bottom line is more strongly illustrated in attacks directed at eCommerce and solely web based entities. In February 2000, a number of high profile eCommerce and media sites were paralyzed by directed DDoS attacks. These sites included Yahoo!, eBay, Amazon, Buy.com, ZDNet, and eTrade, all of whose transactions are entirely web based. A chart listing the attacks and their durations is included in table 7.1-1.

Table 7.1- 1: February 2000 Directed Cyber Attack Targets, Dates and Durations

Victim	Revenue Source	Date	Start	Stop	Duration
Yahoo.com	Advertising	Feb. 7, 2000	10:45 am	1:20 am	2 hr 35 m
Amazon.com	Purchases	Feb. 8, 2000	5:00 pm	6:00 pm	1 hr
Ebay.com	Auctions	Feb. 8, 2000	3:00 pm	6:00 pm	3 hr
Buy.com	Purchases	Feb. 8, 2000	10:00 am	3:00 pm	5 hr
CNN.com	Advertising	Feb. 8, 2000	4:00 pm	5:45 pm	1 hr 45 m

The first attack occurred on February 7, 2000 and was directed at Yahoo.com, an Internet portal. The site's main page was unavailable for nearly three hours as over fifty servers were hacked to launch a DDoS attack against it. The following day, bookseller Amazon.com, auction site eBay, news site CNN.com and electronics site Buy.com were all attacked in a similar manner. Buy.com was struck first with

network traffic levels growing eight times above the acceptable maximum (Kirby, 2000). This coincided with the site's initial public offering that morning, hampering related activities, but not directly affecting the IPO. eBay was down for nearly two hours and was forced to offer its customers credit if an auction was materially affected. The following day, technology news site ZDNet and online broker eTrade were attacked. The attack spanned over an hour, and occurred at the opening of the trading day. In addition to the denial of service attack, the eTrade was further hampered by desperate investors attempting to make trades.

The Yankee Group estimates the cumulative losses resulting from the attacks at $1.2 billion. This includes customer revenue, security and infrastructure upgrades, and market capitalization losses ("By the Numbers", 2000). Soon after the attacks, the FBI arrested the mastermind behind them -- a 15-year-old Canadian nicknamed 'Mafiaboy'.

In short, directed attacks specify their target and seek to halt their victim's operations or highlight their victim's vulnerabilities. Though the vandalism and DDoS attacks above are by no means a comprehensive list, they illustrate the possible effects that a directed attack might have on a web based entity.

7.2 Infrastructure Attack on Australian Sewage System, Spring 2000

The National Infrastructure Protection Center (NIPC), a division of the Department of Homeland Security, names the critical infrastructure components to be: Telecommunications, Banking and Finance, Water Supply Systems, Transportation, Emergency Services, Government Operations, Electrical Power and Gas and Oil Storage and Delivery. Many of these critical sectors are managed digitally. This creates a vulnerability that may invite an attack on infrastructure perpetrated through technology.

In November of 2000, the US Department of Energy and the Utah Olympic Public Safety Command conducted Black Ice, a simulation designed to understand the vulnerabilities of crucial infrastructure components when a loss of infrastructure is compounded by a cyber attack. The exercise began with a fictitious ice storm damaging power and transmission lines degrading the ability to generate and deliver power in the region. This was then exacerbated by a simulated cyber attack on the Supervisory Control Data Acquisition system, which controls the power grid in the area. The simulation discovered that this led to major performance loss in natural gas, water and communications systems. Black Ice demonstrates the acknowledgement of authorities of the potential damage an attack on infrastructure systems poses.

Similarly, in July of 2002 Gartner Research and the U.S. Naval War college conducted Digital Pearl Harbor, a simulation designed to explore the potential of an attack on critical infrastructure components. The experiment exposed the need for a central coordination role by government in the event of such an attack. It also discovered that isolated infrastructures proved much more difficult to breach (Caldwell, Hunter, Bace, 2002).

In the March and April of 2000, a community located on the Southeast coast of Australia was experiencing issues with its waste water systems. The town of Maroochy Shire, located close to Brisbane, saw technical failures lead to massive sewage flows into residential and tourist areas.

Investigations into the matter revealed that these were not the results of technical failure. Rather, they were acts of sabotage. Vitek Boden was a former employee of Hunter Watertech, the company which installed the computerized waste management control system for the Maroochy Shire Council, who managed the system. The 50 year old man from Brisbane, Australia was allegedly disgruntled at the Council for declining his application for employment.

As an act of revenge, Boden stole equipment from his former employer and attempted to break into the waste management system. Using a two-way radio, a remote telemetry system and a laptop computer, Boden endeavored to remotely manipulate the control system. On at least two occasions, Boden was successful. On one occasion in March of 2000, Boden released close to one million liters of raw sewage into local waterways, rivers, parks and a Hyatt Regency tourist center. Furthermore, the Register estimates that Boden attempted to usurp control of the waste management system on 46 separate occasions during March and April of 2001 (Smith).

Effects

The monetary damage of Boden's acts was estimated at AUS$176,000 in repairs, monitoring, cleanup and security for the Council as well as AUS$13,000 for Hunter Watertech. The marine life in affected areas was damaged. Likewise the creek water turned black and emitted an overwhelming stench. The Maroochy Shire Council estimated that the cleanup required seven days and AUS$13,000.

Although one may consider these effects rather small, perhaps the greater impact is the uncovering of inherent vulnerabilities in infrastructure. Indeed, this case highlights the potential for damage perpetrated by an internal malicious actor. Moreover, it underscores the importance of safety cultures, background checks and termination processes to uncover and extract internal threats. In addition, it reveals the accessibility of the equipment required to impose such a breach and the available knowledge to conduct this type of act. Finally, Vitek Boden's many attempts at sabotage highlight the advantages of proper intrusion detection equipment and need to investigate apparently benign disruptions.

7.3 Email Attacks

One way that computer viruses are released is via email. Email is regarded as the 'killer app' of the internet age. Beyond providing a more rapid form of communication, email allows businesses to exchange documents internally and externally with much greater ease than postal service, a messenger service or internal physical mail. This exchange of documents is exactly what virus writers prey upon.

An email attack can be considered a specific type of Denial of Service attack. An email virus arrives as an attachment, usually from a person with which the victim is acquainted. The subject line or email text prompts the victim to open the attachment, which holds the virus. Once the virus is activated, it will send itself to more victims using its current victim's address book. In no time, a corporate network can become flooded and bogged down by these viral messages, thus constituting a denial of service. In addition, an email virus can run scripts and perform other activities that both compromise the infected system and maliciously alter files. A common characteristic of email viruses is that while they take advantage of bugs and program vulnerabilities, they also are launched by exploiting human curiosity.

In this section we will study two email viruses that traversed world networks. The first is the Melissa virus, which hit in the March of 1999, while the second is the Love Bug virus which arrived a little over a year later in May 2000.

7.3.1 Melissa Virus, March 1999

Would you open an important message from a co-worker? On Friday March 26, 1999 many people did, and subsequently set off an email virus that would clog up systems at companies around the world. The Melissa virus was the fastest spreading virus that the technology community had seen to date. It served as a wake up call and a harbinger for what was to come.

Mechanics

The Melissa virus arrived as an email attachment. It was included in an email with the subject line 'Important Message From' and inserted the sender's name. Inside, the email read 'Here is the document that you asked for,' and a word document titled list.doc was attached. As the virus struck during the work day, the sender's address commonly belonged to a coworker or business partner, appearing not just innocuous, but 'important'. Thus the recipient would open the attachment with little hesitation. Upon opening the document, a list containing access information for pornographic websites appeared. Alarming as this might be, the true damage was occurring in the background. The document contained a macro or script that launched the Outlook email program and sent a similar email to the first fifty members of the infect computer's address book.

And thus the virus rapidly spread. Moreover, many companies used global address groups beginning with the word 'all' (e.g. all@company or all_finance@company) which appeared at the top of an address book and hastened the spread. Soon the messages clogged up the networks at corporations around the nation, prompting some to shut down email systems to remove the virus. Anti-virus companies scrambled to create an antidote to Melissa and firms likewise scrambled to install it. At some businesses, notes were hand written at workstations warning users not to open the virulent email.

CERT®, a federally funded organization at Carnegie Mellon University that tracks incidents, described Melissa as the fastest spreading virus to date, while the National Infrastructure Protection Center, now a division of the Department for Homeland Security, issued its first special warning regarding a cyber attack.

Effects

CERT® (1999) reports that nearly 100,000 machines were affected by Melissa at over 300 confirmed companies. Organizations such as the U.S. Marine Corps took down email servers, halting email communications to purge servers of the virus.

Another affected company was Microsoft, who makes the very programs that the virus took advantage of. The software maker shut down incoming and outgoing email. The company went one step further and contacted key customers and partners to alert them to the virus and to explain their temporary loss of email. Other affected companies included Motorola, Intel, Lucent, Honeywell and Merrill Lynch & Co..

The damage from Melissa was estimated at nearly $80 million. Its speed was unprecedented, with Newsweek (Levy, 1999) reporting that Melissa affected one 500 person company with 32,000 messages in fifteen minutes.

Though Melissa was brought under control, it is important to note that the virus struck on a Friday afternoon. Network, email and support professionals had the benefit of the weekend to clean their systems and eradicate the virus. Without the weekend, Melissa might have caused a great deal more damage.

Soon after Melissa was under control new strains were released. Anti-virus software was again updated to fight these new potential attacks. At this point, companies were provided the lessons of Melissa and many were quick to collaborate and search for a more effective approach to security.

