Cornick Garber Sandler

Certified Public Accountants & Advisors

The new paradigm of Disaster Recovery and Business Continuity for the small and mid-size business.

Juan M. Pousada

Disaster Recovery and Business Continuity applied to the Medium and Small Business models.

Cornick, Garber & Sandler, LLP

825 Third Avenue
New York, NY 10022

212 557 3900

11/10/2009

The new paradigm of Disaster Recovery and Business Continuity for the small and mid-size business.

By Juan M. Pousada

Intended Audience:

The ideal reader is the IT Manager of a small or mid-size company or firm that has to contend with budget limitations when designing and implementing a Disaster Recovery and Business Continuity plan. I will try to explain all terms as much as I can, but keep in mind that this document is not intended to convince the owner of a small business of the need of a Business Continuity or Disaster Recovery Plan. The perfect audience are those IT managers that have read the plans designed by the "big boys" and now have do deal with a shoe-string budget, and very limited resources and are looking for a bit more "unconventional" ideas.

BC and DR

Most companies, whether large or small, will experience either one or multiple business interruptions during the course of its existence.

In the past, companies viewed Disaster Recovery as an afterthought, as something that received the lowest priority, because much like an Insurance Policy, it was an expense incurred for an eventuality no one wanted to seriously think about.

As an IT Manager I've been able to actually put into practice a disaster recovery plan that up to the moment that it was needed, it had been deemed overkill by many of my peers. The occasion was September 12th, 2001.

After the initial shock our plan got implemented as follows:

1. Contacted the people identified as Crisis Managers, the managing partners, the Director of Administration, and arranged for a time to go back in the building.

2. IT contacted our ISP (Internet Service Provider) and confirmed they had activated the Alternate Internet Traffic Route for our internet access.
3. Restarted all servers, and configured our Switches and Routers for the new info pointing to the alternate route.
4. Double checked on that all the planned back-up measures were in place,
5. Posted notices on our web site that our Company was open and operational.
6. Our Crisis Manager followed via phones with all the staff and communicated with our most important clients our status.

And we were up and working.

Those were simpler times, though. 2 file servers, 1 e-mail server and remote storage were sufficient for our mid-size law firm at the time.

In order to gather some anecdotal references, I recently tried to reach some of my peers who were LAN Admins at the time, to see how their perception of Disaster recovery has changed since those days, and unfortunately, I couldn't find anyone still working in the field. Most claimed that they couldn't deal with the hard times that the IT sector was traversing, but interestingly, these were the same peers who at the time voiced their opinion that my contingency plan was overkill, the same ones that had their offices closed or without services for a week or more.

As much as the IT field has changed since the early 2000's, so has the options big companies now enjoy for disaster recovery and business continuity.

Fortunately, the same holds true for small and midsized business (SMB)

If you have the budget (and who does, in these austere times) you can find many companies who will come in, evaluate your business, and draft a Disaster Recovery plan, and even run mock simulations with your departments, at your convenience. I actually have seen some Hedge Funds with 24/7 operations use this services to great success and satisfaction.

But if you don't have the budget (and most SMB's don't) you can utilize the internal IT and Management staff, who usually will only be too eager to get involved on a project that will give them exposure to such an important part of business operations.

HOW TO GET STARTED (DR and BC):

Let's distinguish between two aspects:

Disaster Recovery (DR)

And

Business Continuity (BC)

Notice that this is not an "Either or" proposition.

What you can decide, as business owners, is to which one you will allocate more resources and higher priority, but you will try to address both concepts in a way that satisfies your needs and addresses your budget limitations.

Disaster Recovery (DR) (most of the time) will involve setting up new shop in an alternate location, and is the process of restoring your business back to an operational level.

Business Continuity (BC) will involve making sure your business is affected as little as possible by small outages and problems.

It usually makes sense for a SMB's to design and implement first a BC plan and then design and implement a DR plan. You will realize along the way that while putting in place the pieces needed for your business to continue to remain operational during small outages (something that addresses your BC), you are also doing most of the leg-work needed for your DR planning.

