

BCP and DRP from Scratch

del.icio.us

Discuss in Forums {mos_smf_discuss:RichM}

This month's column has been quite a learning experience. Well not the column as much as what I discovered in the process of getting management buy-in for a Business Continuity Planning/Disaster Recovery Planning (BCP/DRP). In all of the information I have read, three main objectives need to be met in order to develop a BCP/DRP good plan. The major emphasis (and motivation behind this column) is point one:

1. Management buy-in
2. Develop the plan (Leave 4 - 6 months for this step)
3. Ability to test and verify plan

Once I approached management they were extremely excited and asked me to come up with a disaster recovery plan in a week. I explained that BCP/DRP takes a long time to create and requires feedback and input from key management members, and that rushing it would create an inaccurate plan. As I watched the decision maker's eyes glaze over, he mumbled something about off site storage of backup tapes and walked away.

And thus my learning experience kicks into high gear.

It is obvious that everything required for the DRP/BCP is not clearly understood by the head decision maker. While good backups are a key ingredient to successful disaster recovery, there are many more components that must be addressed. The only way in which I will get some breathing room to create an inclusive, no-stone-unturned plan is to illustrate all that can possibly happen and how many resources can be compromised that can grind daily business operations to a halt.

Below is a template that you can use to help push a DRP/BCP. When employing this Business Impact Analysis (BIA) template, it is more important to be thorough and detailed than it is to be technical. The main goal of the finished product should be a very shocked and open-minded CEO (president, board of directors, etc.). It is understandable that they

wouldn't think of all the various issues surrounding the events that will impact business productivity. This is your responsibility.

The intent of this style of BIA is to highlight all the little details that need to be addressed in a dependable BCP/DRP. Accuracy is not as important. Painting a vivid image of business grinding to a halt due to the lack of planning (or having too narrow a scope) is. This BIA should be enough to illustrate the need for a proper planning time frame.

Reader's Considerations

Plan for the Unexpected: It is a good idea to outline several varying stages of severity for items like fires and power outage. Though redundant, it helps to create a 360 degree view of what could occur.

3rd Party Vendors: All external access is pre-scheduled and is not mission critical.

Security Implications: All security is handled by the building which requires a physical identification badge for all persons entering and leaving the building.

Satellite Offices: We have several companies all within the same physical location and hence would be under the umbrella of the same BIA.

Acts of God: Prevalent weather and natural disaster considerations which can be region specific such as hurricanes in Florida and earthquakes in California.

Proximity to Hazardous Facilities: Close to a nuclear power plant? It may be a good idea to contact the facility directly, and see if they have a disaster recovery specialist that can help you tailor your BIA.

Compliance Issues: If you are required to be HIPAA and/or SOX compliant, include a brief definition of the statute and any terms not known by your average staff member in the glossary.

NOTE: The BIA below is a small cross section of the document created which, when finished, is over 15 pages and includes over six scenarios including a 100% destroyed workspace and terrorist implications causing widespread disruption at the state level. Please be thorough. The better you can show how devastating the situation can be the more receptive they will be to push your BCP/DRP as a top priority.

Business Impact Analysis

The purpose of the Business Impact Analysis is to identify anticipated risks to business continuity in varying degrees of

severity. The following are the most likely scenarios that could occur (though not an exhaustive list). When an interruption occurs (whether man made or otherwise) multiple factors are impacted and, if not properly identified, could cause a business to close its doors permanently.

The scenarios listed below are not granular but just a representation of issues that could arise and the impact they would have on business activities. They are based on a qualitative assessment and carry a rating of 1 (not likely) to 5 (most likely). A quantitative assessment of losses could be done, but that is beyond the scope of this BIA.

I. Scenario One: Power Outage (Rating = 5)

A. User Impact - The risk for users is minimal, since they would not be able to work for several hours and minimal information would not be processed. Filing of paperwork would be possible if flashlights were made available; therefore, it would not be a complete loss of productivity.

B. Server Impact - Provided the outage occurs during office hours, the UPS will give us approximately 15 minutes to shut down the servers properly. Once power is restored there is no risk of a surge since the UPS' primary responsibility is to keep machines safe from power spikes.

C. Property Impact - This risk is moderate, since not all PCs are on surge protectors. Once the power is restored a spike could occur. This of course could overwhelm the power supplies of the PCs as well and destroy the monitors.

D. Business Impact - The CEO would most likely be able to make phone calls, and, provided the battery on his laptop was adequately charged, he could also enter all pertinent information acquired while on the phone. We may want to look into purchasing 3-4 laptops in case of power failure. Sales people could continue to make calls as well, provided they were willing to use their cell phones. We could also purchase 3-4 pre-paid cell phones to be used in case of emergency.

