

Planning for Disaster

September 2005

by



Clareity Consulting
<http://www.callclareity.com>

Introduction

In the wake of Hurricane Katrina, there is a heightened awareness of the need for disaster recovery planning. Clareity Consulting has been working in this area for many years and is responding to the heightened demand for disaster planning information by publishing this free paper to the real estate community.

Many business risks can be avoided via a rigorous, expert assessment of the physical plant, personnel practices, flood/water controls, housekeeping, fire controls, electrical power, climate control, IT operations and security practices. Regardless, business continuity risks can never entirely be eliminated, whether it is due to employee failings or more difficult to control issues, such as natural disasters and criminal activity. What would your organization do if its main office was destroyed by an earthquake, flooded by a nearby river, consumed by fire, or affected by a criminal or terrorist attack?

Your organization will be better prepared to deal with these eventualities if it has prepared a formal written Business Resumption Plan (BRP) that accounts for each circumstance. Formalized written BRPs improve the ability of an organization to reliably and quickly perform a coordinated recovery in the event of specific business disruptions. BRPs allow the emergency response team to coordinate the recovery effort with both internal and external resources, improve communication to those affected by the disruption, and minimize overall downtime and loss of productivity.

Creating the Business Resumption Plan (BRP)

The following are the components Clareity looks for when reviewing BRPs for an organization:

Definitions of Disruptions and Disasters

The first planning step is to define the types of events that constitute a disruption that will prompt use of a BRP. For example, if yours is a member organization and the disruption (i.e. Chlorine gas spill from nearby railway) means that the office will not be inhabitable for a few hours on a weekday morning, is that a significant disruption that requires BRP use, either to notify members or employees of the event? What if you provide a software application over the Internet and your (only) Internet Service Provider goes down and expects downtime to be an hour – or several hours – or can't tell you when they will recover? Under what circumstances is the BRP enacted?

The easiest way to gauge these circumstances is to define disruptions in terms of their measurable consequences rather than solely in terms of the disaster itself. One might have plans for both single events and a combination of events, such as:

- Employees must evacuate or can not enter office. Office is unusable:
 - For expected period greater than two hours but less than two days)
 - For greater than two days but less than one week
 - For unknown greater period of time
 - Office and contents is a total loss (permanent)
- Loss of key personnel
- Loss of personal / financial information (security breach)
- Office IT system/network disruption (periods of time defined as above)
- Telephone system disruption (as above)
- Member-facing IT systems disruption (as above)
- Public-facing IT systems disruption (as above)

There may be several events that cause “total office loss” such as fire, flood, earthquake, or terrorist attack and it is not necessary to write completely separate plans for each type of disaster – rather, the focus should be on creating a plan that is oriented towards resolving the common disruption that could be caused by several types of disasters.

Formalized Roles and Responsibilities

One of the most important parts of the planning is formalizing who is involved in the business resumption effort - creating a business resumption team and assigning them responsibilities. Who within the organization determines whether an incident is classified as a business disruption and what BRP components to enact? Which staff members are subsequently involved in the business resumption effort and what are their roles and responsibilities? Who are the back-ups to each position in case the person(s) primarily responsible are not available after the disaster?

As described later in this paper, a good BRP will include all of the information needed to resume business, and include step-by-step, definitive procedures for each team member to follow throughout the business resumption process. If it is determined clearly in advance which team members are leading specific efforts and which other human resources they have to work with, then the organization can work efficiently – using all of the resources available to it to recover from the incident as quickly and gracefully as possible.

When defining responsibilities and roles, it is important to make sure that human resources are not over committed. For example, in event of total office equipment loss, the IT manager may be planning to utilize non-IT staff to follow equipment setup documentation and assist in reinstalling newly delivered workstations – but in event of a total office loss, the operations manager may have those same people allocated to help get basic office space, furniture, supplies, and other non-IT related recovery efforts. In that case, the resources would be over committed – so, it is important to define responsibilities and roles carefully.

In the event of an incident, the first thing that will need to happen is that team members need to be contacted. Where is that contact information? In one of the stolen computers? In the flooded office or burnt filing cabinet? The BRP must contain personal contact information, including address, home phone, cell phone, and email address, as well as emergency contact information for all team members. This information must be updated quarterly at minimum, and as needed. Call responsibilities and initiation procedures must be clearly spelled out and kept updated. Will one person in your organization be charged with quickly contacting a dozen others, or will that person (or their alternates) contact two people and those people in turn contact others? Good planning will result in all team members and employees being contacted quickly and efficiently.

An important part of planning roles and responsibilities is to plan for the non-availability of team members. Is there someone ready to take charge of the plan if the head of the organization is away at a conference or on vacation in Mexico? Is someone ready to lead IT operations if the IT manager is on vacation at the top of a mountain in Tibet? Who can order new equipment if the person in charge of the checkbook is unavailable? The plan must account for these kinds of questions, and should reflect the regular cross-training that organizations should be engaging in as a part of their business risk mitigation practices.

Coordination Sites

Where will you meet and what kind of facilities do you need to coordinate your response? Ideally a location is specified that is near one or more of the off-site locations where you store your BRP, has room for your staff to meet, and has office facilities including desks, phones, fax machines, Internet access and any other capabilities you need to coordinate - or even stage - the recovery effort. When selecting a site, remember that incidents can occur at all hours and response coordination may require working unusual hours. Facilities such as public libraries may not allow for off-hours access.

You may wish to consider having more than one coordination site – for example, your office (assuming if it is accessible), a location across town such as an employee's home or member's office (assuming your office is inaccessible), and a meeting place or coordination facility at a more distant location. If a distant location is required, transportation and even lodging logistics may need to be spelled out in the BRP. You may also wish to consider storing emergency supplies at each site, including food/water, first aid kits, cleaning materials, fire-extinguishers, large work gloves and a toolkit.