Remember BC is not DR. DR involves BC but BC doesn't necessarily imply DR. If your business is similar to most modern businesses, your organization relies heavily on the Information Technology infrastructure.

Two examples of items addressed by your IT staff are:

- **Backup Internet Access.**

There are many methods and protocols to ensure your business sustains internet access during minor outages.

Depending on your budget you may have 3 aggregated T1's in bridge, from different geographical providers. That way, if Verizon has a problem uptown, your ISP will automatically switch to the other two downtown, provided by Sprint and the third by AT&T. Since your IT manager has done the research and asserted they all come from different geographical points, that water pipe that just exploded midtown will likely not affect one of the three entry points. Nothing goes wrong? Well your aggregation protocol will make your firm the beneficiary of 3 T1's and its consequent speed!

I've seen some businesses implement even Satellite internet, as a last resort, but the high price of this and the lack of flexibility makes it viable only for businesses with a high profit margin and large companies.

- **Server continuity.**

Your IT manager likely will advocate some type of insurance plan with your server manufacturer. This type of DR Insurance guarantees that the manufacturer will respond to hardware requests in less than 4 hours.

In a perfect scenario, your IT department should have a spare server handy, and of course your IT manager will ensure that the new server is totally compatible with the current back-up procedures that your live server currently uses, but this is a scenario that most SMB's can't afford.

Theater of Life Real-Case-Scenario:

_Sir, our Server just crashed!
_Ah, that's why I couldn't reach the L: drive… But I remember you requested a spare server right?
_Yes sir.
_So how long will it take you to bring it up?
_Well… it should take 2 hours…but it doesn't use the same type of back up tape…
_What?
_No, since this one has a more modern and faster tape than the old one…
_But we have our back-ups in the old media!!!
_Yes… well… we found a hardware company downtown that will sell us the drives that read the old tapes. We need $1000.00 for the drives a 2 hours to install them…and then 4 hours to restore that data….
When the owner regained consciousness, he fired the IT Director.

- **Remote access continuity.**

Your internet access and Domain Name Services (DNS) routing tables have just jumped to an alternate setup due to a problem in the geographical area of your ISP. Now that your DNS has changed, and your remote workers can't get pass the firewall. Half of your staff are remote workers!!

- **Specialized areas and their continuity.**

Your Backup server is up and running, but lo! You forgot that you have a whole department of Internet Faxing, and your new server doesn't support the technology installed in the old server. Now you are scrambling to the electronic store by the corner to pick up a bunch of fax machines, just to realize you don't have enough phone lines to plug them in!!

Another Director of technology fired!

Or you may recover the server but forgot about a critical DOS application, which runs in emulation mode.. and your business owner will only be displeased when you can't produce the reports he/she is used to receiving at the end of the day.

Get started with your BC, and move onto DR

No more preambles, no more elaborate explanations. This is the bullet-point list to follow:

1. **Set up the Crisis Management Team (CMT), and outline specific duties and responsibilities.**
2. **Inventory all areas affected**
3. **Outline the Crisis Management Procedures**
4. **Outline the BC Procedures**
5. **Outline the DR Procedures**
6. **Outline the Dispersion of Information Procedures.**
7. **Set a schedule to test the procedures and make changes as needed (Correct point 3 and onward) and repeat as needed.**

Common Elements in your BC and DR Plan

Some of the elements of your BC plan will also be of use in your DR plan, as I mentioned earlier.

Set up the Crisis Management Team (CMT), and outline specific duties and responsibilities.

The members of the CMT should be managers that represent the principal functional areas of the business.

These are the typical departments that you want involved when forming a CMT:

- Information Technology (IT)
- Human Resources (HR)
- Record and Document Management
- Facilities management

This is the worst time to stroke egos. For your CMT team to be effective, you have to fill it with members that are both knowledgeable in his/her area of expertise and have a no-nonsense attitude as well as members with people's skills, that will act as liaisons and appeasers of jittery crowds.

Make sure that you don't appoint a crowd-pleaser to a no-nonsense position, and vice versa.

In your initial meeting your will gather the managers of each department and you will outline roles and responsibilities for the DR plans.

