

LESSONS LEARNED FROM
KATRINA, SARS, and
OTHER DISASTERS¹

Barbara Frederiksen
Senior Managing Consultant
Johnson-Laird, Inc.
850 NW Summit Avenue
Portland, Oregon 97210
Tel: (503) 274-0784
Fax: (503) 274-0512
Email: barb@jli.com

Barb Frederiksen is the Senior Managing Consultant for Johnson-Laird, Inc., in Portland, Oregon. Barb is a forensic software analyst specializing in the analysis of computer-based evidence for copyright, patent, and trade secret litigation. She is also an expert in computer software design and development, the recovery, preservation, and analysis of computer-based evidence, and computer systems' capacity issues.

¹ Portions of this paper were previously presented as a part of *Significant Developments in Computer and Cyberspace Law*, University of Dayton School of Law (June, 2006).

TABLE OF CONTENTS

LESSONS LEARNED FROM KATRINA, SARS, AND OTHER DISASTERS

Barbara Frederiksen

I. INTRODUCTION	3
II. THE NATURE OF DISASTERS	4
III. FOUNDATIONS FOR BUSINESS CONTINUANCE	6
IV. PERSONNEL DISRUPTIONS	7
V. PHYSICAL DISRUPTIONS	8
VI. INFORMATION DISRUPTIONS	8
VII. INFORMATION DISRUPTIONS – SAMPLE CASES.....	11
VIII. CONTINGENCY PLANNING.....	19
IX. USEFUL TECHNOLOGY	24
X. CONCLUSION.....	30
XI. APPENDIX	32

I. INTRODUCTION

The last five years have presented us with the destruction of the World Trade Center towers by terrorists, an Asian tsunami that killed 186,000, the devastation of hurricanes Katrina and Rita, the flooding of New Orleans, the Kashmir earthquake, an act of bio-terror in the form of mailed Anthrax, and North American outbreaks of SARS, West Nile, and Bovine Spongiform Encephalopathy (“BSE” or “Mad Cow Disease”).

Some of the events listed above occurred without warning, while others were tracked by the media for days, and in some cases even months, before they struck home. In most cases the threat itself was recognized in advance, but the timing and magnitude of the event unpredictable. Each of these events underscores the value of emergency preparation and planning, as well as the dire truth that planning can mitigate outcomes, but not entirely stave off disastrous events.

The United States has almost 20,000 nautical milesⁱ of coastline vulnerable to tsunamis, 160 active volcanoesⁱⁱ, and major cities that straddle geologic faults. We now face the onset of the 2006 hurricane season and a possible pandemic of the H5N1 Avian flu. We cannot predict the exact nature, consequence, or duration of our next disaster. We can however predict with certainty that one will eventually occur.

One of the lessons brought home by Katrina, SARS, and other disasters of the past few years is that contingency planning can help both to contain risk and mitigate damage, even when the precise nature and extent of the emergency cannot be determined in advance.

No matter how harshly one judges the efforts to evacuate New Orleans, it is still clear that things would have been far worse had the evacuation never happened. The fact

that it could have been better managed is self evident. As a first attempt at evacuating an entire city, it left much to be desired.

In some respects the response to SARS appears to have been more successful than the response to Katrina, but as with the Katrina evacuations, the SARS response effort identified many problems. Limitations on response capacity, coordination between local, regional, national, and international authorities, intelligence gathering, and communication all emerged as areas needing improvement.

Katrina is an example of a disaster that strikes first at physical assets; while SARS is an example of a disaster that strikes first at people. This paper will also discuss a third type of disaster, which strikes first at information assets. This paper will compare and contrast the characteristics of these different disasters and discuss the way in which the type of disaster interacts with the creation and refinement of a disaster recovery or business contingency plan.

II. THE NATURE OF DISASTERS

A comparison of Katrina and SARS offers some interesting contrasts and parallels, as well as lessons learned with respect to both the nature of disasters and our responses to them. The two events provide examples of very different types of disasters, requiring very different responses, but posing many very similar problems.

Hurricane Katrina and the subsequent flooding presented a disaster that developed in a matter of days. Even so, most residents had at least some warning before the hurricane hit, and its approximate time of arrival could be predicted with a certain amount of confidence. A large area of the country, including portions of a major city, was damaged so severely that they were literally rendered uninhabitable. Vital services such

as power and communication were disrupted over a widespread area, and residents were forced to flee or face life threatening conditions. In many areas survivors who remained behind were stranded without access to transportation, shelter, food, water, medical care, communication, or sanitation. Despite the wide-spread nature of the disaster, there were still comparatively clear boundaries between the effected areas and the unaffected. The official strategy for coping with Katrina was evacuation to a safer area, at least as an initial response.

By contrast, the SARS epidemic continued to gain momentum over a period of months rather than days. It damaged people but left property and vital services largely intact. The SARS epidemic had no clear boundaries, and appeared in multiple countries with no warning as to where it might strike next. It was an invisible threat that moved very quickly and lacked geographical boundaries. Within a short time after its arrival in Hong Kong it had circled the globe. Victims, their families, and their neighbors were requested to stay put, subject to restrictions on travel, mandatory closure of some public facilities, and quarantine for those infected. The primary strategy for coping with SARS was containment.

These diverse events, despite their differences, are both characterized as “disasters” — that is, an emergency or situation that causes (or has the potential to cause) significant injuries or deaths, or a threat that can cause physical or environmental damage, disrupt operations, threaten financial standing, or destroy the ability of its victims to do business and conduct normal activities. Disasters can occur as localized, regional, national, or global events.

