Interested in learning more about security?

SANS Institute InfoSec Reading Room

Business Resumption Planning: A Progressive Approach

The purpose of this paper is to provide a basic roadmap for those endeavoring to implement a Business Resumption Plan (BRP) within their organizations. Business Resumption Planning isn't simply dealing with the computers and electronic infrastructure, but the overall process of ensuring your organization can continue to function in the event of a disaster. This paper has expanded on certain critical areas which need to be dealt with during the process, but by no means is this all inclusive. Each organization will have ...

Business Resumption Planning: A Progressive Approach

Wayne Freeman
February 2002
Version 1.2f

Purpose

The purpose of this paper is to provide a basic roadmap for those endeavoring to implement a Business Resumption Plan (BRP) within their organizations.

As outlined in the paper entitled Introduction to Business Continuity Planning by Gan Chee Syong[1], there are several different approaches to disaster recovery and Business Continuity or Business Resumption Planning. This paper takes a closer look at Business Resumption Planning, with the assumption that different options may be used depending on the severity of the event you are dealing with. Regardless of the strategy chosen to deal with a disaster, the BRP should be an integral part of every businesses preparation.

There are many definitions but the one which best defines the underlying reason for Business Resumption Planning comes from the Information Security Forum, The Forum's Standard of Good Practice – The Standard for Information Security[2].

"To provide individuals with a documented set of actions to perform in the event of a disaster, enabling information processing to be resumed within critical timescales." [2]

This is an excellent document which can be downloaded for free in PDF format at http://www.isfsecuritystandard.com/index_ie.htm by providing your name and email address.

Disaster Recovery

When we think of Disaster Recovery we often think of occurrences such as a server crashing, a router going down, or a virus or worm damaging our data. More often than not we are ready for these situations with backups, a replacement drive, or the ability to divert traffic to another machine. But implicit in the Disaster Recovery Plan is a critical, although often discounted component – the Business Resumption or Business Continuity Plan. After all, the key reason for preplanning for Disaster Recovery is to get up, running, and back to business as soon as possible.

An effective, workable, and successful Business Resumption Plan is wholly dependent on a comprehensive Disaster Recovery Plan. Your Disaster Recovery Plan should encompass issues such as failed hard drives, processors, motherboards, data loss, data damage, viruses, worms, external or internal attacks and other impacts upon your network and its entities. It generally outlines backup routines and content, strategies, offsite storage requirements, and emergency boot disk preparation.

Business Resumption

The Business Resumption plan deals with how, where, when, and who will be responsible and what they will do when a significant event occurs. This very well may be a situation where you are starting from scratch, up to and including the loss of the use and access to your primary location, either temporarily or long term, but it also encompasses many other degrees of disaster. The disaster could be the result of incidents such as floods, fires, explosion, contamination, storms, terrorist activities, political unrest, war and many others whose impact may not be clearly evident. Any one or a combination of these can result in you needing to reconstruct your critical infrastructure, possibly in a new location, in the shortest period of time possible.

This is where your Business Resumption plan, entirely dependent upon your Disaster Recovery plan for its success, comes in. If you have taken the time to think things through, effectively planned, implemented, and tested your Disaster Recovery Plan you are on your way to getting back to business.

But what do we need to take into consideration for this Business Resumption plan? What "critical" questions need to be asked? How do I get started and what do I need?

This paper will present an outline for a Business Resumption Plan, answer these questions and others, and get you well on the road to being more effectively prepared for a catastrophic event which affects your businesses ability to function.

A good Business Resumption Plan[3]

- identifies the pre-set arrangements you need to have on "stand-by" in order to get vital functions operating again with as little delay as possible
- ensures the availability of necessary resources including personnel, information, equipment, financial arrangements, services and accommodations
- helps an operation to survive an unplanned interruption by making sure essential clients needs can be met until normal operations are resumed

Many people and firms talk about Business Resumption and Disaster Recovery Planning. Amongst all the talk a reasonably consistent process emerges when it comes to putting together a Business Resumption Plan. There are several key areas you must deal with, and the following is a brief outline of these areas obtained from the University of Massachusetts Business Continuity and Planning Guidelines[4].