If you deem that a certain department head is not the best person to be a part of the CMT team, get HR to convey it to them in softer terms, or use the old tactic of assigning that person a dummy task, that will keep them occupied but that is irrelevant enough that won't give him/her room to screw something up.

You will also use this initial meeting to introduce them to the people in charge of the Business Continuity Plan. These are the members they will report back to and bring their questions to.

In the CMT there are no Overall Thinkers, or Big-Picture Planners. From top to bottom every member has to be able to set up operations, facilitate DR venues, and in general, pull their weight.

The last thing you want in a Sept 11th scenario is to have an executive moving around with a notepad and a pencil, expecting everyone in the CMT to report to him/her and wait for him to give out the orders. You should try to find the perfect balance of “doers” and “thinkers”, and that will greatly increase the odds of your business surviving in case of a disaster.

Inventorying all areas affected

It is advisable that you have a tool ready that will be common for all departments in assisting them in inventorying the assets needed for BC and for DR.

For most SMB’s this tool could be a MSExcel Spreadsheet.

Each department will return the completed spreadsheet to a CMT member in charge of unifying all the firm data in one central repository.

This is a good time for your CMT to identify and communicate with outside parties that could play a significant role in a DR effort, especially if the team plans to depend on an outsider for significant assistance in the implementation of the BC/DR plan.

Have a list of accountants, lawyers, insurance agents, IT consultants, bank representatives, suppliers, in general, all the business contacts that may need to be kept informed of the new situation of the firm.

Make arrangements with your bank representative, to have an account created for an emergency fund, cash that will be accessible via ATM. Then make sure the proper CMT personal is informed of this, and arrange to have a backup person keeping track of the card and the pin.

Another list could also display account names and numbers, and representatives direct phone-numbers and e-mails.

Last but not least, create a list of customers that are important to the continuity of the business, and you should have the equivalent of a Client Contact list, because they should be contacted in the event of a disaster, and they should be made aware that the firm is implementing a plan they designed to deal with these eventualities.

Don’t Forget the Added Burden of Compliance.

Depending on your type of industry you will also have to deal with

• Health Insurance Portability and Accountability Act (HIPAA)

• Sarbanes-Oxley Act of 2002

• New Basel Capital Accord (Basel II)

• Gramm-Leach-Bliley Financial Services Modernization Act of 1999—

• Uniting and Strengthening America by Providing Appropriate Tools Required to

Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001

Outline the Crisis Management Procedures

At this point you should be able to start creating a chart with some scenarios and some degree of gravity assigned to each scenario.

You can’t respond in the same way if there is a NOC (Network Operation Center) outage in the Northeast that affects your e-mail, as you would if there was a threat of a flood in Manhattan and you had to evacuate the area.

Some firms decide to create a tool with questions, points assigned to each question, a legend at the bottom that adds the total points and then recommends a course of action based on the points achieved. We will refer to this tool as the Threat Assessment Evaluation Tool. Keep in mind that this tool will be overkill for most SMB’s, but feel free to use one in your company if you think it will be useful.

After assessing the degree of response, your CMT should respond accordingly, by matching the points to the type of response assigned to the threat score.

For example: You encountered a problem that affects BC. You checked the items on the Threat Assessment Evaluation Tool and come up with a score of 11. You look at your legend, and see that for threat levels with score between 10 and 20 (your case), IT Should switch to backup ISPs, HR may want to contact remote workers and explain the situation, a department may need to be moved to an off-site area for a specific amount of time.

The CMT should always report back to the CMT coordinator their implementation times. Like in a high-stress gourmet kitchen, communication of estimated times of implementation is critical to achieve maximum efficiency in the implementations of these DR/BC plans.

The Crisis Management procedures will involve:

- Assessing the level of the crisis. Is it BC or DR? To what degree is each?
- Assessing the CMT members involved.
- Communicating to them their expected course of action.
- Implementation of the action plan.

Planning and implementation of a Disaster Recovery Plan (DR).

As I stated before, you should consider BC only a smaller subset of the DR plan, while the DR plan will be your worst-case-scenario plan.

In planning and preparing your BC, you already have a decent inventory, a CMT, and a Threat Assessment Evaluation tool. I would say that is most of the leg work for the DR.