As demonstrated by the comparison above, the characteristics of a particular

“disaster” will be specific to the context in which it occurs. Despite this, these disasters share a number of important characteristics with respect to the problems they present:

- The extent of the damage and disruption were not known in advance
- The disasters required a suspension of “normal operations”
- The duration of the disruption was underestimated
- Delays in recognizing the severity of the threat adversely impacted initial responses
- Information deficits negatively affected both evacuation and containment efforts
- Communication problems hampered problem management
- Impaired communication and poor coordination affected both responders and victims
- Inter-agency collaboration was required at multiple levels (i.e. local, regional, national, and in the case of SARS, international)

III. FOUNDATIONS FOR BUSINESS CONTINUANCE

In planning our response to disasters or other emergency situations, it is important to recognize that normal operation of both our businesses and our social structure rests upon three resources: personnel, physical assets, and information.

The category of personnel resources embraces both people and the skills they have, because the normal operation of a business or a society requires both the availability of sufficient able personnel to carry the workload, and that the individuals who compose the work force possess the skills and training required in performing their various roles.

Physical resources include the structures that shelter our homes and businesses, as well as the assets that provide essential elements such as electricity, water, food, sanitation services, transportation capabilities, communication lines, and manufacturing resources. These assets must all be secure and operational for “business as usual” to continue.

Information resources include the ability to collect and store data, the ability to process the data into useful information, and the ability to effectively exchange information with others. Examples of information assets include a business’s financial data, contact lists, inventory records, information processing capabilities, and the communication capabilities that enable management, supply chain, and commerce.

A disaster occurs when one or more of these resources is disrupted or threatened. The disruption may be local, regional, national, or global in nature, but for planning purposes can be distinguished by some common characteristics.

IV. PERSONNEL DISRUPTIONS

With personnel disruptions such as pandemic illnesses, food-borne epidemics, and civil disturbances, the physical assets of a business may be intact and fully functional, but key personnel are either unavailable or unable to report to work in their normal setting. These types of threats may require special security and access provisions, quarantine measures, development of alternate command and communication hierarchies, and special provisions relating to knowledge transfer and contingent work force. Restrictions on physical access or travel may also require a company to alter the location from which employees work, for instance by encouraging telecommuting or off-site operations. These changes may in turn necessitate other adjustments, such as the need to provide

clients and suppliers with alternate contacts, phone numbers, addresses, and delivery instructions. Special planning may be required to address basic requirements such as health care, sanitation, and child care because the response to civil disturbances or widespread illnesses may involve quarantines, travel restrictions, school closures, and suspension or limitations placed on public services.

V. PHYSICAL DISRUPTIONS

Disruptions of the physical environment, which include threats such as fire, flood, earthquake, hurricane, acts of terror or arson, radiological accidents and hazardous materials incidents require the relocation of physical operations. At a minimum, these types of threats will involve the need to evacuate from the threatened locale, to subsequently secure alternate facilities, and to transport people, supplies, and materials to the new location.

VI. INFORMATION DISRUPTIONS

Information or communication disruptions occur when an information resource becomes unavailable or when its integrity is no longer trustworthy. Resource availability can be impacted by failures that occur primarily in one of three areas: The data is damaged, the ability to process the data is damaged, or the data is rendered inaccessible. Disruptions relating to data integrity can occur when the ability to verify data accuracy or authenticity becomes suspect. It is interesting to note that in this final scenario, no actual damage need occur, since only the data's trustworthiness need be called into question to precipitate a disruption.

With an information disruption, both physical facilities and personnel may be

unharmful, but key software, data systems, or communication capabilities are inoperative due to accidental or malicious causes. Information disruptions can affect the availability of vital services such as communication, transportation, energy, and emergency response. They may also impact commerce or manufacturing capabilities, or precipitate unsafe conditions such as hazardous material incidents.

Information disruptions may occur as isolated primary disaster events, or in the context of other disasters such as earthquakes or hurricanes. The restoration of information resources and provision for access thereto are therefore key components that must be considered as a part of any contingency plan.

Unlike physical and personnel disasters, the cause underlying an information disruption may not be readily apparent. In these cases one must act as quickly as possible to prevent further harm, and also to capture a precise record of the state of the system at the time of the event so that the cause and full extent of the damage may be determined. Responses to address information disruptions must address three distinct priorities – to contain the damage, to preserve a record of what happened, and to restore normal operations. This is particularly true in cases where the security of a computer system has been breached or where sensitive data may have been damaged or stolen.

Information disruptions may result from internal causes such as hardware failures, software malfunctions, and data corruption. These types of information disruption have much in common with physical threats in so far as they normally occur abruptly and announce themselves clearly. As is the case with physical disasters, these events require the damaged asset to be repaired or rebuilt.

In some cases, such as software failures or unauthorized access, it may be difficult

to determine with specificity what, if any, damage has occurred. Unlike disasters affecting physical counterparts, additional steps beyond simple repair may be required to fully identify and remedy the damage or to determine the integrity of the data. This is especially true if incorrect or incomplete information could have been provided to customers, downstream processors, or regulatory agencies.

A second type of information or communication disruption may result from external causes such as virus attacks, hacking incidents, data theft, Denial of Service (DoS) attacks, sabotage, or acts of cyber-terrorism. The damage from many of these events may spread if unchecked. The response for computers infected by virus or Trojan, or the discovery of unauthorized access in a computer system has much in common with the response used to cope with infectious disease. These types of threats require immediate steps to contain the damage by isolating the compromised system. Compromised systems should be disconnected from both the remainder of the network and from the internet.

As with an infectious disease, it is important to determine what interactions the compromised system has had with the outside world in order to determine the scope of the possible infection or damage. Once the compromised system is isolated, and before any repair is attempted, forensic backups should be made to preserve evidence of the damaging event and to aid in post-recovery diagnosis to determine the extent of exposure to other systems and data. If recovery is attempted before a backup is made, vital evidence may be irretrievably lost.

A third type of information emergency may occur with data theft. Unlike theft of physical assets, data theft may occur while the rightful owner still has full possession and

use of their data. The focus with respect to data theft is not on recovery of the data asset but on containing the damage that may occur as a result of the theft. This may require reporting the theft to customers or regulatory agencies, taking direct action to preserve customer good will and trust, determining how to deal with the press, and assessing legal exposure.