Public Relations and Communications Plans

An important part of disaster recovery is to make sure that the correct information is communicated to members, customers, media and the general public. Someone must be assigned the responsibility of deciding when it is appropriate to make public statements and the responsibility for creating appropriate answers to the questions that will be asked by each of these groups. Again, make sure someone is cross-trained in this capacity, in case of a worst case scenario.

Employees must be instructed that, in event of a disaster, they are not to discuss the business impact externally until they are provided with the official and appropriate answers. It is important that other questions that emerge are referred to the appropriate person for answering at a later time. It may be decided that employees should forward all incident-related questions to specific people in the organization and not answer any such questions themselves, especially if the questioner is a member of the media asking probing questions.

Once the 'who', 'when', and 'what' of communications are outlined, it is important to be sure that a 'how' has been equally well planned. How will you reach your employees in different circumstances? If your office has been damaged, will you put up signs outside or in the lobby? If you are a member organization, do you have various ways to contact your members, and do you have their contact information stored off-site where you can retrieve and use it *quickly*? Remember, you'll need another way to send out email if your email server has been stolen or destroyed. Your broadcast fax machine may be another disaster casualty. Think through the 'how' carefully. If you are drilling on various disaster scenarios, make sure you are not using communications capabilities that you wouldn't have in that scenario.

If your communications plan is well designed, your organization will set good expectations with stakeholders, cut down on the confusion during and after the incident, and maintain the professional appearance that you would expect of your organization.

Multi-Site Information / Data Storage

Having the right information and resources at your fingertips is important for recovering from a disaster. If you don't have this, then the first few days after a disaster will be spent planning the recovery rather than implementing the recovery. Consider the information and other resources that you may need to replace your office:

- Insurance information
- Source of immediate funding
- Acquisitions procedures / sources
- Contracts and other legal and financial information
- Total square footage needed (Personnel & office space needs, etc.)
- Office equipment (e.g. copiers, fax machines, etc.)
- Office supplies, forms, etc. (keep master copies off-site!)
- Telephone and voicemail systems
- Computers and network equipment – including configuration instructions and up-to-date backups of configuration files
- Operating systems and software applications – including copies of software, licenses, manuals, and documentation
- Your encrypted password file
- Your data backups
- Internet communications capabilities
- Special climate control and power requirements
- Staff lodging and transportation
- Vendor and supplier support/contact information, including phone company, software vendors, application service providers, and contractors

- Copies of critical files and documents (possibly electronic)

The more complete the information and resources that you maintain both onsite and offsite are, the smoother your operations recovery will be. **Remember to test your software copies and backups regularly if you don't want to find out they won't work at an inopportune time. And to re-iterate a key point: store your BRPs at multiple secure sites – and not all located on the same fault line, flood zone, etc.**

Multi-Site IT Operations Plans

If your organization provides high-availability application services or requires fast recovery from a disaster that impacts operations at a primary application hosting facility, then Clareity strongly recommends that your organization maintain a remote 'hot' data center that can take over providing application access with no human interaction, a 'warm' data center that requires minimal human interaction to switch to, or – at the very least – plan for what it will take to host the application at another facility and have options arranged and documented. Planning multi-site IT operations is a complex subject, beyond the scope of this paper, but Clareity has three tips to consider:

1. If your primary and secondary facilities have geographic proximity or share the same ISPs, there are many disasters that will render both facilities useless. Consider using a secondary facility that is in another region and does not share the same ISP as your primary facility.
2. If you do not thoroughly test disaster scenarios periodically during scheduled maintenance windows, you are not assured that fail over or your backup site will work when you need it most. Test your backup site regularly, as realistically as possible.
3. If your backup facility does not have appropriate bandwidth or computing power, it will be slow or simply fail when you need it most. Sometimes ISPs that claim your bandwidth will 'automatically burst when needed' have been known to make mistakes. Perform adequate scalability testing to ensure your secondary site will serve you well when needed.

Scheduled Planning Activities

A plan that gets outdated, sits on a shelf in a vault, or that no one knows how to implement, is of limited use. Part of the plan must be a schedule and process for periodically updating the plan, training staff on acquisition and use of the plan, including regularly scheduled drills (at least annually) and resultant corrective activities. It is important to occasionally have key people sit the drill out and just be observers to make sure that cross-trained staff can get the job done if needed.

Conclusions

While many business risks can be reduced by identifying and mitigating risks through a process such as Clareity Consulting's "IT Security / Business Continuity Assessment" service, sometimes disasters or significant disruptions will befall an organization. If your organization participates in business resumption planning and creates BRPs to account for each circumstance, it will greatly improve the ability of your response team to coordinate the recovery effort, improve communication to those who are affected by, or those who are curious about, the disruption and minimize overall downtime and productivity-loss. This paper was designed to provide a starting point for disaster planning, and Clareity hopes that the guidelines presented in this paper encourage further planning activities and help improve the capabilities of real estate organizations to respond to disasters and other business disruptions.

About Clareity Consulting

Clareity Consulting was founded in 1996 to provide information technology consulting to the real estate industry and its related businesses. Clareity provides a wide variety of services to MLS, Associations, brokers, franchises, and software, information, and service companies that serve the residential real estate market.

Since 1998, Clareity has performed more IT Security / Business Continuity Assessments of MLS vendors, software vendors, regional MLSs, and brokerages than any other firm and established Clareity as the real estate industry's leading expert business continuity practices, data protection and security.

For more information on Clareity Consulting, please go to www.callclareity.com

For more information on Clareity Consulting's
Security and Business Continuity Assessment
services please contact:

Matt Cohen
612-331-1788
Matt.Cohen@callclareity.com