Some were not so lucky. In November of 1999 a new strain, called Melissa.A was released and hit unprepared companies including Disney, whose anti-virus software was not updated to combat the strain. Likewise, in January of 2001, the Melissa.W strain was released in the United Kingdom to threaten Macintosh computers in the same manner as Windows based computers. Many companies across England were affected.

Though Melissa was not intended to corrupt machines, steal vital data, or even affect a large cross-section, it nevertheless managed to bring some corporate networks to a standstill. The term virus was fitting as it spread faster than it could be addressed. Moreover, Melissa underscored the real threat of computer viruses.

7.3.2 Love Bug, May 2000

In May of 2000, a little over a year after Melissa corrupted email networks, a similar but more dangerous email virus was released. The Love Bug virus would prove to be more harmful than Melissa and bring a larger price tag along with it.

Mechanics

Love Bug struck on Wednesday May 4 2000, arriving as an email with the subject line 'I LOVE YOU' and instructing the recipient to read an attached love letter. The letter was in fact a visual basic script. Visual Basic is a programming language used by all windows based products from the Microsoft Office suite to the Windows operating systems. This script first spread itself by sending a similar email to all members of the victim's Microsoft Outlook address book. Thus the aggressiveness of Love Bug was much greater than Melissa, which only propagated to the first 50 names. In addition to this, Love Bug attempted to spread itself by also infecting Chat programs, and replacing the contents of certain files with copies of the script, which would launch again when the unsuspecting user opened those files. Love Bug also altered the Microsoft Internet Explorer web browser start page to initiate a password stealing program. Finally, the virus altered operating system files vital to running Microsoft windows. These additional attributes allowed experts to characterize Love Bug as a more malicious worm than Melissa. Variants of Love Bug soon cropped up with still more malicious instructions.

Effects

The Love Bug was first detected in Asia, as their work day begins before the rest of the world. For some Asian countries May 4 was a bank holiday, which may have tempered the situation in those nations. However, many companies were still affected. The Asian Wall Street Journal servers were affected while the Dow Jones Newswire servers crashed. Soon after, the virus appeared in Germany, France and Switzerland among other European nations.

According to the Guardian London (Meek, 2000), an email screening company in England estimated that 10%-30% of U.K. businesses were hit with Love Bug. Some of these businesses included British Telecom, AT&T, Cable and Wireless in London, BBC, and banks, including Barclays. The British Government was also struck as the House of Commons shut down email service for hours to eradicate the bug.

The bug then traversed the Atlantic, and the United States was hit. According to ABC.com (Ruppe, 2000), at least 350,000 files in the United States were struck. Some affected U.S. entities included ABC, Ford Motor Company, the Pentagon and the United Nations operating out of New York City.

Computer Economics, a Carlsbad, CA company that measures IT spending, estimated in 2000 that the Love Bug and its variants cost a total of $8.7B in damages. Thus the Love Bug virus remains regarded as the most damaging from a monetary standpoint.

Epilogue

One year after Melissa struck, businesses proved to be unprepared for the Love Bug. Although the details of the virus could not be predicted, a number of simple steps learned from Melissa could have been followed. First, companies could have installed anti-virus software that filtered out suspicious email attachments. Indeed, Love Bug's attachment was odd in that it was a script of an atypical file format, .vbs. A programmer might be expected to email a visual basic script, but not a lover! In this sense, victims should have been suspicious at the file format as well, since most attachments are familiar word or excel format. Likewise, there are simple settings in Microsoft Outlook that warn a user when a script is going to be run. All of these steps may seem to be benefited by hindsight, however in the wake of Melissa, foresight was amply available.

7.4 Code Red Worm, July 2001

On June 19, 2001, CERT® issued an advisory regarding a Microsoft Internet Information Server vulnerability. The advisory pointed to a patch available at Microsoft's website that would protect a system from the vulnerability. Despite the warning, the following month a malicious worm was released that took advantage of the vulnerability. The worm, dubbed Code Red, then spawned variants and struck twice more in the months to come.

Mechanics

Microsoft's Internet Information Server (IIS) is web server software, designed to allow its user to broadcast a website. Thus the program is inherently vulnerable as it must be accessible to be effective. This makes it and similar web server programs attractive to attackers. Because of this, security mechanisms are built into the software to protect systems from attack. Since IIS is used to run a website, the potential for vandalism or theft of critical data is heightened. eEye Digital Security, a California Security Consulting Firm, discovered a vulnerability in Microsoft Internet Information Server on June 18, 2001 and Microsoft subsequently released a patch for it on June 26, 2001.

The first version of Code Red Worm was released on July 12, 2001. CAIDA, the Cooperative Association for Internet Data Analysis, based at the University of California, San Diego's Super Computer Center, noted that Code Red was a worm which self-replicated rather than a virus that relied on human interaction (Moore, Shannon, and Brown, 2002). The worm followed different instructions based on the day of the month. First, the victim's machine was scanned for availability and the absence of the patch. If this was the case, an exploit script was installed. If it was early in the month, the victim machine then became an attacker, generating a random list of IP addresses and performing a similar system scan to infect more machines. If the infected server hosted a website homepage, that page was replaced with the following message:

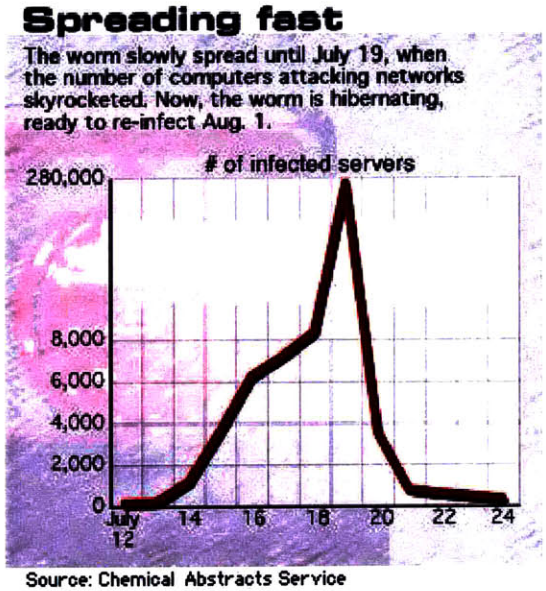
HELLO! Welcome to http://www.worm.com! Hacked By Chinese!

From the 20th through the 28th of the month the infected host launched a denial of service attack at Whitehouse.gov at a specified time and date. If enough machines were infected at this point, it would easily take down the White House site. After the 28th, the worm went into hibernation until the 1st of the next month. Thus, the attack was also designed to alternate between periods of propagation and hibernation. For a particular company, the initial damage was to the victim's website, while the heavier damage was the scanning, which quickly overloaded networks.

Events

The first version of the Code Red Worm was discovered by California network security consulting firm eEye Digital Security on July 13, 2001. Six days later nearly 380,000 servers had been infected (Lemos, "Virulent Worm", 2001). At first, each compromised machine generated the same list of other machines to infect, thereby slowing networks with scans, but only gradually spreading the worm. Then, on July 19, 2001 a more dangerous strain was released that generated a different list of other hosts to infect on every machine. At this point the worm began to spread rapidly, infecting hosts as they were being patched (Moore, et al., 2002). Figure 7.3-1 below depicts the growth of infected machines around July 19th, 2001, and the subsequent drop off as the virus entered hibernation mode late in the month.

Figure 7.4- 1: The rapid spread of the Code Red Worm



source: cnet.com
http://news.com.com/2009-1001-270471.html

Once Code Red entered into hibernation stage, the U.S. National Infrastructure Protection Center4 (NIPC) together with Microsoft issued an alert on July 31 warning that the worm would come alive again the following day. Figure 7.4-2 depicts the demographic locations where the July 19, 2001 attack hit.

Figure 7.4- 2: Hosts infected with Code Red by Country on July 19, 2001

Top 10 Countries		
Country	hosts	hosts(%)
United States	157694	43.91
Korea	37948	10.57
China	18141	5.05
Taiwan	15124	4.21
Canada	12469	3.47
United Kingdom	11918	3.32
Germany	11762	3.28
Australia	8587	2.39
Japan	8282	2.31
Netherlands	7771	2.16

source: CAIDA.org, 2001

http://www.caida.org/outreach/papers/2002/codered/codered.pdf, p7

[4] The National Infrastructure Protection Center was part of the FBI and is now part of the Department for Homeland Security focused on critical infrastructures in the United States.

While the first few days of August were relatively quiet, on August 4 2001 a more damaging variant of Code Red was discovered and named Code Red II. This variant did not hack a homepage or attack whitehouse.gov, but it did launch a stronger scan which had the ability to not only crash Microsoft Internet Information Server, but also routers, switches, and printers. Further, Code Red II installed a dangerous 'backdoor', which would allow a hacker to reenter the server at any time and possibly retrieve sensitive data. Despite its new attributes, this new version continued to exploit a patchable bug in the web server software. During the August attack, a number of businesses and organizations worldwide were affected by Code Red and its follower. Cap Gemini Ernst and Young's internal internet system was affected. Federal Express was also hit and its special pickup service experienced disruptions. Even Microsoft who released a patch saw some of its own servers affected including some that support Hotmail, which provided free email services to nearly 110 billion consumers (Luening, 2001) at the time of the attack.