It is important to note that at the outset, it may not be possible to distinguish between information disruptions that are caused by internal events and those caused by external events. Any information loss or data damage may also have unforeseen downstream effects. Because of this, it is especially important to preserve information that can be used to diagnose the cause of the failure and extent of damage before it is destroyed by recovery efforts.

VII. INFORMATION DISRUPTIONS – SAMPLE CASES

Since threats that directly effect information systems are perhaps less familiar than traditional disaster scenarios, it may be useful to examine a sample of these threats in greater detail before moving on to a discussion of contingency planning.

Historically, information disruptions were primarily the result of failed software, hardware or human error, but the incidence of disruptions that arise from some form of malicious behavior such as sabotage has been increasing steadily. For example, 22.7 % of the respondents to the FBI's 2005 Computer Crime Survey reported that they had dealt with some form of data or network sabotage in the previous 12 monthsⁱⁱⁱ.

A joint study by The US Secret Service and Carnegie Mellon Engineering Institute that focused on the threats posed by current and former employees (“insiders”) suggests that with respect to insider threats, at the time of the incident, 59% of the

perpetrators were former employees and contractors, and 41% were current employees or contractors. This statistic seems to be consistent with 2005 CSI/FBI Computer Crime and Security Survey, which found that incidents involving unauthorized computer use were fairly evenly divided between internal and external sources.

As an example of the potential damage caused by internal sabotage, consider the following examples:

Tim Lloyd of Wilmington, Del., planted malicious software that served as a “software bomb” in a centralized file server at Omega Engineering's Bridgeport, N.J., manufacturing plant. This software bomb was designed to destroy critical files that were used to control the companies manufacturing processes. In order to maximize the damage, Mr. Lloyd first made sure that all of the target files were present on a single computer, and then destroyed the contents of backup tapes that might contain a copy of these files. Once activated, this software bomb succeeded in destroying the programs that ran the company's manufacturing, costing Omega more than \$10 million in losses, \$2 million in reprogramming costs, and eventually leading to 80 layoffs.^{iv} It also cost the company its competitive footing in the high-tech instrument and measurement market.

In November of 2005, Pok Soeng “Freddie” Kwong sabotaged the computer systems of his former employer, American Flood Research (“AFR”), in Plano, Texas. At trial, it was revealed that Mr. Kwong had conspired over an 11 month period to sabotage AFR’s computers so that they stopped functioning, and also deleted critical business information, thereby preventing AFR from conducting business. Kwong and an accomplice also programmed the computer system to erase evidence of their attacks^v, rendering both diagnosis and repair more difficult.

Even without malicious intent, data corruption can occur as the result of hardware failure, software failure, media failure, data transmission errors, or human errors. Once corrupted, the data must be repaired and tested, or recovered from a backup known to be good, before the data can be deemed reliable. Compromise of critical data or systems can render their integrity uncertain, even when the systems appear to operate correctly. The impact of this uncertainty on consumer confidence or internal operations can be devastating.

As a case in point, consider the activities of the international terrorist group Aum Shinrikyo. The Aum Shinrikyo were responsible for the 1995 Sarin gas attack in a Tokyo subway that injured 5000 people and left 12 dead. Less well known is the fact that in 2000, a Japanese police department discovered that its computerized vehicle tracking software had been written by a programmer with ties to Aum Shinrikyo, and that until this discovery Aum Shinrikyo had been compiling data about the whereabouts of both marked and unmarked police vehicles using this program. In the investigation that followed, it was discovered that other members of Aum Shinrikyo had been working as subcontractors for various computer programming firms, and had developed software for at least 80 Japanese businesses and 10 different government agencies. Because these programmers were serving as subcontractors, it was nearly impossible to determine what systems they had actually created, let alone what additional systems they may have been able to access from their vantage inside the firewall of these companies^{vi}.

Threats to data integrity such as attempts to manipulate stock prices, bank transfers, or the foreign currency values can potentially destroy the financial standing of a business or damage an entire segment of the economy. The impact of uncertainty on

consumer confidence or internal operations can be devastating, especially when projected into international markets.

Even without malicious intent, software malfunctions can also cause large scale disruptions with potentially disastrous consequence. The August 14, 2003 power blackout that crippled most of the Northeast corridor of the United States and parts of Canada is a prime example. The blackout was triggered^{vii} when an engineer disabled an automatic software process that allowed the utility to determine power status for its region^{viii}. The engineer forgot to re-enable the software before he went to lunch. Two hours later the utilities Alarm and Event Processing Routine began to malfunction, causing the server it ran on to crash and setting off a chain of cascading software failures that led to a blackout which affected 50 million people. Power was not restored for four days in some areas of the United States, and some parts of Ontario suffered rolling blackouts for over a week. The total cost for this outage in the United States is estimated to be between \$4 billion and \$10 billion (U.S. Dollars). In Ontario, there was a net loss of 18.9 million work hours, and manufacturing and shipping in Ontario were down \$2.3 billion (Canadian dollars)^{ix}.

Threats to information assets that originate from outside sources must not be overlooked. These threats include damage from unauthorized intrusion, virus attacks, data theft, denial of service attacks, and acts of cyber terrorism.

As the technology to protect against external threats evolves, so do the threats. Despite evidence that organizations are investing in more, and more varied, security technologies, 87% of the respondents to the FBI 2005 Computer Crime Survey indicated that they experienced one or more computer incidents during the previous year. Nearly

100% of the respondents to this survey said they used anti-virus software, but even so, 83.7 % reported that they had dealt with some form of virus, worm, or Trojan infection in the previous 12 months^x.

Although incidents involving virus or Trojan infections are often detected before substantial harm can be done, a clever virus or Trojan can be programmed to lie dormant and wait for some predetermined event or date to occur before activating. The risk with these silent intruders is that they may contaminate backup media before they are detected, rendering the recovery of files they infect or damage far more difficult.