This is a **sample** list and is not intended to be all-inclusive.

1. Establish a Business Resumption Planning Committee
   Project Leader
   Project Plan/Control
   Committee Selection
   Assign Responsibilities
   Regular Committee Meetings
   Periodic Management Briefings

2. Perform a Business Resumption Capability Assessment
   - if a disruption were to occur today, how quickly and fully could you resume business/services?
   Security Check List
   Recovery Analysis
   Task Assignments

3. Perform a Risk Analysis
   Risk Assessment
   Risk Management
   Evaluate Threats
   Establish Controls
   Review Security Measures

4. Analyze and Define Requirements for Recovery
   Hardware
   Software - system and application software
   Communications
   Back-up Data
   Physical Facility
   Vendor Support
   Inter-Campus or Commonwealth Agency (MITC) Support
   Personnel
   Security
   Office Equipment
   Forms/Paper Supplies
   Logistics
   Storage
   Funding/Purchase Orders

5. Design and Document the BRP for Recovery Operations
   Organization
   Damage Assessment Team
   User Liaison Team (if needed)
   Communications Team
   Operations Team
   Security/Back-up Team
   System Software Team
   Procurement Team
   Facilities Team
   Identify Processes Required
   Develop Procedures (by team)
   Risk Manager or University Audit Review and Approval

6. Conduct BRP Implementation Training
   Select Training Topics - emergency procedures, use of fire extinguishers, backup retrieval, etc.

Select Instructors
Develop Training Material
Risk Management
Procedures
Select Personnel for Training
Train Personnel

7. Test the BRP
   Frequency - at least annually
   Develop a Test Plan/Script
   Test Scenario
   Evaluation and Reporting
   Follow-up

8. Maintain and Update the BRP
   Follow-up BRP Test
   Report Test Results to Risk Manager
   Institute Controls/Changes - environmental, procedural, personnel, training, etc.

This guideline contains very good sample documents and checklists in support of the above outlined procedure. Many other sites also have excellent information, and a significant amount is available for free. Most, if not all governments, including state, provincial, and federal departments have guidelines for Business Resumption Planning, often with plans and samples online. Some of these guidelines are older, having been developed during the days of Y2K preparation but they are still very valuable references when undertaking this type of planning. Here are a couple of good references,
http://www.irs.ustreas.gov/plain/bus_info/tax_pro/irm-part/part01/28912.html#ss5 ,
Internal Revenue Service
http://www.wa.gov/dis/portfolio/itdisasterrecoverypolicy.htm ,
Washington State Disaster Recovery/Business Resumption Standards

As you can imagine, pulling all this together is an enormous task, and one should anticipate several months from the time you begin this undertaking until the time you have actually tested your plan.

Baseline Requirements

Before you can begin to design a Business Resumption Plan there are some primary Disaster Recovery activities that must be implemented. Without these procedures in place no plan will ever be successful.

- Your mission critical data must be backed up, with a defined schedule, and fully documented. This includes which server is backed up onto which tape, where key data is located, type of backup device, and even backup type (differential, incremental etc).
- At least one set of backups must be in secured offsite storage. This set should be rotated back onsite, with a more recent backup sent offsite. Rotation should occur at a minimum of once per week. You should also

maintain a full month end backup and a set of current emergency repair disks offsite.

- ❖ DHCP and DNS records or databases as well as any active directory or similar databases and registry information should be included in your backups.
- ❖ A set of installed software media, including serial numbers, support account information, contact information, and any other pertinent data should also be securely stored offsite.
- ❖ All mission critical servers should be connected to Uninterruptible Power Supplies.
- ❖ A copy of your documentation for your LAN/WAN should be maintained offsite.
- ❖ A document containing names, addresses, and contact numbers for your key staff members as well as suppliers and clients.

When the above Disaster Recovery prerequisites are in place, you can begin working on your Business Resumption plan.