In the beginning of August, FedEx reported that Code Red had caused delivery delays for up to one day (Leuning, 2001). CNN ("Code Red Impact Felt", 2001) reported that this affected their "call for pickup" service. Later in the month, USA Today (Hopkins & Farrell, 2001) noted that Code Red caused "severe" problems at FedEx, but that customers were not affected. Company spokesman Greg Rossiter stated that FedEx's business requires the express delivery service to be prepared with contingency plans. Indeed the article reported that FedEx handled the issue by isolating the worm and approaching the issue comprehensively.

> "'We isolated it and limited it in our system, and we executed our contingency plans,' Rossiter says. That meant getting help from dozens of company experts, who worked mostly without sleep, and from people in all aspects of the company from field managers to drivers."
>
> – Hopkins & Farrell, USA Today, August 20, 2001.

ISPs were particularly hit as their customers run networks that host web servers. Qwest Communications, a Denver based telecommunications company, saw a disruption that affected over 25,000 of its Digital Subscriber Line (DSL) customers and cost the company $3 million (Hopkins & Farrell, 2001). In 2001, DSL was a popular connection method for small businesses. Hopkins and Farrell (2001) go on to describe Profit Dynamics, an Arizona research firm and customer of Qwest, who relied almost entirely on the web for its promotions and was down for three days before Qwest could provide them assistance.

In an effort to halt the spread, many ISPs shut off service to affected network segments or customers to isolate the issue in those places. According to Computerwire (2001), AT&T was one such ISP, who further told affected customers to patch their systems and eradicate the infection before they would be reconnected. DSL providers DSL.net, Speakeasy Inc., and Telewest PLC. and Blueyonder employed similar tactics. This meant that the customers of those companies, many of which sell or market to end consumers were faced with either patching machines or loss of web connectivity.

It is important to note that a patch was released to battle this worm nearly one month before it was released. And yet, despite extensive media coverage and a warning from government, patching did not occur quickly. CAIDA (Moore, et al, 2002) found that the percent of unpatched hosts as of August 14, 2001 remained surprisingly high, as depicted in Figure 7.4 – 3 below.

Figure 7.4- 3: Hosts patched against Code Red by Country on August 14, 2001

Patch Rate in Top 10 Countries		
Country	patched (%)	unpatched (%)
United Kingdom	65.65	34.34
United States	59.59	40.41
Canada	57.57	42.42
Germany	55.55	44.44
Netherlands	46.46	53.53
Japan	39.39	60.61
Australia	37.37	62.62
Korea	20.20	79.79
Taiwan	15.15	84.84
China	13.13	86.86

source: CAIDA.org, 2001
http://www.caida.org/outreach/papers/2002/codered/codered.pdf, p10

Costs

Computer Economics estimated that more than 1 million computers were infected with a Code Red virus, costing $1.1 billion in repairs and $1.5 billion in lost productivity. Thus the total worldwide impact was measured at $2.6 billion.

Epilogue

In September of 2001, the Nimda virus struck. It was a more sophisticated virus spreading through multiple vectors including email, server shares, browsing, or backdoors. Nimda infected over 2.2 million machines in a twenty four hour period between September 20 and 21 of 2001. Computer Economics estimates the damage from Nimda to be $531 million. Again, it attacked a known vulnerability for which a patch had already been released.

7.5 SQL Slammer Worm, January 2003

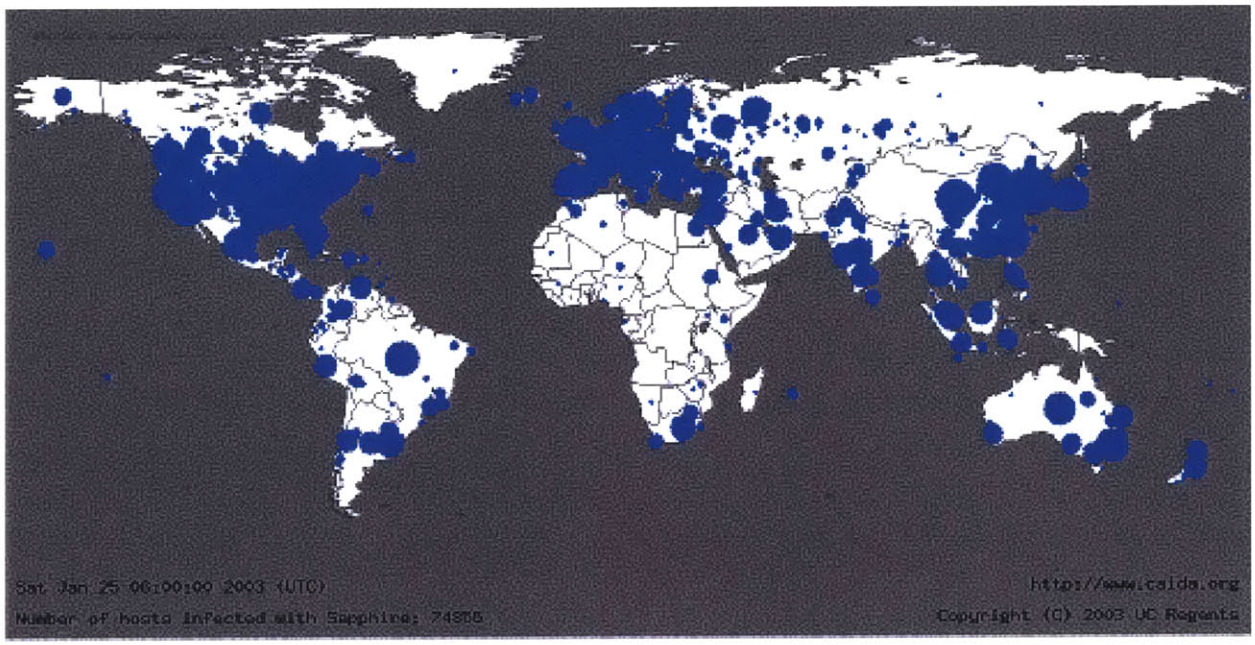
In January of 2003, the Sapphire or SQL Slammer worm struck servers around the world. It spread at unprecedented rates, taking advantage of a Microsoft SQL server vulnerability. Ultimately, the worm caused billions of dollars in damage.

Mechanics

The SQL Slammer worm exploited a vulnerability in Microsoft SQL server, a popular database program running on Windows NT based machines. The vulnerability was discovered and a patch was available from July 20, 2002 at Microsoft's website. The worm began its course close to six months later on January 25 2003 at 5:30 am GMT, or 12:30 am EST. Once the worm infected a machine, it would attempt to propagate itself by bombarding networks with small packets of data sent to randomly generated network addresses. The packets were sent via a port commonly used for SQL database communications, UDP 1434. The UDP protocol was important in that it allowed network packets to travel with less identifying information, thus making them smaller and more nimble. The result was denial of service conditions on critical shared networks.

One part of this attack that surprised security experts was the speed with which it traveled. Some of the speed was due to the diminutive size of the packets. A joint report from the CAIDA located at University of San Diego's Supercomputer Center noted that the worm infected 90% of vulnerable hosts in ten minutes, doubling in size every 8.5 seconds (Moore, Paxson, Savage, Shannon, Staniford & Weaver, 2003). Figure 7.5-1 depicts infected hosts thirty minutes after it the worm was detected.

Figure 7.5- 1: Infected Hosts Worldwide 30 Minutes After SQL Slammer Virus Strikes



The report went on to state that the speed of the Slammer Virus was two orders of magnitude faster than Code Red, which doubled every 37 minutes. With this rate, the virus might have caused more damage, had it not been targeted at a specific service, SQL. In total 75,000 machines were affected, compared to over 350,000 from Code Red.

Effects

The worm hit Asia on Saturday afternoon. South Korea was particularly hard hit as three large ISPs, Korea Telecom Freetel, Hanaro Telecom Co. and SK Telecom experienced extreme network slowness (also described as latency or degradation) when critical servers became overloaded with excessive traffic. The Wall Street Journal ("S. Korean Fincl. Sector", 2003) reported that these Internet providers were down for nearly four hours because of the attack. As those ISP's served a large portion of the nearly 30 million consumers in the most wired nation, the effects were strongly felt in South Korea. ISPs in Taiwan, the Philippines and Malaysia reported similar difficulties.

In the United Kingdom, Hewlett Packard's UK staff worked through the weekend to fix the problem, but was still forced to send employees home as the issue persisted on Monday. Other e-commerce sites hit include Borders.co.uk, Amazon.co.uk and msn.co.uk.

In the United States, networked operations at a number of firms were devastated by the traffic overload brought on by the attack. Seattle's 911 call center serving two police departments and 14 fire departments was downed by the worm as well. The call center instead manually took information using paper and pens. Atlanta, Georgia's main paper, The Atlanta Journal and Constitution, was forced to delay printing of its Sunday January 26 edition for an undisclosed amount of time. The paper also reported difficulties updating its online news site, as did The Philadelphia Inquirer and the Associated Press (Sieberg & Bash).

Another widely affected business was Continental Airlines whose online ticketing and reservation system were impacted. According to CNN (Sieberg & Bash, 2003), "Spokesman Jeff Walt said [ticket] agents reverted to 'the old fashioned way' – phones, and pen and paper – to record reservations and online tickets." The spokeman went on to say that this manual system was much slower, resulting in delays and cancellations of regional flights. Walt went on say that smaller hubs including Houston, Texas, Cleveland and Ohio experienced up to 30 minute delays, while their main hub Newark, experienced longer delays, though no specifics were given (Sieberg & Bash, 2003). The Washington Post (Krebs, 2003) reported that Continental restored ticketing and kiosks in the afternoon on Janaury 26, 2003, about a half a day after the attack began. The company website, used for online purchases however, was down through Sunday January 27 2003, adding up to a nearly two day outage, and causing up to 140 minute waits on its reservation hotline (Krebs, 2003).

