So You Think You Have a Good Business Recovery Plan? – Steps an Asset Management Company can take to Recover from a Major Disaster

By: Roger Elrod, MBA, MCSE
Asset Management Support Services Engineer
rjelrod@bbandt.com

Abstract

The terrorist activities in September of 2001 caused business everywhere to take a long look at disaster recovery plans (DR) and business continuity plans (BCP). The collapse of the trade towers showed the importance of not only having critical data backed up, but having the data moved offsite to a secure location. Offsite storage vendors experienced an increased demand for data storage capabilities.

Business thought they had bought piece of mind now with their critical data being stored offsite. However, the aftermath of Hurricane Katrina will force all companies to re-think about what it really means to successfully resume business after a disaster.

Disaster has a new definition. Is your business ready? This paper will summarize the different kinds of disasters and then discuss some of the different aspects of a disaster-recovery/business continuity plan. These principles will be then be applied to a company dealing with asset management.

1.Introduction

On August 29, 2005, Hurricane Katrina battered the gulf coast of the United States. The category four hurricane brought winds as high as 160 miles per hour and a storm surge of up to 30 feet which devastated an entire region. The largest U.S. hurricane since Andrew in 1992 will result in the largest insured loss from a single event since September 11, 2001.

Hurricane Katrina flooded New Orleans. Power outages, lack of water and difficulty in bringing in necessary supplies are just a few of the problems facing this world famous melting pot. Businesses in the New Orleans area will face an up hill climb in restoring even the most basic functions of their enterprise.

This is now the new definition of a disaster. In this case, a building did not burn down and a power grid did not fail. No, in this case and entire city has been destroyed. There are no passable roads, no viable government infrastructure, no basic utilities, and no real means for the city to rebuild the economy of the region for years to come.

According to FEMA, a total of 906 major disasters were declared in the United States between 1976 and 2001. This indicates that major disasters are not events that happen every once in a while. Major disasters can and will happen at any time (Cerulla 70).

Datapro Research Company found that 43 percent of companies hit by a severe crisis never re-opened, and 29 percent more failed within two years. This research coincides with a FEMA report concerning the 1992 Hurricane Andrew strike. The FEMA report found that 80 percent of all businesses that did not have a Business Continuity Plan failed within two years of the storm (Cerulla 70).

Is your business ready for a disaster like Hurricane Katrina created? This paper will summarize the different kinds of disasters and then discuss some of the different aspects of a business continuity plan. Then these principles will be applied to a generic asset management company.

2. Kinds of Disasters

There are generally three broad types of disasters business need to keep in mind; natural disasters, technical failures, and human threats (Jrad 110).

Examples of natural disaster are hurricanes, tornados, earthquakes, tsunamis, and floods. Some disasters like hurricanes have the ability to be forecasted, so there may be some time to get some last minute plans in order to prepare for the upcoming event. However most of these natural disasters happen without warning.

Technical failures may also create disasters. Power outages that bring down mission critical processes or failures equipment that prevent chemical leaks often cause a complete halt to day-to-day operations.

While natural disasters and technical failures can cause a great deal of business stress, human threats are the most sinister type of disaster. Human threats are characterized by the purposeful act to destroy or disrupt a business.

Human threats can come in many ways; bomb threats, arson, corporate espionage. But the Internet has enabled hackers to create viruses that can bring down a business or businesses just as fast as anything. According to a study by the Presidents Commission on Critical Infrastructure Protection, there are about 19 million people worldwide with the skills necessary to engage in malicious computer hacking (Pekala).

3. Business Continuity Plans

There are many terms to describe the process of a business recovering from a disaster; disaster recovery plans, business continuity plans, and disaster contingency recovery plans. Whatever term is used, the basic concept is still the same; a plan is required to be able to resume business operations no matter what disaster takes place.

While the basic premise is the same, there is a slight difference between business continuity plans and disaster recovery plans. Disaster recovery is really a component of business continuity. DR plans are concerned with the reconstruction and retrieving of information if a primary production facility has been damaged or has been destroyed. Whereas continuity plans encompass measures to actually switch over operations to a backup facility within 24 hours of the incident (Cocheo 28).