Your IT department has planned for small outages, and for temporary hardware failures.

Let's escalate the plan and enter the Disaster Recover area.

At the smaller spectrum of the DR plan, we have a critical server crashing. Business is interrupted, but we are going beyond business continuity, since you now have to actually recover your data. At the higher end of the spectrum you have a full relocation. For example, your building is in danger of collapse, or evacuated indefinitely due to an undetermined contaminant. Let's set up shop somewhere else.

Again, it's your IT Department to the rescue. They should include all devices that are critical to your daily operations.

Spam filter.
Firewalls.
File Servers.
Systems Documentation (Including Passwords, loggings, and unique IP's, and other settings)

All these items are often neglected and not taken into consideration on the BC plans, and much less on the DR plans. Most of these devices have internal software that requires backups. Are your backups of these devices up to date? Do you have a schedule for these backups? And do you store them offsite?

Basically, you should prepare to either move to another location (if you can afford this) or to

set up you staff to continue working remotely.

Currently, this provision is easier to implement than ever before with services like GOTOMYPC being abundant and affordable. These services will basically provide users with remote access to a host. If your company has issued laptops of pc's to users that will take them home frequently, then you have just made your life even easier in the event of a disaster, since you already have in place the framework of a mobile force.

If not, you may have to make arrangements with the critical members of your staff, to make sure they have the tools they need to work from home, both software and hardware.

Another cost-effective solution is to have stored off-site a package with installation disks and licenses of all the critical software you need, and include in your DR Plan the steps to distribute them in the event of a disaster.

Tailoring DR/BC to the SMB

So far all I've done is translate abstract procedures that most large companies have in place to deal with DR/BC, and adapt them to SMB's.

But let's not forget that while most large companies have budgets allocated to DR/BC, one of the greatest strengths of the SMB is its culture of doing-more-with-less and the flexibility of quickly adapting to changes due to the small sized staff.

Some SMB's are in that magic-number area where it makes economic sense to get VOIP. Those companies may want to consider keeping a VOIP phone set in the home of the CMT leader, and make that number available to all the CMT and staff members. Think of it of the equivalent of the little red phone the president of the United States keeps in the oval office.

In the event of a DR, the CMT members will call that number first to coordinate their efforts.

Another cost effective measure is to have one member of the CMT be proficient with FTP and HTML (Web techniques) and have a segment of your web businesses web page dedicated to addressing emergencies.

Most of the time that page will say

"NO NEWS IS GOOD NEWS"

But in the event of a DR, the CMT member in charge of the web page could post the progress of the DR plan on the website, so all CMT members can follow it, or any other pertinent news to that effect.

Heck, it can even be used to post office-closings for snow-days (SMB's in the northeast and midwest know what I'm talking about)

Some SMB's have a main office and a small satellite branch at a nearby geographical location. The CMT should have a plan to relocate its operations to that location in the case of a DR.

Firm-Wide relocations is a topic that many DR Plans addressed to big businesses cover in detail, and goes well beyond the scope of this paper, but let me bring up some pointers that SMB's with satellite offices who wish to implement relocation DR Plans may want to check, just in case:

ACCESS: "Uh…Who has the keys to this place?". Something so basic that is usually overseen is the fact that at least 2 members of the CMT should have keys to the new site, and by keys we mean access, such as electronic keys, clearance with the building, knowledge of the facilities, parking spaces, access points, loading docks, data closets, etc etc.

POWER: Is your new premises properly powered? How many workstations will be installed in the new location, and how many watts and amperes will they need? Are there printers, fax-pools, copiers or other equipment that requires extra power that should be taken into account? How much Amperage can the circuit breakers handle on your floor?

OUTLETS: Yes, you bring in a new copier as per your DR plan, and your new office area can handle the extra 20 amps, but then you realize the plug is different and you have none of that type on your new premises. Make sure your emergency equipment uses standard devices and plugs to avoid unpleasant surprises.

BUILDING POWER: If the disaster is more generalized to your geographical area… does your new building have independent generators? Should you (can you) have fuel power generators?