The theft of sensitive consumer data also has the potential to generate disastrous consequences. Loss of consumer confidence and the potential of subsequent liability litigation could prove disastrous for a business, especially if the business is found to be negligent in their handling of consumer data.

There is also an emerging trend for political activists to use hacking techniques of target web sites, with the intent to disrupt the target's normal operations. This so-called "hacktivism" covers a spectrum of activities from virtual sit-ins, virtual blockades, automated e-mail bombs^{xi}, Distributed Denial of Service ("DDoS") attacks, computer break-ins, and computer viruses and worms.

For example, during the Kosovo conflict in 1999, NATO computers were blasted with e-mail bombs and hit with denial-of-service attacks by hacktivists protesting the NATO bombings. In addition, businesses, public organizations, and academic institutes reported receiving highly politicized virus-laden e-mails from a range of Eastern European countries. Web defacements were also common. After the Chinese Embassy was accidentally bombed in Belgrade, Chinese hacktivists posted messages such as "We

won't stop attacking until the war stops!" on U.S. government Web sites.

Virtual sit-in and other forms of blockade, where activists generate so much traffic against a web site that it blocks out normal traffic are becoming common forms of protest. To facilitate such activities, the organizers may set up special web sites that allow participants to download and install software which then automatically accesses the target site every few seconds.

Distributed Denial of Service, or DDoS attacks are also becoming more common. During a DDoS attack, a target site is flooded with bogus traffic, typically generated by hundreds to thousands of security-compromised ("zombie") machines. The zombies are computers that have unknowingly been infected with automated software used to perform the DDoS attack. Once infected, zombies wait passively until they receive the command to attack and then begin sending a flood of requests to the target system. A single DDoS attack may continue for days, and typically disrupts entirely the normal operation of the target server. Of the 2066 respondents to the FBI's 2005 computer crime survey, 14.5% responded that they had detected at least one DDoS attack against their computer systems in the previous 12 months.^{xii} Targets of such attacks have included military and government sites, businesses, news media, and consumer service sites.

The FBI defines cyber terrorism as "the premeditated, politically motivated attack against information, computer systems, computer programs, and data which result in violence against noncombatant targets by sub national groups or clandestine agents."^{xiii}

Although there have been comparatively few incidents documented as cyber terrorism, the degree to which all aspects of our lives have become dependant on computers presents a target-rich environment for terrorists. Factors such as the anonymity

of the internet, ready access to malicious software tools, lack of cyber-border guards or cyber-checkpoints, and freedom from geographic restrictions all suggest an opportunity ripe for exploitation by terrorists.

Computers perform much of the recordkeeping, computing, and communication tasks that fuel our economy. They are also used to provide monitoring and control functions that are required for the routing of telephone calls and electricity, monitoring of power production facilities, and record keeping related to the transportation of both people and material goods by road, rail, air, and water. Based on these capabilities, potential cyber terror targets include the infrastructures that support important services such as transportation, power, commerce, and communication, as well as those which provide support for emergency response services such as police, fire, and 911.

History shows that these systems have been the subject of targeted computer attacks in the past. Consider the following examples:

In 1989, a hacker group known as the Legion of Doom took over portions of the Bell Telephone system.

In 1997, a hacker disabled the computer system of an airport control tower in Worcester, Mass.

In 2002, Joseph D. Konopka, a.k.a. "Dr. Chaos" was indicted for cyber crimes that included the disruption of energy facilities, the disruption of telecommunication facilities, the disabling of air navigation facilities, intercepting electronic communications and causing damage to a protected computer^{xiv}.

Less obvious targets are vulnerable as well. For example, in 2000, a disgruntled consultant in Maroochy Shire, Australia hacked into a waste management control system,

and released millions of gallons of raw sewage into the town.

In February, 2004, the FBI agents arrested David Jeansonne, 43, of Metairie, Louisiana for sending an e-mail attaching malicious software to certain users of a WebTV service that, once opened, reprogrammed their computers to dial "9-1-1" instead of a local Internet access telephone number. The 9-1-1 calls caused by the e-mail resulted in the dispatch of police in locations from New York to California.

Even the government's own computer systems are not safe. In 2003, Brett Edward O'Keefe was charged in a six-count indictment for engaging in a conspiracy to access military, government and private sector computers. The defendant was the President of Forensic Tec Solutions, a computer security company located in San Diego, California. The object of the conspiracy was for O'Keefe and his co-conspirators to gain unauthorized access to government and military computers, copy computer files and take these files to the media in order to generate public visibility for his company. This would, in turn, lead to new clients and increased profits. According to the indictment, O'Keefe and his co-conspirators possessed files belonging to: the United States Army, United States Navy, Department of Energy and National Institutes of Health, and National Aeronautics and Space Administration (NASA)^{xv}.

Only a few days ago, Christopher Maxwell, of Vacaville, California, pleaded guilty to charges relating to computer malfunctions he caused at Seattle's Northwest Hospital in January, 2005. These disruptions affected the hospital's systems in numerous ways: doors to the operating rooms did not open, pagers did not work and computers in the intensive care unit shut down. Further investigations revealed that his intrusions also damaged the contents of military computers in the United States and overseas. In all,

Maxwell was able to access and infect more than 400 computers before he was caught.^{xvi}

VIII. CONTINGENCY PLANNING

During the response to a business disruption, a contingency plan can aid in bridging the gap between the disaster and a return to normal operations. Although the response to specific incidence will vary according to the type of threat, there are some overarching themes that will help focus the planning effort.

Regardless of the type of disaster, it is important to bear in mind that the goal of the plan you are developing is designed to return business to an operational state in a reasonable amount of time. This does not mean that everything will, or can, be the same as it is during normal operations. The presumption underlying the plan is that when the plan is executed it will be used because normal operations are not possible — you must transition to “Plan B” if business is to continue. The plan must therefore embrace a certain amount of uncertainty, and build in contingency options to deal with factors that may be unknown at the time the plan is actually used. The focus of recovery should initially be on those systems most crucial to the business.