Business continuity plans are simple in concept, but are extremely detailed and intricate in make-up. BCP must contain the following contingencies to be effective.

With the events of 9-11 and Hurricane Katrina, business continuity plans must make plans for the possible loss of personnel. Key business decision makers could be harmed by the event and either unable to contribute to the restoration of the business, or unable to communicate with the DR team.

But having a contingency for the loss of personnel is not enough, there must be a plan to deal with and help with the emotional impact of the surviving employees. Believe it or not, when a disaster strikes, your surviving employee's first concern is not going to be the resumption of your business. Their thoughts will turn to basic family issues, especially if someone they know has been injured or killed (Castillo 9).

The second contingency will be for the total loss of an infrastructure. If the company's building, or even worse, region of the country has been hit by a disaster, one of the major facets of a BCP plan is the resumption of business in an alternate location.

Generally, there are four different alternatives for business resumption. The alternative that is chosen is usually made by the chief operating office or chief financial officer. The decision really comes down to how much "pain" – pain measure in time and money, he or she is willing to endure until the business finally resumes (Morganti 56). All four alternatives involve service level agreements (SLA's) between the business and the company providing the alternate site.

The four alternatives are cold sites, warm sites, hot sites, and mirrored hot sites. Cold sites are for businesses that have a high downtime tolerance. Restoration of business services usually comes between 2 to 3 days after the disaster. Cold sites do not have the infrastructure in place, ie servers, computers all of the time. Instead, all of the required equipment installed and ready after a disaster has been announced by the company. The negotiated SLA will determine how fast the business will be able to resume operations.

Warm sites are required for those businesses that have medium downtime tolerance and have the ability to resume business in 1 to 2 days. Usually, business hardware is already onsite, and when a disaster is called, the operations of recovering data and changing communication links commences.

Hot sites are required for those businesses that have a low tolerance for downtime. Businesses that require a hot site need business activities resumed between 4 and 24 hours after the disaster has been declared.

According to a Yankee Group survey, the average cost of an hour of downtime is $330,000. Businesses investing in a hot site are trying to insure themselves against losses, losses that can easily get into the millions of dollars after a few hours of downtime (Pakala 46).

The last classification of alternate sites is called mirrored hot sites. Mirrored hot sites are for those businesses that have no tolerance for downtime. When a disaster is called, these businesses want zero recovery time.

Mirrored hot sites are a fully redundant mirror of the regular production business systems. All the systems are installed in the redundant center and are continuously maintained to mirror the production environment. As you can expect, the cost of a mirrored hot site is extremely high. Only those businesses that will entail losses in the millions per hour would probably finance such a robust recovery system.

The third contingency would be prioritizing the business resumption activities. After a disaster, what business activities will be the first ones to get back online? Again, this is another question that a senior management executive will answer. Also, again, this answer will be determined by the activity that brings in the most revenue. Processes that are causing the most ill effect to the revenue stream will be brought back online before those functions that bring in no revenue, like administrative or support functions.

A fourth contingency is for the resumption of continuous communications with customers. In a disaster, one of the items that a customer will worry about is the state of their financial condition. Communication lines to call centers need to be re-established in order to reassure the customers about the state of their assets (Castillo 20).

One final contingency is for the continuous testing of all business continuity plans. In fact, the disaster recovery process is a never ending loop of planning, execution and feedback. Without all of these elements, the DR process will become ineffective and outdated (Tura 148).

4. Steps in a Business Continuity Plan

Starting a business continuity plan is like any other major project. A comprehensive approach to the initial planning phase of the project will go to insure a successful development of the plan.

The website www.yourwindow.to/business-continuity/index.htm offers an online guide to business continuity planning and disaster recovery planning and discusses the six major deliverables that any BCP/DRP project will have; ; Initiation of the BCP Project, Business Risk and Impact Analysis, Emergency Preparation, Disaster Recovery, Business Recovery, and Testing the BCP Process (Business

The Initiation deliverable will be just like any other project initiation. In this phase will allow time for the reviewing of current BCP plans, if they exist. Also, in this phase the project team will be created, objectives, and milestones will be defined and reporting procedures will be ironed out (Business).

