

Business Continuity During A Disaster

Introduction

Disasters can come like a lightning bolt, suddenly, unexpectedly and with mind-numbing consequences. Businesses, both small and large, are faced with natural disasters such as fires, tornadoes, floods, earthquakes and hurricanes every year. Those that are prepared survive and recover. The rest become casualty statistics.

Friday evening, August 26, 2005, businesses along the Gulf Coast closed for the weekend as people went to dinner, shopped or pursued other weekend activities. For most, a wary eye was cast toward the Gulf, where Hurricane Katrina had just crossed the southern tip of Florida as a weak category one hurricane. The storm had gained strength over the warm Gulf waters and was a category three storm with landfall along the Gulf Coast expected some time over the weekend.

Most along the Coast were wary but not alarmed. Hurricanes are a part of life along the Coast. Most blow through causing more inconvenience than damage. People living in this part of the U.S. have learned to board up windows and close hurricane shutters.

Businesses have procedures that include covering computers, equipment and inventory with plastic or tarps to prevent water damage just in case windows are blown out or roofs are damaged and leak.

The Gulf Coast had already buttoned up for several storms during the 2005 season. The most recent was Hurricane Dennis, the storm that wasn't. After a big media build-up, Hurricane Dennis rolled through Alabama with wind and rain but causing little damage. It was another false cry of "wolf".

Virtually no one prepared for what would happen within the next 72 hours.

By Monday morning Hurricane Katrina, which had blown up into a huge category five monster with 175 mph winds, plowed into the Coast. The eye of the storm struck very near the Louisiana and Mississippi border but the massive storm extended from near

eastern Texas to the Florida Panhandle, in many areas washing the Coast with a huge 20 to 30 foot wall of water.

It was a disaster of massive proportions.

The destruction extended all along the coasts of Mississippi and Louisiana and for nearly 100 miles inland. Along the coast homes and businesses were simply washed away, leaving only concrete slabs where buildings once stood.

Practically all business came to an immediate halt. Electronic financial and businesses records were inaccessible without electric power. Paper records for many businesses were damaged or destroyed by wind and water.

Communications were completely cut off for most people. Without electricity there was no TV or radio. Telephone service was wiped out and cell phone towers were smashed down. Access to the Internet and e-mail was gone. In most areas it would take days, even weeks, before communications systems could start being restored.

For many businesses it is not the physical damage that is the most destructive. It is the loss of revenue and the opportunity costs that occur during the recovery and rebuilding period.

This is where business continuity planning is essential.

Historical overview

Business continuity development has been driven by stockholders, government regulation and market forces. It has gained steam during the past 35 or 40 years, evolving from disaster recovery into a more comprehensive plan that includes not only recovery but operational continuity during and following a disaster.

The fuel for the fire has been data processing technology. Changing technologies have given companies the opportunity to address critical recovery issues and focus on continuance. Each advance has taken continuity to a new level.

Because of their special vulnerability, crucial importance to their customers and at the prompting of government regulation, banks have been leaders in business continuity

planning for years. An overview of how business continuity planning has developed in the financial services industry provides a picture of just how this important facet of business planning has developed. The lessons learned by this industry can go a long way in helping other companies, both large and small, shortcut the learning curve.

Facilities protection

Facilities protection might be called the first level of disaster recovery and business continuance.

A century ago disaster planning for banks meant building facilities to prevent disasters such as robbery, fires, earthquakes, floods or tornadoes. Banks became brick and mortar fortresses. Everything was built around protecting the cash. Nearly indestructible vaults of thick concrete were designed into buildings that were themselves designed to be as secure as possible.

Insurance

Another level of disaster recovery and business continuance has been the development of insurance to deal with these issues. In addition to property liability insurance, key man life insurance, director and officer liability insurance and business interruption insurance policies have been developed and marketed.

Data protection

By the 1950s, banks and larger companies were beginning to make backup copies of critical records. These records were kept in bank vaults along with the cash.

High speed data processing became possible as main frame computers came into widespread use in the 1960s. The Federal Reserve Banks began using them to process transactions. Large banks established their own data processing centers, selling the service to smaller institutions.

This helped to change the industry in a remarkable way. Customer transaction information and transactions between banks and with the Federal Reserve Bank could be

processed much more quickly. Now, it was no longer necessary for the bank to keep large amounts of cash on hand. Cash not otherwise invested was kept on deposit at the Federal Reserve. Data became the primary commodity.

Data protection included increasingly frequent backups and off premise storage. Data processing centers began using data storage vendors.

In 1983, the Office of the Comptroller of the Currency (OCC) a regulatory body governing banks, issued banking circular BC177, requiring banks to develop, document and maintain recovery plans.