By way of example, it is likely that at the outset the full extent of damage or disruption will be unknown, as will the availability and participation of key employees, service providers and suppliers. The duration of the disruption will be hard to predict. Normal lines of communication may not be available, and the post-disaster command structure for both your company and any responding agencies may be unclear.

It is also important to recognize that all of the individuals who respond during a disaster do so in the context of their own personal disasters. This means that individuals and organizations may have conflicting demands on their priorities, time, and availability.

Their ability to respond will be shaped as much by these demands as by their intentions to help.

As demonstrated with Katrina, plans for evacuation, travel, and accommodations may need to include children/spouses/parents/pets. In hindsight this seems obvious, but in the author's experience it is often overlooked. Employees who are part of the recovery effort may also be coping with dependant children, injuries, housing needs, transportation challenges, exhaustion, and personal tragedies.

In the face of such challenges, a clear, well documented plan can help assure both coordination and appropriate response to the crisis situation.

Whether you are beginning to develop a contingency plan, or in the process of revalidating a plan that already exists, it may be useful to consider the phases that are associated with risk management and disaster response:

1. Planning – The planning phase includes tasks relating to risk assessment, information gathering, analysis of business needs, preparation of the contingency plan itself, and education of those who are to participate in both planning and recovery efforts.
2. Preparation – This pre-disaster phase includes the preparation of backup copies and critical personnel and system records, as well as the actions required to stage these records to a safe location. Activities may also include additional preparations for evacuation or isolation, such as providing phone connections, Internet connections, supplies, and equipment at alternate site locations or negotiating off-site backup or processing contracts.

3. Crisis Survival and Triage – This phase occurs during and immediately after the disruption, it includes actions required to get through the crisis, as well as assessing damage, identifying and locating survivors, activating the contingency plan, identify communication and transportation resources, notify stakeholders, identify active first responders and aid agencies that may be able to offer information or guidance, and securing immediate needs such as medical assistance, water, food, shelter, and security.
4. Restoration/Transition – This is the phase that initiates business recovery and provides for the transition from disaster to some level of resumed operation. It includes reestablishing communication with employees, remote offices, clients, and the outside world, and restoration of critical business processing capability. Non-priority elements may be deferred for later recovery.
5. Business Resumption – During this phase, the critical processes of the business have been resumed, but it is likely that the business is operating from a temporary location. Less critical business systems may still be unavailable.
6. Return – This is return to full normal operations, either at the original or new location of the business.

A. SIMPLICITY, SUPPORT, AND SECURITY

To be helpful in a time of crisis, the contingency plan must be readily available, and simple to follow. It should contain sufficient detail to support recovery activities performed by staff (or contractors) who may be executing recovery processes that are unfamiliar to them. The inclusion of checklists and forms used to document recovery processes, expenses, asset and resource tracking (people, services, goods, and

information), and problem resolution can provide focus for the ongoing recovery effort, and serve as a knowledge resource when transitioning back to normal operations.

Since the plan may be executed by employees who have relocated to an unfamiliar site, the plan itself should contain addresses, phone numbers, and directions to help individuals locate the recovery site and local suppliers and services who can provide medical care, office supplies, electronic components and media such as cables, wireless cards and routers, blank tapes, and hard drives, food, shelter, copy and fax capabilities, and alternate cell phone service.

The need to establish alternative contingent communication protocols in advance was brought home during Katrina. Many evacuees discovered that even after they were outside the disaster area, the circuits that supported the 504 phone exchange were overloaded, and their New Orleans based cell phones were of marginal use for weeks after the disaster. They also discovered that although many employees fled with lap top computers, not all the laptops were equipped or configured to use wireless networks. Many organizations found themselves without the means to coalesce their scattered work force, and individuals were left wondering as to the whereabouts and wellbeing of their colleagues.

The plan should also include a list of technical support providers, temporary staffing agencies, and video conference providers who are local to the recovery site, should their services be needed during the recovery effort. It is a good idea to also include contact information for data recovery services, in case problems are encountered with critical backup media.

Another lesson learned during Katrina is that even materials spared from the crisis

itself may go missing during transportation to a new location. The contingency plan should consider physical safety of personnel, property, and information as people and goods are relocated and staged to new locations. I have listened to several first-hand accounts from New Orleans colleagues who describe the loss of laptops, electronic records, cameras, phones, videotapes, and hardcopy that survived the storm but were subsequently lost in transit, damaged, or stolen from hotels and temporary offices. The loss can occur as a result of theft, or from simple human errors such as mishandling, poor labeling, or inadequate shipping records. Even more tragic were the stories of family members who were separated from each other during the evacuation, and who had no way after the fact of providing emergency contact information that could help in reuniting them with their families.

Since the recovery plan may be executed by contingency staff or even contractors, the plan documentation should include both physical and electronic security requirements. Security standards should be defined for the transportation of data backups and physical assets, and should also provide standards for data and physical access during the subsequent recovery efforts.

It is worth noting that even absent a physical disaster, the steps taken to preserve critical information can themselves precipitate a disaster if the backup copies are not handled properly. For example, consider the following:

In February 2005, Bank of America reported that backup tapes containing customer and account information for 1.2 million federal employees. The loss occurred as tapes were being shipped to a backup data center.^{xvii}

In April of 2005, Ameritrade admitted that it had lost backup tapes containing

personal data of 200,000 current and former customers. This loss occurred as tapes were being shipped to an off-site storage facility.^{xviii}

A similar incident, involving theft of a device the size of an iPod that contained personal data on at least 26.5 million veterans from the home of a VA employee, may cost taxpayers as much as \$500 million^{xix}.

One of the best ways to safeguard information assets and sensitive data is to use encryption to ensure they are not subject to unauthorized access. If encryption is used, special considerations must be made to ensure the recovery team has access to any required decryption keys.