The Business Risk and Impact Analysis deliverable is concerned with identifying four areas; Incident Assessment, Business Risk Assessment, IT and Communications, and Existing Emergency Procedures (Business).

The Incident Assessment area will define the types and levels of disasters that are possible. The terminology in this section of the project could be the same for any business building a BCP. Environmental disasters, organized-deliberate disruptions, utility and basic service losses, equipment failures, and security breeches are all areas of concern for every business entity (Business).

The Business Risk Assessment identifies the key business areas of concern. Processes like E-commerce processes, email, production processes, sales, R and D, IT services and accounting. This area is also concerned with the financial and operational impact for the potential loss of key business processes (Business).

The third major deliverable is when the process becomes very business specific. In the Preparing for a Possible Emergency phase, backup and recovery strategies are reviewed, a BCP-DR organizational chart is developed and key documents and procedures are defined (Business).

The backup and recovery area is where the determination of what type of alternate site will be established; cold, warm, hot, or mirrored hot. The backup and recovery of both data and customer services is also defined. In addition, all insurance coverage's are reviewed (Business).

The Key Documents area is concerned with pointing out all records that are vital to the overall business process (Business).

The fourth phase of the process is the Disaster Recovery Phase. This phase is tasked with identifying the current potential disaster possibilities and creating a notification process to mobilize the DR team (Business).

The fifth phase of the process is the Business Recovery Phase. This phase is tasked with organizing the business recovery after the disaster team has been mobilized. Then this phase concentrates on the specific business recovery activities such as: Restoring power, communications, production equipment, and support services (Business).

The sixth phase is very important to the entire process. This phase concentrates on the testing of the entire business recovery plan process (Business).

Now that the Business Continuity Plan/ Disaster Recovery Plan process is clear, we will now attempt to apply the principles to the recovery of business operations in a firm dealing with Asset Management.

5. Business Continuity for Asset Management Companies

Asset Management companies, especially those handling security and bond trades for multi-million dollar clientele, pose a unique challenge for the resumption of business in the aftermath of an emergency.

Most Asset Management companies have any number of portfolio managers that handle various types of funds. Outside of the trade order management systems in use, and the portfolio management and reporting systems used, there is very little hardware that is required in order to resume normal business operations. However, this does not mean DR should be taken lightly.

Going through the project plan explained earlier in this paper, the first phase that directly relates to individual business practices is identifying key processes.

Asset Management is all about executing trades at the correct time to get the greatest return for the individual clients. This beings said, key business processes would be communication, either by email, phone or fax, and the trade order management system being used.

In preparing for the possible emergency, the expense of a hot-mirrored site probably out paces the potential benefit. However, a hot non-mirrored site, one that can be up and functional in less than 24 hours is justifiable.

The location of the hot site will need to be one that is in a different region than that of the normal business. Prior to Hurricane Katrina, the term 'region', might have been defined as any area as close as 50 miles away. Given the size and enormous destructive power that Katrina brought to the New Orleans area, the term 'region' needs to be re-defined. Now, alternate sites needs to be at least 500 miles away. And, for travel sake, need to be located close to a major airport.

The hot site would have to contain the exact computer equipment used in normal business operations. The servers would have to be loaded with the trade order management software and workstations would have to be ready, loaded with all of the required software packages that the portfolio managers and traders require, in order to conduct trading.

While the utilization of a hot site, instead of a mirror hot site will be less costly, the hot site will require more steps to get the infrastructure ready for business.

The database on the trade order management servers will need to be migrated over and installed on the hot site server. In order for this to happen, and for the data to be up-to-date, the database will need to be backed up and stored offsite everyday. For fastest recovery results, the offsite storage of the database backups should be located close to the hot site. Using an offsite storage center in the same region of normal business operations can result in the problem of getting the backups to the new location.

Having a daily activity surrounding the backup of storage of the trade order management server database will enable a quick restoration of business operations.

In the normal business production, both the servers, and workstation often communicate with vendors and custodians to a specific port in the firewall. The new hot site would also have to allow for this communication, either by having the specific ports open, or by allowing all traffic. Allowing all traffic may not be the most secure fashion, but in a disaster recovery scenario, may be useful in resuming business operations quickly.