Banks and credit companies were similarly affected. American Express's servers were affected, barring service representatives from accessing customer and credit information. According to Computerworld (Bajkowski, 2003), the Australian

American Express' external customer website slowed to the point of inaccessibility for about a day and a half, restoring operations late Sunday, January 26, 2003. Mortgage firm Countrywide Financial's website, which allows customers to send payments online, was down through Monday, January 27, 2003, nearly 3 days from the start of the attack. Perhaps the hardest hit bank was Bank of America, who saw most of its 13,000 automatic teller machines affected. Customers could not withdraw money or make similar transactions on affected machines. A company spokesperson told CNN (Seigberg & Bash, 2003), that most ATMs were restored by Saturday afternoon, 12-16 hours into the attack.

Case Study: Global Manufacturer

During the course of research, the author had the opportunity to speak to a global manufacturer headquartered in Silicon Valley regarding its experience with SQL Slammer.

The worm was first detected in local pockets of the company. The company, however, had an escalation path and emergency operating procedure. As increasingly similar local reports were received, global emergency managers determined that the issue was company wide. The manufacturer quickly worked to technically isolate factories from the infected network, to ensure continuity of operations and diminish the spread of the virus. The company also prepared to take orders using phone and fax rather than online, given that the online order system was affected. Since the company was able to remove the worm from its network quickly, this method ultimately proved unnecessary. The manufacturer attributed its success in dealing with the virus to its quick recognition of the scope of the attack and the subsequent comprehensive global management of the reparations.

Costs

The SQL Slammer proved to be an expensive attack. Mi2g, a London research firm, estimated the cost of the worm to be between $950 million and $1.2 billion, while Computer Economics estimated costs between $750 million and $1 billion.

8.0: Synthesis and Conclusions

Despite the breadth of the events discussed, it remains possible to find similarities between them and thus draw conclusions. For example, a biological virus initially spreads quickly and undetected, much like a network worm or virus. But what does this mean for companies? What can be learned from these many accounts of disastrous and sometimes deadly events? This section seeks to synthesize those accounts and derive generalized guidelines that may assist corporations in navigating the next disruption, whether it is accidental or malicious. This section also returns to the themes discussed earlier, and attempts to support those themes with the data that have been presented.

8.1 Prior Warnings and Events Should Be Acknowledged And Utilized

Throughout this text we have seen examples of disruptive events, some preventable and some unavoidable. In many cases, there existed a similar prior event which was studied and offered useful knowledge and insight to managing the disruption at hand. In other cases, clear warning signs were apparent, but were not acknowledged. Finally, with some events a preventative tool was available, and somehow not utilized.

The Influenza of 1918 struck swiftly across the world, arriving in waves. Outbreaks on the East Coast of the United States were waning just as the disease began to wreak havoc on in the West. Western cities might have learned from Boston and Philadelphia that public gatherings were dangerous, and that hospital and city support staff might face shortages. Instead, San Francisco held bond rallies while Seattle held war related gatherings. Eventually, San Francisco faced coffin and garbage worker shortages as well. As the disease took its toll, all of these areas suffered the same depletion of medical staff experienced in the east.

With the 2001 Foot and Mouth outbreak in England, the 1967 outbreak provided valuable lessons for the 2001 government. A written report from 1967 advised to promptly utilize the army's logistics forces to assist with slaughter and carcass

disposal. However, in 2001 these forces were not brought in until nearly one month into the crisis. Similarly, the 1999 report stating that the British government was not equipped to handle a large scale outbreak failed to prompt the Ministry of Agriculture, Fish and Food to take action. The 1967 Foot and Mouth report also discussed the use of Vaccines in subsequent outbreaks. However, this tool was not considered by government until well into the 2001 epidemic. Farmers in the area feel that this might have prevented the unnecessary slaughter of thousands of livestock.

Overlooking of reports is not reserved only for biological outbreaks however. The Bhopal chemical disaster in 1984 occurred in the wake of a 1982 general safety inspection that cautioned the Bhopal plant about a catastrophic event and recommended changes and replacements of safety systems. Not only were the recommendations disregarded, the company also did not follow up with a more detailed inspection. Perhaps even more surprising is that Union Carbide did not use the lessons from the Bhopal disaster to prevent or more deftly handle the subsequent leak in its similar West Virgina plant. In the same manner as Bhopal, a leak in Institute, West Virginia was released with little information provided to the citizens of the area.

In the same way, the Cherynobyl nuclear reactors were not surrounded by a secure concrete structure like many other nuclear power plants that existed at the time. This simple structure would have contained much of the radiation that rendered the area unsuitable for living.

The mismanagement of preventative tools and warning signals has emerged repeatedly with regards to cyber attacks. Despite the damage resulting from Melissa, organizations still fell prey to Love Bug, which operated in the same manner. Melissa should have taught administrators to implement measures that filtered suspicious attachments containing macros. The Love Bug virus arrived as a visual basic attachment, which should have immediately tripped alarms in the wake of the Melissa virus. The Code Red and Nimda worms attacked a known and patchable vulnerability in Microsoft software. These patches were readily available in June of 2001, and publicly recommended in July of 2001, yet most of the damage occurred in August and September of the same year. Similarly, the SQL Slammer virus occurred in January of 2003, while the patch to avert such an attack was available nearly 6 months earlier, in June of 2002. Management of patches has become a hotly debated topic within security circles, with some placing blame on bug-ridden software and others placing blame on lax administration. The author feels that responsibility lies on both sides of that debate. That is, software should be inherently safe, but those who buy it take on its risks and are responsible to maintain it if security patches become available.

Through all of the instances above, it is clear that firms should be motivated to proactively study past events, acknowledge warning signals, and implement preventative measures in an effort to avoid, or at least mitigate, the effects of disruptions.

8.2 Government Intervention may Strain Business Flow

In times of crisis, governments often step in to provide assistance and guidance. Generally, government decisions are intended to contain damages and maintain continuity. However, in some cases, government actions overshoot their intended goals and as a result bring businesses to a halt.

During the Foot and Mouth epidemic in England, the government implemented some policies that negatively affected businesses. For instance, the Ministry of Agriculture

Fish and Food's decision to cull all animals found within a certain radius of a known infected animal is believed to have resulted in the slaughter of thousands of unaffected livestock. Though this was intended to halt the spread, it was viewed as indiscriminate and devastated many farmers with healthy animals. Similarly, the government decision to close footpaths and restrict movement in the area crippled the tourism industry. In the same way, the 1918 Influenza prompted governments to close public gathering places, which negatively affected the profits of theaters and hospitality establishments. Finally, the travel restrictions prompted by SARS have resulted in most Asian airlines cutting service, including a 40% Cathay Pacific reduction.

During the Anthrax attacks in the fall of 2001, post offices were closed for inspection and cleaning. Though this was necessary, it prevented many local businesses from receiving mail for over a week. For some utilities, lenders and credit card companies, the mail service was their revenue channel and a disruption of this sort affected the bottom line.

8.3 Alternate Sourcing can Ameliorate Supply Issues

When a disruption occurs, it may not directly affect a business, but it may affect that business' supply chain of raw materials and inputs. A company can soften this blow by creating supply chain contingency plans. One effective plan is to find alternate sources for raw materials and engage them prior to the emergency. Without prior relationships, companies are forced to find alternate sources on the fly while competitors are as well, which will drive prices up for all.

During the 1918 Influenza, the coffin shortage produced creative supply contingency plans. In Philadelphia producers of other wood products were engaged to assist in the construction of coffins. The city of Buffalo took production up itself, no longer relying on outside producers. Finally, most cities turned to cheap pine as a raw material to inexpensively produce the vast number of coffins required.

The 2001 Foot and Mouth outbreak placed a strain on English leather hide supply. This caused leather makers to seek alternate sources including Australian Hide, American Hide, and elk hides. Regardless, prices saw a significant rise.

The Anthrax scare of 2001 provoked many mailrooms to scrutinize incoming mail and implement secure technology. This created a change in the mail room supply chain design. This change caused significant delays and highlighted the need for a flexible supply chain design. Anthrax also sparked redesigns such as rerouting for companies like Covad Communications and product redesign for direct mailers who returned to printed return addresses on envelopes.

The SARS virus prompted redesigns in the order supply chain for toy companies that have moved to overnight delivery to replace face to face sales meetings. Similarly, during the SQL Slammer worm companies such as Continental Airlines returned to paper based reservations and ticketing as an alternative to their normal network and web based methods.

Thus it becomes apparent that a supply chain designed with flexibility and resilience will be better equipped to meet dynamic requirements that emerge from disruptions.

8.4 A Comprehensive Forthright Approach is Reccommended

A system wide approach to a disruption allows businesses to correctly assess the scope of the damage and therefore apply the correct treatment measures. This is in contrast to a localized approach that may treat one local area at the expense of another. Comprehensive management is enabled by a proper monitoring and escalation system. With a forthright approach, organizations freely exchange information regarding the disruption. This facilitates outside assistance and encourages those external to the system to contribute to a solution.

Following the Anthrax scare in New York, the city created its Syndromic Surveillance System, monitoring prescriptions, drug store purchases and hospital admittances to find patterns. Thus a system wide, top level approach is being used to identify a virus or attack that may begin in a very narrow portion of the population.