The contingency plan must also provide guidance for record keeping during the crisis and all phases of the recovery efforts. These records should track assets and expenditures, document recovery efforts and problems, log calls and follow-up, document departures from the procedures provided in the recovery plan, and prepare a record that will help ensure a smooth transition back to normal operations. A contemporaneous written record of the recovery effort can aid tremendously in determining the cause of problems that may occur as data and operational systems are recovered. This record keeping is also important to document expenditures that may be covered through insurance and disaster relief, and to provide the details that it can be used post-recovery to evaluate the effectiveness of the plan and help provide input into future planning efforts.

IX. USEFUL TECHNOLOGY

The steps required to fully implement and validate a contingency plan will be determined by the needs of your business. What follows are general observations gleaned

from my own experience and interviews with individuals who dealt directly with Katrina, SARS and events that damaged information assets. The appendix to this paper contains specific question lists which may be useful during your own planning process.

Individuals I spoke too about SARS and Katrina consistently cited communication, coordination, and the need for documentation and recordkeeping as major problem areas in their disaster response. In the cases of both SARS and Katrina, individuals were forced to try and resume their lives and businesses under conditions where they could not operate in their normal locations. Access to information appeared to be key problem areas for both survivors and responding agencies.

Advances in technology, coupled with the fact that cyberspace is not is not burdened with geography, can offer some assistance in dealing with these challenges. In addition to the suggestion noted below, consider storing copies of the disaster plan, contact lists, and other important documents on non-volatile media such as CDs, DVDs or thumb drives. Copies of these materials can be staged off-site at your firm offices in other cities or distributed to key employees. Sensitive documents can be encrypted to prevent unauthorized access.

A. TELEPHONE COMMUNICATION

During Katrina, all phone numbers in the 504 exchange, both land and cell, were paralyzed. Although some cell phones continued to operate, circuits were saturated and most calls could not go through. This continued to be a problem even weeks after residents had relocated to Houston, Atlanta, and other locations well outside the disaster zone.

Fortunately, “pay as you go” phones were readily available at outlets like Wal-

Mart and Target, allowing individuals to quickly secure alternate phone numbers. Of course this presented a challenge as to how to propagate the new numbers. In many cases this was accomplished via informal phone trees, and some individuals were not located for weeks.

In situations where voice calls could not be completed, text messaging often worked, but as one colleague remarked “only the kids knew how to send text messages on my phone – I had to ask my daughter for help!” Individuals with Blackberries and similar web enabled devices seemed to fare better, since e-mail addressed to their Blackberry e-mail IDs was still deliverable.

Another phone alternative exists in the form of voice over internet (VOIP) services such as Skype and Vonage. Since VOIP numbers are not coupled to geographic exchanges, they continue to function, requiring only an internet connection from which to operate.

VOIP services allow communication with both other VOIP users and traditional phone services, and it is even possible to have your normal phone number set up as a so-called “soft phone” associated with your VOIP account, so that when you are online you can receive calls that were not specifically directed to your VOIP identity. VOIP directory services such as Skype’s allow you to search by both name and e-mail address to locate other VOIP users.

B. E-MAIL COMMUNICATION

During Katrina, many evacuees discovered that although they fled with laptops, their computers were configured to use Internet Service Providers (“ISPs”) based within the disaster zone, so they had no immediate internet connectivity or e-mail. Although

many hotels, coffee shops, and airports offer the ability to connect to the internet, these connections do not automatically provide e-mail service. Individuals were forced to seek out alternate e-mail services such as those provided by Google, Yahoo, and MSN, and to establish new e-mail id's. Again, there was the problem of propagating the new ID to other evacuees. One potential solution to this problem is to partner with remote offices to set up alternate e-mail IDs for your employees as a part of your disaster plan. Another option would be to set up an e-mail address known to all, such as "disaster-your-company-name@gmail.com" which can be used as a clearinghouse for contact information and other crisis response directives. Individuals can send contact information or messages to this ID, or log on to the ID themselves to collect contact information sent by others.

Another problem faced by many evacuees was that they did not know how to change the settings on their laptops to enable wireless access, or they had older model computers that were not enabled for wireless communication, and did not know that inexpensive cards are available to add this capability.

In addition to facilitating e-mail communications and internet access, wireless capabilities can be helpful in establishing networks for collaborative work during recovery efforts and when the business must be resumed at a contingent location. Wireless networks can be set up much faster than traditional wired networks, and have the advantage that they do not require snaking cables between rooms, allowing private networks to be set up on the fly in hotels or other contingent locations.

Restoration of e-mail and web capabilities using your normal business domain name is comparatively simple. Your e-mail and web servers must be recovered, or

temporary alternates configured, and then the appropriate registry contacted to provide the new IP address for your domain name.

C. WORKING FROM REMOTE LOCATIONS

In order to enable telecommuting capabilities, individuals require the capability to connect to the corporate network or work autonomously from isolated computers. Generally, the ability to connect to a shared network offers numerous advantages, especially if individuals are isolated from their normal work environment. Individuals who travel frequently are probably familiar with connecting back to their office networks to access files via a Virtual Private Network (“VPN”) connection that allow for secure connection via the Internet. Connection via VP requires both authorization to the VPN server and setting up the appropriate configuration on the laptop.

Software such as Windows Remote Desktop allow employees to securely access and use all of the software programs and files on their normal office PC without reporting to the office. This capability is built into Windows PC, and available for other platforms including older Windows systems, Macintosh systems, and Linux systems. Similar capabilities are also provided by software that is readily available on the web at sites such as www.GoToMyPC.com.

Employees can work remotely and still collaborate on documents using software tools such as NetMeeting, which is built into the Windows operating system, or by using hosted web services such as Web-X www.GoToMeeting.com, and www.MeetMeNow.com. These tools allow the users to hold on-line meetings and to see the same desktop and to work in the same document from remote locations.