While some trading packages are available to the traders and portfolio managers on the Internet, some require workstation installation. Bloomberg, for example, not only requires a specific port for communication, but also a workstation installation piece.

In addition to software packages, and Internet communication, most trade order management servers require links to Sungard. Sungard is a leader in processing solutions for financial services. The trade order management servers often download information daily to get up-to-date transaction lists from different vendors at one time. This link is vital to the integrity of the trade order management system. Account values and positions change on a daily basis, and this connection is necessary for basic business functions.

Now that basic contingencies have been created for the re-creation of the hardware needed for resume normal trading, personnel contingencies have to be made. Following the BCP planning phase, key personnel have already been identified. The BCP plans call for someone from executive management to formally call for the enactment of the BCP process. At the time the disaster is called, the key personnel would be required to make travel plans to the hot site.

In the Asset Management business, the essential personnel would be a representative from senior management, the trade order management administrators, the traders, and any specialized technical support personnel.

These different personnel would have to have a copy of the disaster plan, and would be the first ones contacted and 'ordered' to proceed to the alternate hot site.

After arriving to the alternate hot site, the trade order management server database can be brought up-to-date with the daily backup, the different vendors can be notified of the company's new-temporary location and phone lines can be re-routed in order for remote customers to have a seamless communication to the new location.

6. Conclusion

Business Continuity Plans and Disaster Recovery Plans are important to the long-term health of any business. Just as having data stored offsite is not enough, restoring the infrastructure is also inadequate (Castillo 12). Both people and processes need to survive the event. People need to be able to reconstruct the data and the processes need to be documented in order to resume business operations (Cocheo 29).

Still, as important as a business recovery plan is, some executives feel apprehensive about spending the necessary amount of money to get the desired results. The BCP must have a senior management champion. One who will be able to sell the importance to other executives and support the year to year maintenance costs of the plan (Cerulla 71).

[1] “Business Continuity Planning / Disaster Recovery Planning: An Online Guide” < http://www.yourwindow.to/business-continuity/index.htm>.

[2] Castillo, Carolyn. “Disaster Preparedness and Business Continuity Planning at Boeing: An Integrated Model.” Journal of Facilities Management Vol 3 No. 1: 8-26.

[3] Cerulla, Virginia, Michael Cerulla. ”Business Continuity Planning: A Comprehensive Approach.” Information Systems Management Summer 2004: 70-78.

[4] Cocheo, Steve, Lauren Bielski. “Can Your Bank Bounce Back in Real-Time.” ABA Banking Journal September 2002: 28-32.

[5] Friedman, Gregory. “Compliance Issues and the Use of Technology.” Journal of FinancialPlanning January 2005: 30-32.

[6] Hlavacek, Donna, Karl Madsen, Robert Reimer. “A Vendor and Service Providers Partnershipfor Preparing to Manage Disaster Recovery.” Bell Labs Technical Journal March, 2004: 173-180.

[7] Jrad, Ahmad, Thomas Morawski, Louise Spergel. “A Model for Quantifying Business Continuity Prepardness Risks for Telecommunictions Networks.” Bell Labs Technical Journal February, 2004: 107-123.

[8] “Just 24 Hours Away from Shutdown.” Management Services May 2004: 3.

[9] Karakasidis, Kon. “A Project Planning Process for Business Continuity.” InformationManagement & Computer Security Vol. 5 1997:72-78.

[10] Leander, Ellen. “Fast Disasters, Fast Losses.” Treasury and Risk Management September 1997:47-49.

[11] Lister, Iain. “On the Look Out.” International Power Generation May 2005:35-26.

[12] Morganti, Michael. “A Business Continuity Plan Keeps You in Business.” Professional Safety January 2002: 19,56.

[13] Pekala, Nancy. “Back to Business: Business Continuity Planning is Key to Recovering from Disaster.” Journal of Property Management November/December 2002: 44-46.

[14] “Planning for the Worst.” The Information Management Journal May/June 2003: 3-4.

[15] Tura, Nick De, Susan Marie Reilly, Srilatha Narasimhan, Zhenhua Jack Yin. “Disaster Recovery Preparedness Through Continuous Process Optimization” Bell Labs Technical Journal March 2004: 147-162.