Where to Start

Some prerequisites for successful Business Resumption Planning[3]

1) Senior management must be actively involved in the development of the business resumption plan. They must:

- agree to the need for such a plan
- assign the necessary resources for plan development
- concur in the selection of essential activities and priority for recovery
- agree to back-up arrangements and the costs involved
- be prepared to authorize activation of the plan, should the need arise

2) A large organization should have a project coordinator to develop the plan. The plan should be developed with input from managers and employees at all levels who will be involved in implementing the plan

3) Personnel

Have key employees seen the business plan and are all employees aware that there is such a plan?

- Have employees been told their specific roles and responsibilities if the business resumption plan is put into effect?
- Have information sessions on business resumption plan been held?
- Does your business resumption plan include home/ pager/ cellular/ numbers of personnel with key roles in the implementation of the plan, and are they available on a 7 X 24 basis if necessary, (vacation, etc.)?
- Do designated employees know who does what in the event of an emergency?
- Have people with special needs been identified and provisions made for them?

- Does your business resumption plan provide a means for replacement staff when necessary?

4) Building Premises

Consider the condition of your buildings, -- old, recently retrofitted or new and the impact this may have on some details of your business resumption plan.

- Do you have access to a building engineer who can inspect the building and facilities soon after a disaster so that damage can be identified and repaired to make the premises safe for the return of employees as soon as possible?
- Is there a plan for the regular inspection of the buildings and facilities, with an inspection checklist?
- Are there hazards in neighboring and adjacent buildings that could endanger life or your business / organization?
- Do you have plans for alternative shelter, if needed?
- Do employees know where the alternative facilities are located?
- What is the risk of failure of such systems as electrical power, natural gas, toxic chemical containers, and pipes?
- Are toxic materials safely stored?
    - If public or general transportation is disrupted, will that affect your operations? Has this been considered in your business resumption plan?

5) Information Technology

- What arrangements exist for emergency telecommunications?
- Have provisions been made so that employees can communicate with their families without overloading telephone circuits?
- Is there a plan for alternative means of data transmission if the computer network is interrupted? Is the plan in writing? Are key staff aware of it? Has the security of alternative means of transmission been considered?
- How frequently do you test your recovery plan for electronic data processing? For communications during an emergency?
- Does your business resumption plan incorporate a review of computer operations and analyze networking and interdependent systems?
- Are computers protected from leakage from fire sprinklers and pipes on upper floors?
- Does your business resumption plan consider accessibility to a back up power generator? Power conditioning?

6) Administrative procedures

- Does your business resumption plan cover administrative and management aspects in addition to operations? Is there a management plan to maintain operations if your headquarters is severely damaged or if access is denied or limited for an extended period of time?

- If some or all of senior management are unable to work, does your business resumption plan have procedures that will enable others to assume these responsibilities? (Is there an executive succession plan?)
- Is there a designated emergency operations center where incident management teams can co-ordinate response and recovery?
- Have essential records been identified? Do you have a duplicate set of essential records stored in a secure and approved location?
- Are essential records separated for easy retrieval from those that will not be needed immediately?
- Does your business resumption plan include the names and numbers of suppliers of essential equipment and other material?
- Is there a procedure to check the protective and emergency devices in offices? (alarm systems, security procedures)

7) Contracts

- Do any of your contractors provide a service or deliver goods that are essential to the continued operation of your business and if so do these contractors have business resumption plans in case they are also affected by the same disruption that has interrupted the functioning of your business?
- Have alternative sources of supply been established?

Although these are only an outline of the prerequisites for a BRP, they provide an excellent starting point for our discussion. As you can see significantly more than just computers and technology is involved. We will now expand on some of the primary points, and try to bring them into the context of the overall Business Resumption Planning process.