As stated above, I would recommend that flashlights be purchased to expedite the abilities of all parties making calls. Light should be concentrated in one or two main areas (ex. conference room and open space in IT office kitchen area) to maximize light and minimize the drain on batteries. Lanterns (which run on batteries) would also be recommended.

E. Client Impact (locally) - Guests should be advised to wait 15 minutes to see if power is restored. If power is not restored, they should be asked to re-scheduled and escorted to the lobby via a stairwell. If they are unable to use the stairs every effort should be made to make them comfortable including temporary use of cell phones (if they do not have one) and spare laptops.

Recommended Actions:

1. Purchase enough surge protectors so all printers, fax machines, phones and computers are protected from a power surge.

2. Purchase 3-6 laptops which only have Office 2003 installed, not to be lent out for anything other than an emergency.

3. Purchase 10 flashlights.

4. Purchase 4 battery-powered lanterns.

5. Purchase 3-6 pre-paid cell phones.

II. Scenario Two: Fire in the Server Room (Rating = 3)

A. User Impact - Depending on damage to actual servers, switches, and telecommunications equipment, staff may or may not be affected. If servers are damaged then it will be difficult for staff to work until alternate arrangements regarding a domain controller, mail server and in-house database can be made.

B. Server Impact - As long as the servers affected are not the most critical then business will continue as usual. The most critical servers (in-house database, domain controller, and mail server) must be brought up as soon as is possible. These three machines involve email, in-house database, and the ability for each machine to see the other. It may be advantageous to locate a hot/cold site (depending on desired expense) which can be up and running in a matter of hours or days depending on which option is chosen.

C. Property Impact - There will be destruction of property and it may require emergency ordering of hardware or even replacement of electrical/telco outlets. The floor may need to be repaired and lan cables may need to be replaced. Having a spare switch may mean the difference between working and not working. Old switches should be kept on hand for just such an emergency.

D. Business Impact - As above, the CEO would most likely be able to make phone calls, and, provided the battery on his laptop was adequately charged, he could also enter all pertinent information acquired while on the phone. We may want to look into purchasing 3-4 laptops in case of power failure. Sales people could continue to make calls as well, provided they were willing to use their cell phones. We could also purchase 3-4 pre-paid cell phones to be used in case of emergency.

As stated above, I would recommend that flashlights be purchased to expedite the abilities of all parties making calls. Light should be concentrated in one or two main areas (ex. Conference room, and open space in IT office kitchen area) to maximize light and minimize the drain on batteries. Lanterns (which run on batteries) would also be recommended.

E. Client impact (locally) - There really shouldn't be any issues, since the clients are there to meet and speak face-to-face. There are no technology implications and should not be a concern.

Additional Considerations - First and foremost, a fire alarm should be pulled. While this may cause panic, fire spreads quickly and could easily become a real danger. If possible the fire should be extinguished (fire extinguishers should be charged).

III. Recommended Purchases

a. Surge Protectors - <http://www.cdw.com/shop/products/default.aspx?EDC=375109>

b. Pre-paid cell phones - <http://www.boostmobile.com/plans/premiumprepaid/gettingstarted/>

c. Laptops - http://www.cdw.com/shop/products/default.aspx?edc=1116827&cm_re=HP-_-PZ-_-FP1+HP+Smart+Buy+510

d. Flash lights - http://www.foreverflashlights.com/forever_flashlights_3.htm

e. Battery powered lantern - http://www.batterysavers.com/Bright_12_%20LED_-Lantern.html

IV. Example Glossary (definitions not supplied)

Business Continuity Plan

Business Impact Analysis

Cold site

Disaster Recovery Plan

Domain controller

Hot site

Power tap

Qualitative assessment

Quantitative assessment

Spike

Surge

Surge protector

V. Conclusion

The BIA is the very beginning stage of creating a complete approach to disaster recovery.

Through the identification of certain potential events, we are able to incorporate every key asset and the counter measures necessary to maintain business as usual (or as close to it as possible).

It is important that we attempt to identify business disruption on multiple levels to identify any underlying issues/processes to validate the usefulness of the completed disaster recovery plan. Once the process of creation and testing are complete all information must remain current and should be tested a minimum of once a year.

Hopefully this rudimentary sample BIA will help you in your own organization. As I continue my education on the perils of C-level buy-in, I will be sure to keep you updated in the accompanying forum post for this article. Feel free to use it as well for any comments, questions or recommendations.

Additional Resources:

[Disaster Recovery Journal](#)

[Disaster Recovery Institute](#)

[Business Continuity Institute](#)