

Katrina – The Harsh Teacher

June 2007

The year 2005 brought with it the largest and most destructive hurricane season on record in the United States. The queen of the season was hurricane Katrina, which was the most devastating storm to hit the Gulf Coast Region in over 200 years. Its cost to the national economic infrastructure, estimated to exceed \$200 billion dollars, was greater than any other storm in the history of the United States.

Katrina taught us many painful lessons, ranging from evacuation to communications, emergency management, tracking missing people, family reunion, property security, protection of individuals, municipal infrastructure, and a whole lot more. Buried in these massive problems were the corporate problems of business continuity.

2005: A Season of Firsts

- First with 26 named storms
- First with 13 hurricanes
- First with three Category 5 hurricanes
- First with four major hurricanes hitting the US

Source: NOAA 2005

When we look at the problems that companies in the area faced as a result of Katrina, the IT infrastructure, though terribly important, was just one part of the multifaceted business continuity problem. Shortly after the business effects of the storm began to dissipate, IBM shared their learning experiences in an in-depth Web seminar.¹ Patrick Corcoran, Director of Marketing and Strategy, IBM Business Continuity and Recovery Services, focused on the broad range of problems which companies faced while trying to survive. These problems included:

- People
- Communications
- Transportation
- Data availability
- Business Continuity Plan currency
- Insurance
- Infrastructure
- Power
- Hardware replacement

We summarize his advice here, knowing that "those who cannot remember the past are condemned to repeat it."²

¹ D. Walch (IBM), P. Corcoran (IBM), B. Woodworth (IBM), M. Evanson (Oreck), *Lessons Learned from the 2005 Hurricane Season*, IBM Web Seminar; January 19, 2006.

² George Santayana, philosopher and poet.

People

Problems

The last thing on employees' minds when Katrina hit was the corporate business. They were protecting their families and property, or they were disabled by trauma.

They didn't know what to do in a disaster of this magnitude. They didn't know where to go or who was in charge.

Employee safety had often not been considered in the business continuity plan. Employees were sometimes expected to perform functions that were simply not possible or that entailed high risk.

Little thought had been given to the personal needs of the company's employees. There were no plans to accommodate families, spouses, and children. There were no provisions for emergency loans or other funds for employees.

Actions

Companies must ensure that their employee needs are addressed in the business continuity planning process and that roles are clearly defined. Alternate teams should be established to assume the roles of employees who are unable to function.

Communications

Problems

There was virtually no way for people to communicate with each other. Landline telephones were out of service. Cell phones could not be recharged. There was no way to get onto the Internet for email. There was no way to communicate with the public sector agencies.

Even if there had been a modicum of telephone service, there was no centralized number for employees, customers, or partners to call for information, status or directions. Nor were there plans to address the media.

Actions

Employees must be provided with a centralized number, email address, or Web site for reporting in and sharing status information as soon as they can communicate.

Satellite phones should be considered along with wireless cards for laptops and text messaging services.

Transportation

Problems

People did not follow the directions of local agencies for evacuation in a timely and orderly manner. Even if they did, there was little if any gasoline for their cars and limited air transportation. Furthermore, the supply of rental vehicles was rapidly exhausted.

Even for those "fortunate" few who had automotive transportation, roads had become parking lots; and many cars broke down due to high temperatures.

Actions

Encourage employees to follow evacuation guidelines regardless of the business continuity plan. Try to anticipate a problem, and move key employees and their families as well as critical corporate data out of the affected area prior to the problem.

Plan for the availability of hotels and car rentals and be prepared to have a source of gasoline for employee travel.

Data Availability

Problems

Magnetic tape backups proved to be a major problem. Tapes were often stored in affected areas, including offices that were no longer accessible. As a result, tapes, disks, and critical documents were seriously damaged or destroyed.

In many cases, tapes could not be shipped because of travel restrictions; or they got lost in transit.

If backup tapes were available at a remote site, backup procedures were unknown or out-of-date.

Actions

Utilize electronic media such as virtual tape to send backup data and critical documents to multiple remote locations. One or more of these locations should be the corporate backup site(s).

Ensure that system recovery procedures from the backup data are well documented and frequently tested.

Business Continuity Plan Currency

Problems

Business Continuity Plans (BCPs) were either nonexistent or outdated. Often, BCPs were not linked to a change management system so that they did not account for changes since the plan was last reviewed or tested.