Management's Involvement

We all know management can be a tough sell on anything security related. We will hear the no money, no manpower, and various other reasons to avoid implementing many of the tools we need to do our jobs. Unfortunately, selling Business Resumption Planning to management may be an easier task today than it may have been previously.
This stage of your plan is critical. Without senior management buy in an already significant task will become onerous, if not impossible. Key information and data needed for your plan may be lacking and other areas may fall short as input, cooperation, and prioritization of critical information needs are minimized by key players in the organization in favor of what they consider their priorities.
Prior to presenting your request to management for approval, you need to spend some time preparing. Outline what you are setting out to accomplish, the process, a cost estimate on resources such as person hours, any hard costs you can think of which are relevant to your situation such as hot or cold site fees, recovery hardware, backup tapes, offsite storage fees, and add a small buffer for unforeseen expenses. Senior management likes to see what the cost of anything will be prior to approving it.
You should provide them with an outline of your plan of action so they can be aware of what activities will be occurring, and when. If others begin to ask senior management

what this is all about and why, they need to have the answers. There is nothing worse than having to placate an executive who was questioned about something and didn't know what was up.
Make certain you supply senior management with copies of your proposal, timeline, and cost details, and ask for a sign off to proceed. You may also wish to draft an email explaining what will be happening, who will be involved and at what level. Ask management to review and send out this information (or approve for you to send) to the key individuals whose input and assistance you will need as you proceed.

Project Coordination and Key Players

After receiving approval to proceed you will need people from other departments within your organization. This means meetings, discussions, and the compilation of a good quantity of information into consistent standards within your plan. This is another big reason for the need for management's buy in to this process.
You will need to identify the key people in certain areas who will eventually become integral within the actual plan itself. For now these key people must be involved in the project as their operational knowledge is critical to a successful plan. Their expertise and input, especially departmental and responsibility specific information will be needed during the information gathering.
During this stage you need to define the project, appoint a project leader or coordinator, outline the requirements and responsibilities such as identifying key departmental players, specialized department equipment, minimal required operational needs as well as what it will take to fulfill these identified needs to maintain the minimal acceptable level of operation. Once these have been identified you will be able to proceed with the information gathering stage of the process.
In some cases this process may be done on a department by department basis, with the overall plan being compiled, coordinated, and finalized using the departmental mini-plans.

Information Gathering

Information gathering begins with determining what you currently have, how it is used, who depends upon it, and how it fits into the overall scheme of things. This is the most important aspect of the planning process. Everything you gather here will be used throughout the rest of the process to define your actual plan. Some of these items will overlap with the Baseline Requirements, but this is indicative of the interdependency of the Disaster Recovery and Business Resumption plans.

The Inventory

- The first thing you need to inventory is the people in your organization. Human assets and more specifically their specialized skill sets will be very important when it comes time to define specific responsibilities within your plan. Skills, be they technical, logistic, or organizational are important components of your plan.
- Assess your existing building and adjoining premises. Determine what exists around your organization and if proper restrictions or controls in place to deal with these items. This component is covered in somewhat more detail in the upcoming section titled Your Location.

- The physical inventory must be detailed and accurate. This doesn't just mean you have 42 servers, 950 workstation, 2 routers, 22 switches and so on. Don't get me wrong, this is important but you need more. The more detail you have in this area of your plan the better. You need to inventory all hardware, complete with all the pertinent technical details. An example of this would be a Cisco router, series 7500, X ports. This router was setup in this way, and here are all the subnets, the configuration, the passwords and it managed this internet connected IP address. Another example would be a Microsoft Exchange Server™. It was on a dual PIII 800, 1GB of ECC ram, 8 36GB hard drives which were set up in this manner, and it was server Y and a member of site X. The exchange service account name was exchgservice and the password was a2c/1B3]*. You also need departmental information for hardware such as fax machines, secure fax machines, photocopiers, production equipment like industrial CD Burners, as well as any other hardware used in the day to day operations. This process is actually beneficial in two ways. It is needed for your BRP and it can be used for insurance purposes.
- What documentation and records exist which would have a direct bearing on the businesses ability to function. These would need to be identified, on a departmental basis and reasonable processes put into place to ensure their availability. This may simply be synchronization with an offsite server, or sending copies off to secure storage. This brings into question the need for a records, document recovery, or repository strategy. This is a topic for another paper, so suffice it to be said it is something you may need to consider in the future. Certain papers and documentation like banking information, corporate registrations and incorporation documents, signing officer verifications, as well as contact information should already be stored offsite at a lawyer or accountants office.
- You need to ask the question, if something happened do we have or need an alternate site to relocate to? If you do you will need to visit and assess this site as well. This site should conform to some specific requirements, but aside from military guidelines which are older and may not have any applicability to a civilian situation, recommendations on this aspect are hard to come by. You should take into account items such as separate power grids (producers maybe too), water and other utility supplies, location relative to your current site with respect to flood plains, avalanche paths, coastal plains, forests, nuclear facilities, airports and other areas which may be locked down during a disaster.
  As a rule of thumb your alternate site should be a minimum 25 miles from your existing location as should your offsite backups[9]. This ensures that they are outside the blast radius of a tactical nuclear explosion. I know this sounds a bit "cold war" but information security has been, and will continue to be heavily influenced by government, especially the military.
  Overall this implies that any event which could cause enough destruction to force you to relocate will likely be large scale and you need to plan for this.
  This secondary location may be another corporate office, and if that is the case a portion of your plan should be dedicated to outlining how this will work, and if there are more than two offices what goes where, and when depending on what disaster actually occurs. A second company office may make your plan somewhat