Data management has become crucial not only for banks but for all businesses. Over the past 20 years government regulatory bodies, including the Federal Financial Institutions Examination Council (FFIEC) and the Securities and Exchange Commission (SEC), have adopted a number of rules requiring companies protect critical data.

Communications

Another critical area, being driven to new levels by changing technologies, is communications.

During times of crisis, a company has several groups of people with whom it must communicate. These include 1) investors and directors, 2) employees, 3) suppliers and vendors, 4) customers and potential customers and 5) the general public. It is critical to the ongoing success of the business that communications with each of these groups not be disrupted and be restored quickly. Investors and directors must know that management is dealing with the crisis in the most effective manner possible. Employees need to know what is expected of them, whether or not they still have jobs and when they will be able to return to work. Customers and potential customers need to know if the business is still functioning and if it will be able to provide the needed products or services.

The number of ways and the speed with which these different groups may be reached has exploded over the past two decades. Electronic technology has expanded written and print communications to include telephones, fax machines, cell phones, e-mail, the Internet and mass communications that include radio and TV.

Most of these systems share a common problem during disasters and crisis periods. They are ground based. Natural and man-made disasters can disrupt ground based communications.

Highlights in the development of business continuance

Other highlights in business continuity planning during the past few years include the following.

1989 – FFIEC requires documentation, maintenance and testing of recovery plans

1990s – Business continuance strategies begin taking the place of disaster recovery plans

1997 – FFIEC declares that boards of directors are to be held responsible if disaster recovery plans are not in place

2000 – The National Fire Protection Association (NFPA) publishes NFPA 1600: “The Standard on Disaster/Emergency Management and Business Continuity Programs”

2001 – The Gramm-Leach-Bliley Act, dealing with the protection of non-public personal information goes into effect

2002 – The Sarbanes-Oxley Act goes into effect. This act deals with the accuracy of corporate disclosures of financial information.

2004 – The SEC approves NASD Rule 3510 and NYSE Rule 446. Rule 3510 deals with business continuity plans and emergency contact information. NYSE Rule 446 deals with establishing and maintaining business continuity and contingency plans.

Building a business continuity plan

In 1992, the Gartner Group, a large technology consulting firm, released a study showing that 40 percent of all businesses experiencing a major disaster will never reopen their doors. Another 20 percent will go out of business within two years.

The difference between business survival or demise during and after a disaster is the ability to continue operating with the least possible disruption. There are tremendous losses that occur when a business is shut down for extended periods. During a shut down

the revenue stream may be cut, but the stream of expenses does not stop. Employees need to be paid and if the flow of regular paychecks is disrupted they have to seek other employment. Suppliers need to be paid, even if inventory is lost, destroyed or damaged. There is also the cost of lost sales and the costs of opportunities missed.

Severe thunderstorms and heavy rainfall swept through Alabama in late April and early May, 2003, with some of the heaviest rainfalls on May 7. Torrents of water swept down the Black Warrior River causing unprecedented flooding.

One of the Birmingham businesses in a warehouse along that river was an established specialty apparel manufacturer. The company designed and manufactured camouflage hunting clothing, backpacks for hunting and hiking and ATV accessories including seat cushions and fabric pouches.

The privately held company had recently upgraded with new computer equipment, including computerized sewing machines.

Record level flood waters poured into the building that housed company offices, manufacturing and warehousing. Equipment that was not washed away was covered in silt and reduced to trash. Company records were lost, either washed away or soaked and illegible.

Insurance coverage was inadequate.

Some inventory and equipment was salvaged. For months the company owners tried to reconstruct sales and accounts receivable records. Revenues ground to a fraction of pre-flood levels. Employees were let go as the company tried to staunch the flow of expenses as worried suppliers and bankers cut off credit and demanded payment.

Valiant efforts were made to keep the once very profitable business alive for more than a year. It was all in vain with the company eventually forced to close its doors.

A well conceived business continuity plan with a realistic assessment of risks and data protection measures could have made all the difference for this company.

Analysis

A first step in business continuity planning is a realistic analysis of the threats. These can include such things as weather threats, disease outbreaks, fire, cyber attacks, extended loss of electrical power or terrorism.

Weather threats include floods, earthquakes, hurricanes, tornadoes and blizzards.

Planning for weather events should be realistic. Major weather events occur in 25, 50 and 100 year cycles.

Disease outbreaks are also threat possibilities. A potential flu pandemic, perhaps stemming from a mutated form of the Asian avian flu or bird flu could be a disaster of huge proportions. The bird flu pandemic scenarios are being modeled on the Spanish flu pandemic of 1918. That global outbreak killed 500,000 people in the United States and more than 20 million worldwide. It killed more people than died during all of WWI. Since that time there have been two other smaller scale flu pandemics, each killing hundreds of thousands of people.