For problem resolution and configuration help, your system administrators can

use services such as www.HelpOnMyPC.com to establish a secure control of remote computers in order to help fix problems or set up communications. This service can also be used to provide training or collaborate on documents. [www.HelpOnMyPC](http://www.HelpOnMyPC.com) allows those who need help and those who can offer help to establish a connection by sharing a unique 12 digit code that keeps their session private. Once the session is established, the two see a common screen image and the helper can diagnose problems, eradicate viruses, or make changes to a user's computer configuration while the user observes.

To enable remote operations or telecommuting, it is helpful for key employees to have the capability to print, fax, and scan at their contingent locations. Software fax capabilities allow employees to prepare and send a fax directly from documents stored or created on their PC. If this software is supplemented with an attached scanner, even documents received in hard copy can readily be shared with others via either fax or e-mail.

Scanned documents stored on CD, DVD, or non-volatile media such as thumb drives have the advantage that they are extremely portable, comparatively safe from water damage, and capable of being encrypted to prevent unauthorized access.

If the ability to print or ship documents is required, the remote location should be equipped with printers and supplies such as paper and toner, as well as appropriate shipping and postage supplies.

Because files created at remote locations still need to be backed up, some thought should be given to how this can be accomplished. If employees are using Remote Desktop to access their office computers and servers, normal office backup procedures will be sufficient so long as the backup procedures are either fully automated or someone is

available to handle tape manual procedures such as mounting tapes or other media the backups require.

If backups are to be performed at the contingent site where an employee is working, the employee will need to know how to perform the backup, how to operate any required software or hardware, and to have available sufficient supplies of the backup media (i.e. tapes, CD, or disks).

A few cautionary notes are appropriate with respect to the use of these technologies. First and foremost is that most will require at least some minimal setup or training to use. These tasks are far easier to accomplish before a crisis than during one.

If employees are to be working from home or other contingent locations, it is also highly advisable that they use antivirus and firewall software. Firewall products such as Symantec's Internet Security Suite, Zone Alarm, or SunBelt's Kerio Personal Firewall are designed to protect the user's computer against unauthorized access from hackers, and are especially important to protect computers that are attached to the network through insecure networks at hotels, airports, and coffee shops.

Employees working remotely should also be educated on appropriate procedures to protect against theft and unauthorized access of their authentication data (i.e. network sign-on and password) and any sensitive data in their possession.

X. CONCLUSION

No contingency plan will ever be a perfect fit for the crisis it seeks to address, nor are we ever likely to develop a way of predicting our disasters with absolute precision. At best, we may have some advanced warning of the events that may disrupt our lives and businesses. Even so, individually and in conjunction with agencies at the local, state, and

federal levels we can form plans that can help us address a variety of emergency situations. A wealth of information is available to help us in these efforts. Some good sources include:

The Disaster Recovery Guide (Disaster Recovery Planning from A-Z) at <http://www.disaster-recovery-guide.com/>

The Disaster Recovery Journal (Sample Plans) at <http://www.disaster-recovery-guide.com/>

Business Guide to Pandemic Bird Flu Preparedness, available at <http://www.pandemicinfosite.com/bird-flu-business.htm>

Us Department of Homeland and Security Emergency Planning Guidelines at <http://www.ready.gov/business/index.html>

Business Continuity Planning / Disaster Recovery Planning (An On-Line Guide) at <http://www.yourwindow.to/business-continuity/>

XI. APPENDIX

A. DEVELOPING A CONTINGENCY PLAN

During the planning process it will be important to determine business recovery goals and prioritize systems to be recovered. The plan should consider business needs for then recovery effort itself, operations during the business resumption phase, and the eventual transition back to normal operations.

As a starting point, the plan should communicate decisions and contingency procedures with respect to the big “W” questions:

1. Who will prepare the plan?
2. Where will the plan be kept?
3. Who will need copies?
4. Who will carry it out?
5. What information and systems are critical to the business?
6. Where (and how) will this information be preserved?
7. What else will be needed to restore and operate these systems (hardware, software, staff, knowledge skills, empty media for backups, etc.)?
8. What or who can trigger activating the plan?
9. What records need to be kept?
10. Where will people go during an evacuation?
11. How will they find each other afterwards?
12. How will they respond if there is a need for quarantine?
13. Can recovery efforts be carried out remotely?
14. Once key systems are recovered, can business be conducted remotely, or must staff relocate?
15. Are there training needs associated with the recovery plan that extend beyond the recovery team?

16. When actions must be taken during recovery to pave the way for a smooth transition back to normal operations?

As a next step, consider the composition of the contingency planning and response teams. The planning team's primary role is to build and validate the plan. The response team's primary role is to execute the plan, and the response effort will probably require both a local "home" team and also an "away" team made up of individuals who travel to the off-site recovery location. The team members must know their roles, the team command structure, how they are to report in after a disaster. Provision should be made for both primary and alternate team members and for contingent chain of command in case key decision makers can not be located.

The contingency plan should include preparations for both containment and evacuation responses, and consider the differing needs of local v. regional disasters, and local v. remote recovery efforts.

It may be useful to provide a decision matrix for quick reference. This matrix can be used to direct responders to the appropriate section of the plan with respect to

1. First-response procedures for localized emergencies such as medical/fire/flood/vandalism/power failure/bomb threat
2. First response for immanent or actual large scale evacuation and containment emergencies
3. First response for information threats such as sabotage, unauthorized intrusion, DDoS attacks, and data theft emergencies.

The plan should incorporate answers to the following questions:

1. What events or actions will precipitate declaration of a disaster or activation of the plan?
2. What human needs must be considered during initial disaster response and subsequent recovery efforts?
 - a. How will employees communicate?
 - b. Where will they work?
 - c. How will they travel?

- d. Who will be with them?
- e. What will they need?
- f. Where is their relief team?
3. What risks does the plan itself introduce?
 - a. What were the underlying assumptions as the plan was formed?
 - b. How well do these assumptions reflect the actual business needs?
 - c. How will responders handle missing links in the chain of command?
 - d. What provisions are needed for protection, security, and authentication (both physical and electronic)?
 - e. How should the plan itself be tested or validated?
 - f. How will the plan be kept up to date?
4. How will the transition back to normal operations occur?