easier to do, but it still doesn't remove the need for one. Some or all data may be available at both locations, but some may not. Also, most offices will not have the necessary space to handle the relocation of all your employees. This issue needs to be dealt with no matter what your situation is. And a word of warning – DO NOT JUMP INTO TELECOMMUTING as a solution, especially using modems.

- Make certain your ISP and Telephone Company can provide you service at the alternate location. You also need to document your connectivity, both externally and internally. Know who your ISP is, who to contact and what time frames you are looking at for replacement service. Know who manages your DNS records and how to contact them for changes if you don't manage your own. Fully document your internal network, including subnets, IP addressing schemes, what servers connected where, and how any intra or inter site communication was set up (replication etc). Find out and document who takes care of your telephone system, how to contact them, and how they would go about providing your service, and at what level within what time frame should a disaster occur.
- You should document your server configurations and one fairly easy way to accomplish this is by using screenshots. Take screen shots of critical setup information using Paint shop Pro™ or a similar program. This includes DHCP, DNS, and WINS settings, mail server settings, and any other software package settings that have custom setups. Then take all the screenshots, sort them into folders with meaningful names and burn them on a CD. This CD is then placed in offsite storage. As the majority of these settings rarely change you can simply monitor your change log book and if necessary take a new screenshot, burn a new CD, and then swap out the CD from offsite storage. This makes rebuilding any machine significantly easier.

You now need to assess this inventory and begin to prioritize. During this stage you will need to define how exactly you would start to reconstruct your network. For example, are phones and faxes or a customer service counter more important? Is your mail server more important than your database server? Are you prepared to put your web server up before your firewall?

Prioritization

Prioritization is the process of understanding what will be needed, when, and how long you have to get things rolling again.

Of course every department manager will tell you they can't possibly live without their computers, phones, accounting program, printer and many other things. But this process, once defined is not inflexible. The one consistent activity is the establishment of basic telephone communication and should always be first on your list. You should however present your draft of this to management and once again get their buy in. You will find out very rapidly if you have it right, for all you know they want accounting up before email. This will also give you the confidence that you are meeting management's expectations.

From this inventory and priority assessment you will eventually be designing a procedure for enacting your plan should it ever become necessary. Although this comes later, the information you compile now will be important when you begin this aspect of your plan. For example, knowing what hardware your mail server runs on will be critical if you need

to acquire new hardware after a disaster. This initial planning and documentation stage makes the recovery phase that much easier.

The Government of Canada outlines the following as a process to follow when completing this step of your plan. This list is available as part of their **Business Resumption Planning: A Guide**[3] which is available free online.