The flu is just one disease that can cause a business disaster situation.

Recent years have also shown that terrorism threats are a real possibility. Terrorism is such a threat because there is so much uncertainty about when, where or what kind of attack may next occur. For example, the attack may be nuclear or biological with the possibility of being very widespread.

This analysis of potential threats should include probabilities of each threat occurrence with time frames in which critical functions must be resumed after the disaster.

Organizational responsibilities

Someone must be responsible for making the continuity plan work. People must be identified within the organization that will assume key roles should a disaster occur. This phase of the plan needs depth with more than one person or group assigned to each role, in case the first person or group is incapacitated by the disaster.

This section of the plan should identify who is responsible for what activity or strategy both during the disaster and during the recovery phase following the event.

Continuity strategies

The next step is to develop strategies for pre-event, event and the recovery phases of the disaster. These should include developing training programs; procedures for notifying and mobilizing key employees; establishing contact with key public officials, police, informational media, emergency response personnel and hospitals and data backup and protection procedures. These strategies should also identify goals for minimally acceptable time frames for restoration of critical functions and systems.

In addition to time frames, the strategies should establish the amount of critical data or function loss that is acceptable. For example, suppose a subscription fulfillment house uses a tape back up system. It backs up magazine subscription information at the end of each day at 7 p.m. The tapes are shipped to an off site storage facility the following day at 10 a.m.

If subscription processing takes place over two eight hour shifts, beginning at 8 a.m. and the disaster struck at 9 a.m., the amount of data lost would be 17 hours. This includes both eight hour shifts from the previous day and the one hour of the current day. The average dollar value represented by each shift may be calculated, giving management a reasonable estimate of revenue loss. Management must decide if this amount of loss is acceptable, or if alternative strategies should be implemented to reduce potential loss.

Implementation

The next step is identifying the trigger points when a continuity plan is activated. This might be, for example, when the local emergency management office declares a state of emergency would be a trigger point.

At this point the firm is in crisis and management is concerned with stabilizing and preventing further damage.

Implementation may also involve emergency response or evacuation procedures, delegation of authority or responsibility and following checklists for recovery and restoration.

One essential component of crisis management is communications and includes communications taking place before, during and after the event. This will include communications with employees, customers, the community, regulatory agencies, shareholders, directors and others affected by the situation.

For example, the emergency declaration activates a sequential call tree. In this situation each member of a small group is each responsible for making a few phone calls to an assigned list of people. The members of this second group in turn each call a few more people and so on creating a communications network.

Recovery

Once the disaster event has occurred, recovery must begin as quickly as possible. This includes caring for the sick and injured, stop loss or damage, begin making repairs to facilities and reestablishing service or product delivery.

Among the many heroes during Hurricane Katrina were the electrical power companies and their employees. Any sense of recovery progress depended upon restoration of electrical power. Power was needed for basic essentials such as pumping water, making ice, preserving and cooking food.

Immediately after the hurricane winds subsided, predictions were that it would take months before power could be restored to some areas. These predictions were based on prior hurricanes, including Camille in 1969 and Frederick in 1979.

But times had changed since those storms. Mississippi Power, like the other electricity distribution companies serving the Gulf Coast, had contingency plans in place with aggressive service restoration goals. Men and equipment from power companies from all over the United States were on standby to move into the Gulf Coast even before the hurricane made landfall. Once in place, these men and women worked around the clock, doing whatever it took to restore power street by street and country road by country road. In many cases the fixes were temporary. It was a mammoth task but power was restored to most areas within days or weeks, rather than months.

It was an excellent example of good disaster recovery, business continuity planning and execution by the power companies.

Testing

Once the plan has been devised and recovery procedures developed, it should be tested to work out problem areas. Testing also provides additional training to staff.

One method of training is to create roundtable discussions. In these discussions a disaster scenario is presented. Each person is responsible for describing how his or her department or responsibility would respond to the event. As each department response is given, a picture of the plan's effectiveness begins to emerge.

Another testing method is to create exercises simulating disaster events. Rather than simply talk about the response, each person must physically act out the response.

These testing methods give the staff an opportunity to evaluate the plan. It also has the added benefit of creating greater staff buy-in or acceptance of the plan.

Maintenance

Periodic review and maintenance of the plan will be required. This may involve training new staff members, reviewing procedures for relevance, evaluating software and hardware requirements and preparing management reports and audits of the plan.

Data security

One of the primary assets for most businesses is data, even small businesses. Preserving critical data is a primary component of any continuity plan. Loss of data can mean lost revenues, loss of competitive position and also create liability exposure in tax or regulatory agency audits.