Such plans that did exist were sometimes not available, having been stored in the facility that was destroyed or severely damaged.

BCPs were not typically linked to an Incident Command System so that they could be executed as part of a larger response to the disaster.

Actions

Keep the Business Continuity Plan current and tested. It should be linked with the corporate IT and business change management systems so that it can change as the business changes. It should be tested frequently – at least once per year or more often.

Keep the disaster recovery vendor, if any, current with respect to the changing BCP. Periodically review the contract with the vendor to ensure that it adequately supports the BCP in its current form.

Create an Incident Command System and a crisis team to manage the crisis. Plan on the unavailability of some or all of the members of the crisis team.

Insurance

Problems

When it was too late, it was often discovered that insurance coverage was inadequate. Management did not even know what disaster activities were covered. Fire is typically covered, but did the insurance cover floods? Wind damage? Social unrest?

To compound the problem, there often was no recorded inventory of assets that could identify lost or damaged property for the claims adjuster, nor was there documentation of activities relating to the preservation of those assets.

Actions

Understand all risks associated with disasters, and ensure that they are adequately covered by insurance.

Keep a current inventory of all assets, and document all employee and other activities (police, fire, etc.) throughout the disaster.

Periodically obtain an independent review of the company's insurance coverage.

Infrastructure

Problems

Company facilities were located in high risk areas. The result of the disaster made these facilities unusable due to structural damage, contamination, or mold.

Critical assets were often stored in susceptible areas such as basements.

Mobile solutions sometimes didn't work in affected areas.

Actions

Evaluate the risks and vulnerabilities of the corporate facility locations. Ensure the security of the facilities and their accessibility during and following a disaster. With these in mind, conduct a vulnerability assessment of corporate facilities.

Arrange contracts with vendors ahead of time for the repair and cleaning of each facility, if so required.

Power

Problems

Power outages were almost complete in the area. There were no estimates for the duration of power outages (in fact, this could be weeks in some areas following hurricane Katrina).

Many companies had inadequate or no backup power supplies such as UPS or diesel or gasoline generators. Some generators wouldn't start. When diesel or gasoline generators were available, it often was impossible to keep them refueled.

Generators were often poorly located, such as in basements where they were flooded or on rooftops where they were blown off.

Actions

Ensure that backup power sources are regularly tested and that fuel is fresh. Reevaluate the location of backup power supplies.

Have contacts in place to acquire additional backup generation capacity if needed. Above all, ensure an adequate fuel supply for the generators for the maximum anticipated duration of a power outage.

Hardware Replacement

Problems

The hurricane damaged a significant amount of equipment and left remaining equipment without power. There were no plans to relocate equipment to an alternate location, even if this had been possible.

There were no plans to dispose of damaged equipment or to replace such equipment. Service contracts were incomplete and did not anticipate a disaster of this magnitude.

Actions

Consider a contract for immediate acquisition of new or used hardware. Have vendors lined up to relocate equipment if required.

Understand and document the procedures for removing and relocating equipment and for the disposal of damaged equipment.

Summary

Each of the above categories represents key areas that should be addressed when creating or updating a Business Continuity Plan. Even if the company has a remote backup site that is standing by with current backup data just in case of a disaster, the problems of communication with employees and getting them to the backup site still exist as do the follow-on problems of insurance and facility repair or replacement. All of these must be addressed in the BCP.

A severe hurricane such as Katrina is only one of many possible disasters. There are the obvious ones, such as fires, floods, and earthquakes. But what about those that are not so obvious, such as facility quarantining due to disease or contamination (remember the anthrax scare); unthinkable terrorist actions, such as 9/11; wide area power blackouts, such as the 2003 Northeast Blackout that extended for hundreds of miles throughout the United States and Canada; and social unrest.

As we have discussed in much of our content in the Availability Digest, a powerful approach to disaster tolerance is an active/active system. With such a system, two or more sites are actively providing processing services with a common application accessing a common replicated database with copies at, or accessible to, each processing node. Should one site be taken out by a disaster, all that needs to be done is to switch users from that node to an alternate surviving

node. Providing that a user still has access to communication facilities, that user is up and running in seconds. There is no problem with communicating with employees or with getting them to a backup site since the surviving nodes in the active/active application network are already in full production with a full complement of staff. Of course, the damaged or destroyed site needs to be repaired or replaced. But that can wait for another day.