- 1. List the major functions or activities of your business or organization. (in a large organization, list the "time-critical" functions or activities of each unit, division, department, branch etc.)
- 2. Determine which activities are "time-critical" business functions
    - An essential business function is a service or activity whose continued operation is considered essential by management. Non-performance of this function would significantly impair the successful functioning of the business or organization.
    - Consider the following as they apply to your business or organization:
        - What functions would have to be done immediately after a business interruption? What could be postponed?
        - What are your external requirements on a day-to-day basis? What do you need from outside your business/organization in order to be able to continue to function?
        - What are your immediate internal requirements? Where do they come from?
        - How long can your essential business functions be inoperative?
        - Are there regulatory requirements or penalties that must be considered if you cannot fulfill your obligations due to an unplanned business interruption?
        - What is the financial impact of non-performance of a business function? How significant is this impact? Is it measurable?
        - What are the costs to respond/recover versus the short-term lost revenue?
        - Are other organizations dependent on functions that your business or organization performs? What are your external outputs?
        - What legal or contractual liabilities would arise if the activities were curtailed or shut down?
        - What would be the public relations implications of a curtailment of your activities or a shut-down of your business?
        - Would the safety or security of personnel and property be jeopardized if your operations were interrupted?
        - Which of your essential operations are dependent on computer support? [Mainframe, WAN, LAN and stand-alone] Are there

alternative manual operating procedures in place with people who know how to use them? How long could these operations be performed without computer support?

- Are there provisions for overtime for staff and for additional or replacement staffing?
- List important clients or contacts, external and internal.
- Identify essential operating information for vital business functions and prepare a checklist of essential records. Maintain copies of essential records off-site.
- Determine what essential office equipment is required. Specify any special computer hardware, software, databases, networks or other technology.
- Identify your work in progress. Determine the work flow and business impact if the identified information and work in progress were destroyed and could not be recovered.
- Identify any work in progress for your business or organization that is being done outside your facility.

- 3. Assign a priority to each of the "time-critical" activities you have identified.
  - One way of assigning priorities is to assign a numeric scale from 0* to 5 to show the length of time the activity can remain disrupted. For example:
    - Immediate = Priority 0 (*author's addition)
    - 1 day = Priority 1
    - 2- 4 days = Priority 2
    - 5- 7 days = Priority 3
    - 8-10 days = Priority 4
    - 8-10+ days = Priority 5

Once you have completed the identification and prioritization of the business functions it is time to outline your planning objective, or basically what gets fixed, how quickly and to what level of service. It may help to structure this in the form of a table such as that shown below.

Essential Function	Resumption Objective (priority)	Recovery Alternative
Telephone Service	0 - Immediately	Cellular Telephones
Email Connectivity	0 - Immediately	Free service – temporary solution
Firewall Protection	1 - First Day	Co-Location

You may also wish to deal with other less serious issues at the same time. These may not seem significant relative to some disasters however the more thoroughly documented this information is the better off you are. It is also much easier to complete this while you

have all the pertinent information at your fingertips. The following is an example of some issues which more closely reflect what we are likely to see.

Equipment	Impact	Action	Interim	Down Time
File Server PC	Loss of access to data on machine	Advise Help desk	Recover data to other server (if available)	Several hours up to 1-2 days
Gateway/Firewall PC	Loss of services to users and file transfer	Advise Help desk	Users would lose some external connectivity	1 day
Hard drive in file server - RAID unit	No impact	Hot spare hard drive should start up	N/A	Possible 1-2 hours - ability to schedule downtime exists

- 4. Develop a planning objective for each activity.
    - A planning objective states your goal for resuming each activity, specified to a level of service and within a specific timeframe.
    - *For example:*
        - To staff essential or designated positions at an alternate site within four hours of the business interruption.
        - To have alternate information processing arrangements that will meet essential computer requirements within 48 hours of the business interruption.
        - To be capable of answering 50% of incoming customer calls within one hour and 100% of calls within four hours of an interruption.