The continuity plan must provide analysis of appropriate back up systems. This may include using a vendor to provide off site storage. Any back up system and off site storage vendor or facility must also provide protected access to the information.

The importance of satellite communications

The Army National Guard was called out in force during hurricanes Katrina and Rita. One National Guard commander made an interesting observation about Hurricane Katrina. He said it was an excellent exercise for the Guard because dealing with it was much like dealing with a classic military attack. One of the first things the hurricane did was knock out communications systems as it swept inland through Louisiana and Mississippi.

The hurricane cut a 100 mile wide swath through homes, trees, electrical transmission lines and telephone substations, knocking out cellular towers as it moved north out of the Gulf.

People were without communications for days. There was no land line telephone service or cell phone service in much of the southern regions of Louisiana, Mississippi and Alabama. Businesses could not communicate with employees, vendors or customers. Family members could not communicate with one another.

"If we learned anything from Hurricane Katrina, it is that we cannot rely solely on terrestrial communications," Kevin Martin, chairman of the Federal Communications Commission (FCC), told members of the Senate Commerce, Science and Transportation Committee. "When radio towers are knocked down, satellite communications are, in some instances, the most effective means of communicating."

Martin made this statement while testifying about communications failures and effectiveness following Hurricane Katrina. The storm did tremendous damage to earth-based communications infrastructure along the Gulf Coast. Nearly three million telephone customers were left without land line service. Thirty eight emergency 9-1-1 call centers were disabled and millions of calls failed in the days immediately following the storm and hundreds of thousands of customers were without cable television, Martin testified. Through all of this, he said, satellite telephones continued to provide effective service. "So we should consider satellite communications as a part of our overall solution in response to disasters?" Senator John McCain (R-Ariz.) asked.

"That's correct," Martin said.

Advantages of satellite phones

Hurricanes Katrina, Rita, the Indonesian tsunami and other disasters in recent months have allowed people to compare satellite phones and their advantages to terrestrial communications.

A satellite phone is simply a mobile phone that uses commercial space satellites instead of land-based radio towers to connect to phone lines. The phone signal is transmitted to an orbiting satellite and then beamed transmitted back to earth. This creates a number of advantages.

1. Satellite phones will work almost anywhere in the world. All that is needed is signal access to the satellite. The phones are not dependent upon cell towers.
2. Satellite phones will work during power outages. All that is required is a charged battery in the phone. There are also a number of accessory power supplies available to extend the life of the phone during the crisis period. These include chargers that plug into the cigarette lighter of a car or truck, additional batteries, data kits and solar chargers.
3. Satellite phones are compact and convenient to carry and use. Just as with other phone technologies, these phones are now much smaller than predecessor models.
4. Satellite phones are affordable. At one time this technology delivery was expensive for customers. As acceptance of these phones has increased over the past decade, the cost of using satellite phones has decreased. There are also a number of plans available to provide the service you need at the lowest possible cost. For less than \$1,000, you can purchase both a handset and a one year airtime plan.
5. Satellite phone equipment and plans provide voice communication, Internet access, voice mail and access to e-mail. Secure link communications are also available and you can have T1 speed available in a portable, hand-held device.



The Globafone solution

Globafone has had just one vision since it was formed in 1998: to provide a wide array of wireless solutions to its clients, especially in times of emergency. To this end Globafone has developed a wide array of products and an international network of service providers, giving clients a number of advantages.

One of the first advantages is no boundaries on your ability to communicate with your clients or branch offices. Regardless if it is a natural disaster or putting the finishing touches on a big sale or a company merger, you will be connected directly to the people you need to reach from anywhere in the world. This includes voice, e-mail, fax or having access to a portable high speed Internet connection.

Another Globafone advantage is its partnerships with service providers in places like Dublin, London, Seoul, Singapore and Tokyo. These partnerships use local experts, the people who know how business is done in their homeland or region, to help you succeed globally.

GlobaFone is an eight year old company that is based in Portsmouth, NH. They are a two-time winner of the GSA's Industry/Partner Service Excellence Award and provides FEMA with more of their satellite phones than any other supplier.

GlobaFone has been in the handheld satellite business since its inception and they offer five brands of satellite phones from Globalstar, Iridium MSV, Thuraya and INMARSAT. Clients other than FEMA include DoD Inspector General's Office, the EPA, NASA, BAE Systems, Chevron, Hoffman LaRoche, General Dynamics, and the Massachusetts Department of Public Health.

GlobaFone continues to lead the industry with innovative thinking by offering such packages as; hurricane and disaster response kits, their Quick Start system and other unique approaches to providing the essential equipment to the people who need it most. Let GlobaFone help you find solutions you will need as you develop your business continuance plan. Call them at 603-433-7232 or e-mail

l.altman@globafine.com