With respect to comprehensive management, The British Government, particularly the Ministry for Agriculture Fish and Food (MAFF), was frequently criticized during the crisis for lacking a system approach which led to inconsistent and sometimes inaccurate messages. For instance, Nick Brown misstating that the disease was under control. Further, the Anderson report recommended that MAFF create a "National Strategy" to manage future outbreaks. The MAFF, now named the Department of Environment, Food and Rural Agriculture (DEFRA), has attempted so much with its Foot and Mouth website.

In China, the slow release of information related to SARS allowed the disease to spread outside the country and continue to proliferate within it. Had that government initiated dialogue in the Fall of 2002 when the earliest cases were detected there, some believe that SARS would have been identified earlier and contained to a smaller region. In Bhopal as well, Union Carbide's pointed fingers at its Indian subsidiary and localized the responsibility to that location. UC went on to make frequent misstatements regarding safety within its plants. This created great mistrust of the company.

Similarly, the Soviet government's secrecy surrounding the events at Chernobyl kept the international community at bay. Indeed, news of the accident was discovered by Swedish radiation detectors. The USSR's unwillingness to share details of the accident resulted in reduced aid and assistance reaching the region as nations struggled to understand the extent of the damage.

Finally, during the release of the Code Red worm, FedEx attributed its ability to return online quickly to a comprehensive approach involving people from drivers al

the way to executives. Similary, with SQL Slammer, in the manufacturer case study it is stated that the company had already created a monitoring system to detect a network problem. This, coupled with an escalation path allowed managers to quickly realize the scope of the issue and take action across all company nodes, and not just those that reported problems.

8.5 A Safety and Security Culture are Important Tools against Attacks and Proliferation

In a hazardous work environment, employees should be educated with a great sense of safety and empowered to make all decisions with safety as a critical factor. This is the concept of a safety culture, one where safety is emphasized and permeates all facets of the company. In this type of culture safety concerns become second nature for employees, who will then consider safety priority to taking actions.

In the Bhopal example, the absence of a safety culture was apparent. One cannot help but ask why warning systems did not sound, why a flare was not available to eradicate the gas, and why an alternate storage tank was not empty. With safety on the forefront of the company and its workers minds, these gaps might have been noted and addressed prior to the accident. Perhaps even more glaring is the choice of workers on duty to take a tea break instead of investigating an issue with their gas tank. Through proper safety training, emphasis and consequences, workers might have felt more urgency to scrutinize symptoms. The tea break also points out that creating an environment focused on safety requires overcoming cultural barriers.

Conversely, the Chernobyl disaster emphasized how a culture can create positive outcomes. A sense of safety and protection prompted teams to build the concrete shelter around the exploded reactor despite the high radiation levels that existed in the construction zone. With SARS we see that a safety culture in Singapore that is replete with consequences. This system allowed that nation to isolate the disease and

even feel discomfort at the relaxed attitude that might result from the declaration that the island nation was safe from the disease.

With regards to cyber attacks, a company may purchase state of the art detection tools and implement crisis management policies, but an overarching culture that places emphasis on security is the best ways to contain and prevent disruptions at the grass root level. This culture is created when an organization stresses security and awareness at all levels so that employees almost unconsciously consider these ideals in their work. This concept though not new, is well supported through the examples that have been discussed.

Vitek Boden, the disgruntled Australian worker who released waste into the water system, was able to steal the computers that he used to breach the system and was able to breach it because he was on the team that built it. A company with a security culture will implement strict procedures that cut off service to former employees. In addition, a security culture might have led the company to research the many unsuccessful attempts by Boden prior to his actual break in.

With email viruses, a security culture might have slowed the spread of the attacks. In the case of the Melissa virus, employees were not made aware of the dangers of running macros in documents. Though one might take issue with this and attribute Melissa's damage to being the first attack of its kind, no such excuse exists for the Love Bug virus, which arrived one year after Melissa. Businesses who were not hit by Love Bug implemented better filtering and secluded emails with suspicious attachments, such as a Visual Basic Script. Desktop users were also warned against such attachments and understood the dangers of macros.

A security culture also prompts employees to manage security proactively. With Code Red and SQL Slammer, this might have prompted more IT departments to install the available patches before these damaging worms struck. By implementing this type of policy, organizations empower their workforce to enforce and enhance data security.

8.6 Prepare systems to operate in isolation

As businesses operate in an increasingly global environment, they become more reliant on systems that connect activity between employees, offices and nations. With increased reliance, these systems become more vulnerable. Along the same lines, systems also become conduits to rapidly spread attacks and disruptions. In light of this notion, systems should be enabled to quickly switch to a disconnected operating mode. By employing this practice, business continuity is preserved while the spread of any detriment is contained.

The first application of isolated operations is the basis for quarantines. Quarantines are intended to isolate affected elements from non infected elements. Quarantines were employed in many of the events described including the Spanish Influenza, Foot and Mouth Disease and SARS. One step beyond quarantine, however, is the voluntary isolation of unaffected parties to ensure business operations. This was utilized during the SARS breakout as the Hong Kong & Shanghai Banking Corp., created a 'clean' office prepared to continue trading in the event that the main offices became infected. Similarly, JP Morgan and Swiss Bank UBS among other companies asked employees to work at home to contain any further spread to healthy employees. Unless a company is prepared with remote capabilities such as Virtual Private Networks or laptop computers, these isolated operations become impossible to implement.

The notion of isolation is often employed with respect to cyber attacks. Indeed, during the Melissa and Love Bug email viruses, companies shut off mail servers to the outside world in order to treat them. Employees were forced to continue to function without email, thus employing phone and fax capabilities instead. Similarly, during the SQL Slammer attack company networks were brought to a standstill. Continental Airlines resorted to paper based ticketing and reservations to maintain business continuity while systems were down. The manufacturing company provided in the case study also prepared to take orders manually and conduct business using

the phone rather than the Internet. Although this preparation proved unnecessary for them, it is underscores the important to prepare for such activities in the event that affected systems cannot be brought online quickly. In the same way, the manufacturer is currently updating its security architecture to allow factories to isolate themselves from other networks at the flip of a switch.

8.7 Often, Impact is not as Dire as Originally Predicted

While an event is unfolding, estimates are often made predicting extensive damage and impacts. However, when studied in hindsight, the estimates are often found to be extreme, while the system actually returns to its original state more quickly or smoothly than anticipated.

With Foot and Mouth disease, data supported that farms in affected areas were operational again within a year of the outbreak, and that only two farms in the hardest hit country, Cumbria, had gone out of business. In fact, in the same area, unemployment actually fell following the outbreak. Similarly, with Anthrax, the US mail system returned operations to normal within a few weeks of the attacks. Though the SARS outbreak has not concluded yet, predictions regarding the devastation of the manufacturing sector have not yet proven true. Indeed, large companies in the area such as Intel, Motorola, and Toys 'r' Us report smooth operations and little damage beyond travel restrictions.

Though Chernobyl is considered the worst nuclear accident in history, plant and wildlife thrives in the area, including as boars, deer, herons and field mice (Schmidt, 1995). Further a statement in 2000 by the International Atomic Energy Agency found "no evidence of a major public health impact attributable to radiation exposure 14 years after the accident," ("Chernobyl not so deadly", 2000).

Similarly, the victims of directed attacks on websites in winter 2000 (Yahoo!, eBay, Amazon, Etrade) are operational today and remain among the most visited on the

web. With Melissa, Love Bug, Code Red and SQL Slammer, despite the slow down to networks, most systems returned within one to two days with little to no permanent damage.

8.8 Closing

In closing, while each of the events described provide evidence that the supply chain requires resilience and flexibility to absorb the effects of a disruption, they also teach us valuable lessons in preparedness and operations. These lessons include acknowledgement of prior warnings, absorption of government intervention, alternate sourcing and contingency planning, comprehensive and forthright approaches, implementation of safety and security cultures, preparing systems to operate in isolation, and frequent overestimates of damage.

9.0 Opportunities for further study

Although this document serves as a tool for learning from historical disruptions, it may also act as a catalyst for further research. As the topics considered here cover a broad subject area, further research may follow many paths. These paths include in depth study of Safety and Security Cultures, Cyber Attacks and Network Security, Technical Methods of Network Isolation, and continued documentation of the SARS epidemic.

To learn more about historical disruptions and their effects, this document should be read in conjunction with a related document covering physical attacks and natural disasters. This document is authored by Christopher B. Pickett, and is also part of the MIT Supply Chain Response to Terrorism initiative (SCRT). Further information about other research connected with SCRT including company surveys and interviews, studies of Public Private Partnerships and Risk Assessment Methods can be found at http://web.mit.edu/scresponse/index.html, the research website.

Security Culture information can be found at:

http://www.elefire.com/security.html

http://www.admin.ox.ac.uk/mis/oxsecpol.shtml

http://www.cyberguard.com/pdf/securitypolicy.pdf

http://www.gartnerg2.com/site/FileDownload.asp?file=rpt-0102-0010.pdf

Internet Security information is readily available in online journals and sites. The two below are well respected and an excellent starting point.

Cert.org

CERT® is a federally funded research organization at Carnegie Mellon University. CERT® tracks vulnerabilities and incidents and provides assistance regarding internet security.

SANS Institute

The SANS institute is a resource for education about network security

References

General

Sheffi, Y. (2001). Supply Chain Management Under the Threat of International Terrorism. International Journal of Logistics Management, v12, no. 2.