CABLE-RUNS: Few things are more detrimental to the staff morale than working at a provisional location, than feeling that such provisional location is a spider-web of RJ45 cables, Coaxial cables and such, and every step could be their last. You could take some time to provision the bare-bones wiring and leave room for growth, while providing covers for the cable runs.

PHYSICAL LOCATION: Any DR space looks great when empty, but.. Does your Canon Imagerunner (HUGE COPIER) fit next to the large servers? Do you have enough room for

all the workstations you plan, and are you taking into consideration the variable sizes of your personnel? Are there any staff members with special needs, such as wheelchair ramps or such?

A lot of SMB's only use an e-mail program, a word-processing program and a spreadsheet program. If that is your case, you may want to invest in CLOUD COMPUTING. Services such as Google Apps or Office Live from Microsoft allow you to work on your documents as long as you have an internet connection. Pricing varies depending on quantity of users and storage space, but it is an incredibly frugal and practical DR measure.

The downside is that you do have to have a decent Internet connection, and then you are at the whim of a third party, such as Google or Microsoft, that albeit they are big companies, they also suffer outages and downtime.

For those of you who have the luxury of having a satellite office, you can make arrangements with your hardware provider (HP, DELL, LENOVO, ETC) and some of them will allow you to pay a monthly fee for DR Server Replacement. In the event of a disaster, they will ship you a preconfigured server to the location you specified.

A measure often neglected by non-IT personal involved in CMT is to ensure that they have off-site copies of the software to be installed.

Nothing worse than having a server arrive, but not having a CD of the tax software you need to have your staff up and running, or worst yet, no software to restore the backup tapes!

Also pretty embarrassing is when you have the applications CD at hand, but no license code to enter, nor the customer account number, much less the secret password to authenticate your account with the customer rep in… let's say… India!

There are too many variables to cover in a simple article like this, but the combinations and variations are only limited by your budget and your imagination.

I have advised a firm with a staff of 5 to insure the server, purchase ONLINE backup licenses, and then make sure that all 5 users can work from home with their existing pc.

The owner established a "re-use" program, in which instead of making the PC's last for 5 years, they would keep them for 3, and then "donate" them to the staff, so they could have something usable at home, in case of a disaster.

In larger firms, I isolated problems such as wrong amperage on the circuit-breaker closets, to the lack of usable land-lines (POTS) to use in the case of an interruption on their VOIP.

Using your firm’s “slowtime” is ideal for revising on an annual basis your DR plans, which means, sending new software to offsite location, updating the list of contacts and licenses, and maybe even choosing a day to run a mock-scenario for disaster recovery.

IN CONCLUSION:

Bottom line is you have to do what matches your firm's needs and your budget. Now keep in mind that a bit of DR and BC planning goes a long way, and it doesn't have to break the bank.

Any vendor worth their salt will try to sell you the most effective and complete plan for BC and DR, partially because the reputation of their business is at stake, but also because they are looking at their own profit margins.

But we all know that most SMB's usually operate at very marginal profits and don't have too much room to work out a budget for DR or BC.

That shouldn't stop you from checking out most well conceived DR and BC plans available out there (GOOGLE is your friend) and then use some of the ideas laid out here to tailor those big plans to your SMB.

There is a saying that has been attributed to Chinese lore which states: "May you live in interesting times"

I can't stress enough that if your business were to live through "interesting times" a little bit of BC or a bit of DR may be all you need to ensure that you sail through turbulent times, and come out on the other side of the storm alive and thriving.

Something simple as using your website to inform your clients and staff of your situation, or making sure that the staff gets the hand-me-down pc's with the software needed to work from home may get you through those moments that may close other businesses, and it may not cost you as much as you think.

Remember, you may not have the big budgets that the bigger firms have, but your small size also makes you more flexible to change, and more malleable to adapt to the "interesting times" that are to come.

Juan M. Pousada

IT Manager at Cornick, Garber and Sandler, LLP

Special Thanks to Robert Reitman CPA and partner and Cornick, Garber and Sandler, LLP for his patience editing this paper

Thanks to Roger Cormoran, from the Wilkins Group, for his input on the section on RELOCATION.