During planning, it is important to first identify the key resources that would be required to permit business resumption or sustain ongoing operations. Consider the following questions as they relate to each of your three primary resources:

B. PHYSICAL RESOURCES

1. What are the primary physical risks your business faces?
2. What physical assets does your business require?
 - a. Do you require all operations to be housed in a single office or building?
 - b. How much space would you require?
 - c. How many phone lines?
 - d. How many computers?
 - e. Are there special power or environmental requirements?
 - f. What level of physical security is needed?
3. How will these resources be provided?
4. Where will they be located?
5. How do the answers differ if the disaster is localized vs. regional?
6. Are your employees able to perform some or all of their work from alternate locations?
7. What facilities would be required to enable them to do so?

C. PERSONNEL RESOURCES

1. How many personnel are required to operate the business?
2. What skills are required?
3. How many shifts?
4. During emergency operations, how many would need to be involved in recovery efforts?
 - a. Away teams
 - b. Home teams

- c. Scribes
5. What do they need?
6. Where will they work?
7. Where will they sleep?
8. Are provisions needed for family/babies/pets?
9. Must the recovery team commute or relocate, or could they telecommute?
10. If telecommuting is a possibility, what resources will workers need to allow them to telecommute?
11. Support for communication/alternatives
12. Remote check-in/alternate contact
13. Alternate e-mail ids

D. INFORMATION RESOURCES

1. Where is your data?
2. How is it organized?
3. When is it backed up?
4. Where are the backup copies stored?
5. How can the current set of backups be identified?
6. Can either the data or the backups be readily transported or replicated?
7. Can you identify and prioritize the backup copies by business need?
8. Which business systems are critical?
9. In what order should they be restored?
10. How much space would be required for the restore?
11. What outside information do you rely on?
12. Did you identify all software used by your critical systems?
 - a. What about communication and contact management:
 - i. E-mail
 - ii. Contacts
 - iii. Calendars
 - iv. Collaboration tools
 - b. Document creation and management
 - c. Business applications & databases
13. Do you know where critical software backups are stored?
14. Do you know whether authorization keys are required to activate the software when it is installed on a recovery platform?
15. Are authorization keys, user documentation, and configuration information stored with your software backups or readily accessible for recovery purposes?
16. Is the plan prioritized as to both technical requirements and business requirement?
17. Where are copies of the recovery plan located?
 - a. Consider a “red box” that contains a printed copy of the plan and tape inventory, record keeping supplies, directions to the recovery site, copies of vital papers such as insurance and maintenance contracts, software license documentation, and primary and

secondary contact information for employees, clients, and suppliers.

18. Are precise restoration procedures documented?
 - a. Where to start?
 - b. Where is the plan and the “red box” ?
 - a. What to do – a detailed plan!
 - b. Who will do it?
 - c. Who will do it if the “A” team isn’t available?

E. COMMUNICATION RESOURCES

1. What communication is required to run your business?
2. To whom must you communicate outside your business?
3. What special communication will you need if disaster strikes?
 - a. To assess the damage
 - b. To assemble the team
 - c. To preserve vital information during the transition phase (a scribe).

ⁱ 19,924 Nautical Miles, according to the United States Central Intelligence Agency (“CIA”) World Factbook, <http://www.cia.gov/cia/publications/factbook/fields/2060.html>

ⁱⁱ The Global Volcanism Program, visited May 2006, http://www.volcano.si.edu/world/find_regions.cfm lists 90 active volcanoes in Alaska, 8 in Hawaii and 62 in the Western United States.

ⁱⁱⁱ Federal Bureau of Investigation “2005 FBI Computer Crime Survey”, July 2005, www.fbi.gov/publications/ccs2005.pdf

^{iv} <http://www.networkworld.com/news/2000/0515convict.html>

^v <http://www.usdoj.gov/criminal/cybercrime/kwongConvict.htm>

^{vi} Adam Savino “Cyber-Terrorism” available at <http://cybercrimes.net/Terrorism/ct.html>

^{vii} The triggering event and subsequent software failures were not the only cause of the blackout. Inadequate System Understanding, Inadequate Situational Awareness, Inadequate tree trimming, and Inadequate Diagnostic support were all cited as causal elements in the final study conducted by the U.S.-Canada Power System Outage Task Force.

^{viii} Computerworld (Security), November 20, 2003

<http://www.computerworld.com/securitytopics/security/recovery/story/0,10801,87400,00.html>

^{ix} U.S.-Canada Power System Outage Task Force “Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations”, April 2004, <https://reports.energy.gov/BlackoutFinal-Web.pdf>

^{x x} Federal Bureau of Investigation “2005 FBI Computer Crime Survey”, July 2005, www.fbi.gov/publications/ccs2005.pdf

^{xi} The use of automated tools to bombard a target site by sending thousands of e-mail messages at once, thereby jamming the recipient’s incoming e-mail box and effectively blockading normal e-mail.

^{xii} Federal Bureau of Investigation “2005 FBI Computer Crime Survey, July 2005, www.fbi.gov/publications/ccs2005.pdf

^{xiii} Dick, Ronald L. “Cyber Terrorism and Critical Infrastructure Protection, 24 July 2002 www.fbi.gov/congress/congress02/nipc072402.htm

^{xiv} <http://www.usdoj.gov/criminal/cybercrime/konopkaIndict.htm>

^{xv} <http://www.usdoj.gov/criminal/cybercrime/okeefeArrest.htm>

^{xvi} <http://www.usdoj.gov/criminal/cybercrime/maxwellPlea.htm>

^{xvii} http://news.com.com/Bank+of+America+loses+a+million+customer+records/2100-1029_3-5590989.html

^{xviii} <http://www.enterprisestorageforum.com/continuity/news/article.php/3499531>

^{xix} http://news.zdnet.com/2100-1009_22-6077062.html