Martha, J. & Vratimos, E. (2002) Creating a Just-in-Case Supply Chain for the Inevitable Next Disaster. Viewpoints, Marsh and McKlennan Companies. http://www.mmc.com/views2/autumn02Martha.php

Martha, J. & Subbakrishna, S. (2002, September 1). Targeting a Just-in-Case Supply Chain for the Inevitable Next Disaster. Supply Chain Management Review. http://www.manufacturing.net/scm/index.asp?layout=article&articleid=CA243747&text=disaster

1918 Influenza

The Spanish Influenza, 1918. http://www.vortex.is/~sigrun/Evropa.html

Billings, M. (June, 1997). Medical and Scientific Conceptions of Influenza. http://www.stanford.edu/group/virus/uda/fluscimed.html

Billings, M. (June, 1997). The Influenza Pandemic of 1918. http://www.stanford.edu/group/virus/uda/

Billings, M. (June, 1997). The Public Health Response. http://www.stanford.edu/group/virus/uda/fluresponse.html

Brainerd, E., & Seigler, M. V. (September 2002). The Economic Effects of the 1918 Influenza. http://faculty.econ.northwestern.edu/faculty/ferrie/wksp/Sept%2026th.pdf

Crosby, A. (1989). America's Forgotten Pandemic of 1918. Cambridge, England: Cambridge University Press.

Grant, A. Influenza 1919: Portland, Victoria. http://www.ballaratgenealogy.org.au/digby/1919flu.htm

Meltzer, M. I., Cox, N. J. & Fukuda, K. (1999). The Economic Impact of

Pandemic Influenza in the United States: Priorities for Intervention. Emerging Infectious Diseases, 5.5 p. 259.

Foot and Mouth Disease, Spring 2001

(2001). Foot-and-mouth: The Key Stats. BBC News Online. http://news.bbc.co.uk/1/hi/uk/1334466.stm

(2001, March 8). Foot-and-Mouth Disease Spreads. Woolmark.com. http://melpub.wool.com/enews2.nsf/vwMonthlyWoolmark/5c61cb01164 3a5f600256a090034c0ed?OpenDocument&Archive

(2001, March 19). Hiding to Nothing for Leather Trade. BBC News Online. http://news.bbc.co.uk/1/hi/world/europe/1230249.stm

(2001, March 29). Foot and Mouth Disease. The Costs and Cures. The Economist.

(2001, April 1). Cheltenham's £30m Blow. BBC Sport Online. http://news.bbc.co.uk/sport1/hi/1254790.stm

(2001, April 12). Travel Firms Hit by Farm Disease. BBC News Online. http://news.bbc.co.uk/1/hi/business/1273482.stm

(2001, May 30). Foot and Mouth Crisis Time-Table. CNN.com. http://www.cnn.com/2001/WORLD/europe/UK/04/11/fandm.timeline/

(2001, June 5). Most Exporters Surviving Foot-and-Mouth Impact. Ananova. http://www.ananova.com/business/story/sm_316328.html?menu

(2001, June 8). Farm Crisis 'body blow' to Tourist Industry. Ananova. http://www.ananova.com/business/story/sm_320820.html

(2001, August 29). FMD Report: Outbreak's Economic Impact. BBC Online. http://new.bbc.co.uk/1/hi/uk/1515327.stm

(2001, October). £3.3 billion foot-and-mouth cost to English tourism. Ananova. http://www.ananova.com/business/story/sm_437193.html

(2002, March 9). The Disaster that Never Was. The Economist.

http://www.economist.com/displayStory.cfm?Story_ID=S%27%29H%2C%2EP A%5B%25%20%20%23%2C%0A

(2002, July 22) It was a Hell of a Mess. BBC Online. http://news.bbc.co.uk/1/hi/uk_politics/2144145.stm

(2002, July 22). Q&A: Anderson Inquiry. BBC Online. http://news.bbc.co.uk/1/hi/uk_politics/2144551.stm

(2002, July 24). County verdict on Anderson Report. North Devon Gazette. http://www.northdevongazette.co.uk/archived/2002/wk30/news/30news23.asp

(2002, July 27). Learning the Hard Way. The Economist.

Anderson, I. (2002, July 22). Foot and Mouth 2001: Lessons to be Learned Inquiry Report. http://213.121.214.218/fmd/report/index.htm

Cameron, E. (2002, August 29). Foot and Mouth Disease: State of the Countryside Report, Supplement to 2001 State of the Countryside Report. United Kingdom Countryside Agency, pp. 6-10, 23-40. http://www.countryside.gov.uk/stateofthecountryside/past.htm

Fleetwood-Jones, C. (2001, April 2). Festival and Six Nations Give Up the Fight. The Guardian. http://www.guardian.co.uk/footandmouth/story/0,7369,466940,00.html

Kaufman, L. (2001, March 29) Luxury Leather Prices Climb as European Supplies Dwindle. The New York Times. http://www.nytimes.com/2001/03/29/business/29LEAT.html?ex=1049518800&en=937d63eabeaff36a&ei=5070

MD discusses methods of future growth at Pittards. The Wall Street Transcript, twst.com. http://www.twst.com/notes/articles/lss035.html

Anthrax, October 2001

(2001, November 5). Pony Up to Cure Mailroom Anthrax. Newsweek, p.29.

(2003, January 1). Anthrax, One Year Later. The Washington Post, p. A18.

Armour, S. (2001, October 18). Workplaces Grapple with Anthrax Worries. USA Today, p. 1B.

Atlas, R. D. (2001, October 27). Anthrax Slows the Mail and Paying of Bills. The New York Times, section C, p. 4.

Begley, S. & Springen, K. (2001, October 29) Anthrax: What you need to know. Newsweek, p. 38.

Chen, D. W., and Greenhouse, S. (2001, November 1). As Anthrax Cases Mount, the Tranquil Rhythms of Suburban Havens are Disrupted. The New York Times, section B p. 9.

Crowley, G. (2001, October 22). A Run on Antibiotics. Newsweek, p. 36.

Elliot, S. (2001, October 16). With Consumers Concerned About Unexpected Mail, Direct Marketers Will Try New Approaches. The New York Times, section C p. 4.

Foust, D., & Khermouch, G. (2001, November 19). A Hit to the Mail is a Hit to the Economy. Business Week.

Goldstein, A., & and Powell, M. (2001, October 30). Anthrax in Five More D.C. Buildings. The Washington Post.

Grimsley, K. D., Smith, L. (2001, October 21). Businesses Fret as Schools Cancel Trips to Capital. The Washington Post, p. C01.

Hedgpeth, D. (2001, October 18). Anthrax Called Tourism Threat; DC Officials Fear Further Drop in Business. The Washington Post, p. E15.

Irwin, N. (2001, October 24). Mail Security Strategies Slow Down Businesses. The Washington Post, p. A15.

Janofsky, M., & Chen, D. W. (2001, October 16). In Mail, A New Meaning for 'Handle with Care.' The New York Times, section B p. 1.

Mayer, C.E. & Stern, C. (2001, October 25). Anthrax Fears Prompt Direct Mailers to Adjust Marketing. The Washington Post, p. E01.

Mayer, C.E. (2001, October 17). Anthrax Scare Forces Postal Changes. Direct Marketers Adopt New Tactics on Mailings to Avoid Losing Business. The Washington Post, p. E01.

Maynard, M. (2001, October 28). Anthrax Trips Up Some Mail

Campaigns. The New York Times, section 3 p. 4.

SARS, Spring 2003

(2003, March 27). The Singapore Model on SARS. The Wall Street Journal.
http://online.wsj.com/article/0,,SB104871720745536900,00.html

(2003, April 1). SARS Forces Airlines to Cut Flights. MSNBC.
http://www.msnbc.com/news/894076.asp?0si=-

(2003, April 3). Spread of SARS in Asia Prompts Fears for High-Tech Industry. Associated Press.
http://online.wsj.com/article/0,,SB104939642270543800,00.html

(2003, April 30). SARS, Thailand, Tourism, and Business Travel: How Fast for Recovery? Asian Market Research News.
http://www.asiamarketresearch.com/news/000305.htm

Altman, L. K. (2003, April 2). Many Questions, Fewer Answers on a Mysterious Respiratory Syndrome. The New York Times.
http://www.nytimes.com/2003/04/02/health/02SYMP.html

Bradsher, K. (2003, April 2). Virus Spreads Havoc on Business. The New York Times.

Bradsher, K., (2003, April 3). Virus Imperils Commerce and Economy in Asian Hub. The New York Times.

Buckman, R. (2003, April 1). Big Hong Kong Firms Resort to Corporate-Ordered Detox. The Wall Street Journal.
http://online.wsj.com/article/0,,SB104914123414547500,00.html

Curren, D. (2003, April 3). Mysterious SARS disease seen weighing on Canada Economy. Dow Jones Newswires.
http://online.wsj.com/article/0,,BT_CO_20030403_005126,00.html

DeLeon, C. (2003, April 3). AC Moore Warns SARS May Affect Ability to Buy Merchandise. The Wall Street Journal Online.
http://online.wsj.com/article/0,,BT_CO_20030403_003310.00.html

Einhorn, B., Engardio, P., & Shari, M. (2003, April 21). SARS: Damage in the Delta. Business Week, p. 56.

Flannery, R. (2003, April 28). SARS Breeds Threat to Taiwan Tech. Forbes.com. http://www.forbes.com/business/manufacturing/2003/04/28/cz_rf_0428taiwan.html

Foo, F. (2003, April 3). SARS Underscores need for Mobile Workers. The New York Times.

Gibson, R. (2003, April 3). Starbucks Reports Some Sales Decline in Asia from SARS. Dow Jones Newswires. http://online.wsj.com/article/0,,BT_CO_20030403_007313,00.html

Hellweg, E. (2003, April 9). Is SARS Sickening Tech? Business 2.0.

Khalid, A. (2003, May 9). Impact of SARS on Manufacturing Firms Mild: Survey. The Straits Times. http://straitstimes.asia1.com.sg/sars/story/0,4395,187984,00.html

Korporaal, G. (2003, April 14). SARS May Ground Cathay Fleet. The Australian. http://www.theaustralian.news.com.au/common/story_page/0,5744,6279775%255E23349,00.html

McBride, S. (2003, April 2). A Run on Stylish Surgical Masks Can't Hide Hong-Kong's Fear. The Wall Street Journal. http://online.wsj.com/article/0,,SB104922474535234900,00.html

Murray, C. J. (2003, April 7). SARS Virus Plagues the Industry. The Work Circuit. http://www.theworkcircuit.com/story/OEG20030407S0061

Perez-Pena, R. (2003, April 4). System in New York for Early Warning of Disease Patterns. The New York Times. http://www.nytimes.com/2003/04/04/nyregion/04WARN.html

Richardson, K, Borsuk R., & Chang, L., (2003, April 3). Parts of Asia Remain in Grip of SARS as Infections Rise. The Wall Street Journal. http://online.wsj.com/article/0,,SB104906989441722100,00.html

Roberts, P. & Evers, J. (2003, April 3). In U.S. and Europe, SARS Affecting Travel, Meetings. Computerworld. http://www.computerworld.com/printthis/2003/0,4814,80003,00.html

Bhopal and Chemical Events

(1995, March 31). Killer Droplets. Asiaweek, p. 30.

(1995, April 22). Disneyland Gas Attack is Foiled, Paper Says. St. Louis Post-Dispatch, p. 1A.

Diamond, S. (1985, January 28). The Bhopal Disaster: How it Happened. The New York Times, section A, p. 1.

Diamond, S. (1985, January 30). The Disaster in Bhopal: Workers Recall Horror. The New York Times, section A, p. 1.

Diamond, S. (1985, February 3). The Bhopal Disaster: Lessons for the Future. The New York Times, section A, p. 1.

Fink, S. (1986). Crisis Management: Planning for the Inevitable. New York, NY: AMACOM, A division of American Management Association, pp. 168-202.

Fruedenheim, M.., Giniger H., & Levine, R. (1985, March 24). Bhophal's Fatal Chain of Events. The New York Times, section 4, p. 2.

Kirkland, I. R. Jr. (1985, January 7). Union Carbide: Coping with Catastrophe. Fortune Magazine.

Lerbinger, O. (1986). Managing Corporate Crisis. Boston, MA: Barrington Press, pp 11-40.

(1993) Seabee Combat Handbook, Non-Resident Training Course, U.S. Navy. Chemical, Biological and Radial Defense, Chapter 9, pp. 1-3. http://globalsecurity.org/military/library/policy/navy/nrtc/14234_ch9.pdf

Thomas, A. (1985). Effects of Chemical Warfare: A Selective Review and Bibliography of British State Papers. Solna, Sweeden: SIPRI, pp. 5, 10, 47.

Weisman, S. R. (1985, March 31). Disabling and Incurable Ailments Still Affect Thousands. The New York Times, section 1 p. 1.

Weisman, S. R. (1985, December 1). Bhopal is in Midst of Grim Recovery One Year After Leak. The New York Times, section 1, p. 1.

Chernobyl and Radiological Events

(1986, May 3). Catastrophe at Chernobyl. The Economist, p. 13.

(1986, May 10). The Cloud Over Russia's Crops and Energy. The Economist, p65.

(1996). Brama Assorted Maps and Pictures Pertaining to Chernobyl. brama.com.
http://www.brama.com/ukraine/cbyl.html

(1996). Chernobyl 10 Years After Photo Archive. Greenpeace.org.
http://archive.greenpeace.org/~comms/nukes/chernob/cherfoto.html

(2000, June 13) Chernobyl 'not so deadly. BBC Online.
http://news.bbc.co.uk/l/hi/world/europe/789822.stm

Bar'yakhtar, V., Poyarkov, V., Kholosha, V., & Shteinberg, N. (2000). The Accident: Chronology, Causes, and Releases, p.5-21; The Shelter, Containing the Destroyed Reactor, p. 35-47. In Vargo, G. J. (Ed.), The Chornobyl Accident: A Comprehensive Risk Assessment. Columbus, Ohio: Battelle Press.

Kholosha, V., & Poyarkov, V. (2000). Economy: Chernobyl Accident Losses, p. 209-221. In Vargo, G. J. (Ed.), The Chornobyl Accident: A Comprehensive Risk Assessment. Columbus, Ohio: Battelle Press.

(2000, June 13). Chernobyl 'not so deadly.' BBC News Online.
http://news.bbc.co.uk/1/hi/world/europe/789822.stm

(2002). Chernobyl: Assessment Of Radiological And Health Impacts; 2002 Update of Chernobyl Ten Years. Nuclear Energy Agency Organisation For Economic Co-Operation And Development.

(2003). Responding to Radiation Attacks. Council on Foreign Relations.
http://www.terrorismanswers.com/security/radiation.html

(2003, April 24). Chernobyl Officials Admit Danger of Sarcophagus Collapse. The Wall Street Journal.
http://online.wsj.com/article/0,,BT_CO_20030424_015079-search,00.html?collection=autowire%2F30day&vql_string=chernobyl+and+shelter%3Cin%3E%28article%2Dbody%29

(2003, May 6). Ukraine Plans to Repair Chernobyl Plant to Prevent Leaks. The Wall Street Journal.
http://online.wsj.com/article/0,,BT_CO_20030506_006693-search,00.html?collection=autowire%2F30day&vql_string=chernobyl+and+shel

ter%3Cin%3E%28article%2Dbody%29

Barnathan, J., Strasser, S., Barry, J., & Cook W. J. (1986, May 12). The Chernobyl Syndrome. Newsweek, p22.

Chaze, W. L., Santini, M., & Daniloff, N. (1986, May 19). Living Dangerously; Chernobyl's Fiery Story. U.S. News and World Report, p. 23.

Holstein, W. J., Hall, A., Glasgall, W. (1986, May 12). Russia's Nuclear Nightmare. Business Week, p. 24.

Karon, T., & Thompson, M. (2002, June 10). The Dirty Bomb Scenario. Time.com.
http://www.time.com/time/nation/article/0,8599,182637,00.html

Markham, M. A. (1996) Chernobyl.com Photographs.
http://www.chernobyl.com/chernobylphotos.htm

(1993) Seabee Combat Handbook, Non-Resident Training Course, U.S. Navy. Chemical, Biological and Radial Defense, Chapter 9, pp. 1-3.
http://globalsecurity.org/military/library/policy/navy/nrtc/14234_ch9.pdf

Schmidt, K. (1995, July 17). The Truly Wildlife Around Chernobyl. U.S. News and World Report, vol. 119, no. 3, p. 51.

Visscher, Ross. Chernobyl Nuclear Disaster Website.
http://www.chernobyl.co.uk/

Whitaker, M., Newell, D., Strasser, S., & Coleman, F. (1986, May 12). Business as Usual? Newsweek, p34

Infrastructure Attacks

(2001, October 21). Utah's 'Black Ice': Cyber-attack Scenario. CNN.com.
http://www.cnn.com/2001/TECH/ptech/10/21/black.ice.idg/

(2001, October 31). Australian Hijacker Jailed for Disrupting Sewage System. Ananova.
http://www.ananova.com/news/story/sm_438245.html?menu=news.technology

(2002). Cyberattacks: The Results of the Gartner/Naval War College Simulation. Gartner Inc.
http://www4.gartner.com/2_events/audioconferences/dph/dph.html

Caldwell, F., Hunter, R., Bace, J. (2002). 'Digital Pearl Harbor' War Game Explores 'Cyberterrorism.' Gartner Research, E-17-6580.

Green, G. (2001, October 17). Hacker Caused Sewage Overflows, Court Told. Nationwide News Pty Ld. Courier Mail, p.11.

Green, G. (2001, November 1). Hacker Jailed for Sewage Sabotage. Nationwide News Pty Ld. Courier Mail, p. 4.

Garrison, L. & Grand, M. (2002, June 15). Wastewater Control Systems: Australian Case Illustrates Threat and Risks. NIPC Highlights, vol. 2-3, p. 4-6. http://www.nipc.gov/publications/highlights/2002/highlight02-03.htm

Smith, T. (2001, October). Hacker Jailed for Revenge Sewage Attacks. The Register.
http://www.theregister.co.uk/content/4/22579.html

Tagg, L. (2001, November). Aussie Hacker Jailed for Sewage Attacks. Iafrica.com.
http://cooltech.iafrica.com/technews/837110.htm

Townsend, I. (2001, November 2). Queensland Cyber Attack Smells of Vulnerability. Australian Broadcasting Corporation.
http://www.abc.net.au/worldtoday/s406755.htm

Verton, D. (2001, October 18). Black Ice Scenario Sheds Light on Future Threats to Critical Systems. Computerworld.
http://www.computerworld.com/securitytopics/security/story/0,10801,64877,00.html

Directed Attacks

(1999, May 11). Was the White House Attacked? ZDNet.com.
http://zdnet.com.com/2100-11-514615.html.

(2000, March). By the Numbers. Information Security, pg 12.

(2002, December 27). Falun Gong Members Jailed for Hijacking China TV Signal. Dow Jones Newswires, The Wall Street Journal Online.

(2003, March 28). Al-Jazeera Web Traffic Hijacked. The Boston Globe, p. A20.

De La Rosa, B. (2000, February 16). Yahoo! Amazon and Ebay Fall Victim to DOS Attacks. Network News, pg 3.

Kapadia, R. (2003, March 25). New Al-Jazeera Web Site Runs Into Headaches. Yahoo News.

Kirby, C. (2000, February 9). Net Hackers Strike Again. The San Francisco Chronicle, p. A1.

Larsen, A. K. (1999, July 12). Global Security Survey Virus Attack. Information Week.

Mueller, M. (1999, August 1). Computer 'crackers' Sets Sights on .gov for Chaos. The Boston Herald, p. 001.

Schwartz, J., Cha, A. E., Vise, D. A. (2000, February 10). Hackers Attack Top Web Sites for Third Day; Government Launches Probe. The Washington Post, p. A01.

Stross, R. (2001, June 18). Malicious Mischief. U.S. News & World Report, p38.

Melissa

(1999, April 8). Backbytes; A Deadly Fe-mail. Computing.

(1999, April 12). A Virus that Messes With Your Addresses. Newsweek, p. 62.

Alexander, G. (1999, April 4). Sabotage by Computer Hackers Costs Big Business Millions. Sunday Times.

Bray, H. (1999, March 30). Computer Virus Melissa Leaves Many Users Reeling. The Boston Globe, p. A1.

Goodwin, B. (2001, January 25). Firms Block E-Mail As Melissa Strikes Again." Computer Weekly, p. 33.

Lemos, R. (1999, March 28). IT Experts Scramble to Stop Melissa. ZDNet.com.
http://zdnet.com.com/2100-11-514161.html?legacy=zdnn

Lemos, R. (1999, November 18). Spies Hit Disney? No, Just Melissa. ZDNet.com.
http://news.zdnet.co.uk/story/0,,s2075269,00.html

Levy, S., Croal, N., Stone, B., Roberts, E., & Reno, J. (1999, April 12).

Biting Back at the Wily Melissa. Newsweek, p. 62.

Mitchell, I. (1999, May 27). The Problem – Security Policy, After Melissa. Computer Weekly, p 33.

Sandberg, J. (1999, April 12). The Friendly Virus. Newsweek, p. 65.

Verton, D. (1999, March 31). Melissa Takes Down Marine Corps e-Mail. CNN.com. http://www.cnn.com/TECH/computing/9903/31/melissamarine.idg/index.html

Love Bug

(2000, May 4). Mimos Hands a Warning as World Counts Cost of Love. New Straits Times, p. 1.

(2000, May 4). CERT® Advisory CA-2000-04 Love Letter Worm. CERT.org. http://www.cert.org/advisories/CA-2000-04.html

Brister, K. (2001, July 25). Code Red Virus Hit State Computers Hard. The Atlanta Journal and Constitution, pg 10D.

Compton, Jason. (2000, May 29). Get Immunized: Don't Let an Email Virus Infect Your Customers' Systems. VAR Business, vol XVI, no. 11, p. 56,58.

Goodwin, B. (2001, January 25). Firms Block E-Mail As Melissa Strikes Again." Computer Weekly, p. 33.

Meek, J. (2000, May 5). Love Bug Virus Creates Worldwide Chaos. The Guardian, p. 1.

Moskowitz, R. (2000, February 7). Crime and Punishment. Network Computing

Ruppe, D. (2000, May 4). 'Love Bug' Travels the Globe. ABCNEWS.com. http://abcnews.go.com/sections/world/DailyNews/lovebug00503_world.html

Wells, Amanda. (2000, May 8). It's a Long Haul to Clean Up Love Bug Virus. Infotech Weekly, Edition 2, p. 4.

Code Red

(2001, July 17). Code Red Advisory. eEye Digital Security. http://www.eeye.com/html/Research/Advisories/AL20010717.html

(2001, July 19). With New IIS Worm, Security Practices Questioned. The Industry Standard.

(2001 August). Code Red Virus Hits Cap Gemini. Het Financiele Dagblad, p. 8.

(2001, August 6). Time For Code Red II. The Industry Standard.

(2001, August 9) 'Code Red' Impact Felt at Major Companies. CNN.com. http://www.cnn.com/2001/TECH/internet/08/09/code.red

(2001, August 9). Code Red II Spreads In Asia. The Industry Standard.

(2001, August 9). Study: Code Red Costs Top $2 Billion. The Industry Standard.

(2001, August 10). Code Red Infected Microsoft Hotmail Servers. Computerwire.

(2001, August 10). Fedex Corp. The Wall Street Journal, section B, p. 2.

(4 September 2001). Code Red Computer Worm Cost set at $2.6 Billion. The Houston Chronicle.

(2001, October 5). More ISPs Disconnect Nimda Victims. Computerwire.

Brister, K. (2001, July 25). Code Red Virus Hit State Computers Hard. The Atlanta Journal and Constitution, p10D.

Buncombe, A. (31 July 2001). Global Alert Over Computer Worm. The Independent, p. 1.

Chan, S. P. (2001, July 21). Virus Hits White House Website. The Seattle Times, p. D1.

Doyle, E. (2001, August 2). Net Under Threat from Code Red Worm. Computer Weekly, p. 22.

Hopkins, J. & Farrell G. (2001, August 20). Code Red's Lesson: Act Fast! USA Today, pg 1B.

Hopkins, J. (2001, August 10). Code Red Worm an Exclusive Target. USA Today, p. 1A.

Hulme, G. V. (2001, September 24). Nimda Infects Thousands of Internal Networks. InformationWeek, p. 31.

Kirby, C. (2001, July 31). Web Facing New Code Red Attack Today; Second Coming May be Worse. The San Francisco Chronicle, p. E1.

Lemos, R. (2001, July 27). Virulent Worm Calls Into Doubt our Ability to Protect Net. CNET.com.
http://news.com.com/2009-1001-270471.html

Leuning, E. (2001, August 9). Code Red Hits Hotmail, FedEx Servers. CNET.com.
http://news.com.com/2100-1001-271357.html?legacy=cnet

Moore, D., Shannon, C., & Brown, J. (2002). Code-Red: A Case Study on the Spread and Victims of an Internet Worm. CAIDA.org.
http://www.caida.org/outreach/papers/2002/codered/codered.pdf

Musgrove, M. (2001, September 20). Computer Worm Called More Potent Than Predecessors. The Washington Post, p. E03.

O'Clery, C. (2001, August 1). FBI Remains on Alert as 'Code Red' Virus Infects Swiss Firms. The Irish Times, p. 15.

Peachy, P. (2001, August 2). Late Appearance by Code Red Internet Worm Leaves Most Websites Unscathed. The Independent (London), p. 2.

Smith, M. (2001, August 8). Discovery of Code Red II Computer Virus Sparks Another International Alert. The Herald (Glasgow), p. 20.

Strunk, S. (2001, August 13). Code Red Worm – Importance of Swiftly Eliminating Vulnerability. SANS.org.
http://www.sans.org/rr/malicious/code_red4.php

SQL Slammer Worm, January, 2003

(2003, January 25). CERT®-Advisory 2003-04 MS-SQL Server Worm. CERT.org. http://www.cert.org/advisories/CA-2003-04.html

(2003, January 25). Internet Attack Disrupts Asia and Europe. Associated Press.

(2003, January 27). Companies Recovering Well After Computer Worm Attack; Los Angeles Times, part 3, p. 3.

(2003, January 27). Internet Worm's Havoc Exposes Vulnerabilities. The Associated Press.

(2003, January 27). S. Korean Financial Sector: No Major Problems From 'Slammer.' The Wall Street Journal.

(2003, February 10). Security – Slammer Costs $1BN. Computer Reseller News.

Bajkowski, J. (2003, February 5). AmEx Site Holed up By Slammer Worm. Computerworld. http://www.computerworld.co.nz/webhome.nsf/UNID/8C2805B74C653290CC256CC3000678B2!opendocument

Barker, G. (2003, January 27). Global Worming Brings The Net to its Knees. The Age (Melbourne), p. 5.

Broersma, M. (2003, January 27). UK Sites Hit by SQL Worm. ZDNet.com. http://news.zdnet.co.uk/story/0,,t269-s2129363,00.html.

Krebs, B. (2003, January 26). Internet Worm Hits Airlines, Banks. The Washington Post. http://www.washingtonpost.com/ac2/wp-dyn?pagename=article&node=&contentId=A46928-2003Jan26&notFound=true

Lemos, R. (2003, January 31). Counting the Cost of Slammer. CNET.com. http://news.com.com/2100-1001-982955.html

Miller, S. K. (2003, January). ISPs Shutting off the Tap. Information Security, p. 14.

Moore, D., Paxson, V., Savage, S., Shannon, C., Staniford, S., & Weaver, N. (2003, January). The Spread of the Sapphire/Slammer Worm.

Caida.org.
http://www.caida.org/outreach/papers/2003/sapphire/sapphire.html

O'Harrow, R. Jr. & Cha, A. E. (2003, January 29). Internet Worm Unearths New Holes. The Washington Post, pg A01.

Richmond, R. (2003, January 27). Companies Continue to Wrestle With Slammer Computer Worm. The Wall Street Journal Online.
http://online.wsj.com/article_print/0,,BT_CO_20030127_007064,00.html

Seiberg, D. & Bash, D. (2003, January 26). Computer Worm Grounds Flights, ATMs. CNN.com.
http://www.cnn.com/2003/TECH/internet/01/25/internet.attack/