These levels may differ depending on the event. You should define a Minimum Acceptable Recovery Level (MARL) for each item based on an incident[6]. The Minimum Acceptable Recovery Level will be set significantly different for a hard drive failure than it will for an event requiring relocation.
You can see from the above points how the previously gathered information can be pivotal. For example, without the contacts and time expectations from your telephone provider you cannot set realistic objectives.
The one thing this plan must be is as realistic as possible, particularly when you consider that your organization and more specifically your senior management will be setting their expectations based on what you tell them. These objectives need to be as specific as possible and focused on the impact of the disaster, not its cause[3]. As an example, the second point above is very vague. You have prioritized your time critical activities so why not set specific objectives. For instance you could set an objective that all priority 1 items will have alternate arrangements within 18 hours, all priority 2 items within 36 hours and so on. You could also break out your priority items in order of importance. Within priority 1, item 1a (firewall) will be online within 9 hours, item 1b (email) will be online within 10 hours. This will assist in further defining the process, and focusing people on specific tasks.

The one component of this that is often overlooked is the complete interdependency of a business resumption plan. There will be no way you can meet your objectives if the person responsible for acquiring replacement hardware takes 8 hours to make the first phone call. This also goes to the absolute importance of knowing as much as you can about the services you are dependent upon. Saying the firewall will be up within 9 hours won't cut it if your ISP will take 24 hours to get you connectivity.
Telephone service is a little easier, you can generally acquire several cellular telephones almost immediately and most telephone companies can redirect your primary incoming lines in short order. This isn't a long term solution, but it does provide basic communication and allows staff and customers to contact your company. It also allows you to advise customers of the situation and direct staff to alternate locations or request they perform or assist with critical tasks.

People and Responsibilities

As evidenced in the previous discussion there are a significant number of tasks which will have to be undertaken simultaneously. Within your BRP you will need to outline the key players, and how you can contact them in an emergency. But after you have contacted them you both need to know what tasks they will be doing and when. Having this information documented and communicated up front will ensure everyone is focused on what needs to be done, not what they think they should be doing. You also need to define some way of differentiating between levels of disasters.
Documenting the people, their roles, what tasks they are responsible for, how to contact them as well as a backup person is imperative. It is also very important that all this information is communicated to these people, and that they have a complete understanding of what they need to do, why, and when. The tasks throughout your plan are interdependent, and if one area or task is missed, incomplete, or partially done it will affect everything else.
When assigning these tasks you need to carefully consider the roles themselves and the tasks in need of completion, as determined within your human asset inventory. You need to assign appropriate people to these tasks, and the person who is normally responsible for completing a task is generally the best person to assign the task within your BRP. You don’t want your top system engineer running to the offsite storage to get your tapes while your asset management person is fumbling around trying to get your primary admin workstation installed.
You also need to deal with issues such as contacting all your staff to advise them of the situation. Having all the staff show up at work and the building is flooded with two feet of water is not ideal.

Your Location

The building housing your organization as well as those in close proximity can affect certain areas of your BRP. Each building is unique, and like everything else you will need to take into account factors which may impact on your plan. One good place to begin is with your building's management. They may have their own disaster response or recovery plan which will assist you in dealing with certain situations.
Items such as backup power generators, fire response plans, and hazardous material handling plans will provide you with procedural information as well as other related data. In some situations your building management's plans will directly affect your response

time. However, this information will assist you in setting reasonable expectations for resumption, provide you with contact information, and allow you to be more realistic when outlining your plan.
Based on this information you can also begin to determine at what point you will actually begin to relocate, under what circumstances you would need to acquire replacement equipment, and to what level you respond. You may only need to relocate temporarily, and it may be possible to gain access for the purposes of retrieving existing hardware for use at your temporary location.
As previously outlined, certain distances and fundamental issues need to be closely examined when selecting an alternative location. If there is a major power outage, your secondary location will also be useless if serviced by the same power grid as your current location. A toxic spill may result in the evacuation of a large radius, and if your secondary location is too close it may well fall under the same access restrictions as your primary site.

Pulling it Together

After all your information gathering, research, discussions, and documentation has been collected and organized you need to begin the process of compiling the data into an operational plan.
In order to do this you need to define some processes and procedures. First, you need to define possible occurrences or threats in an order based on the potential they will occur. Below is a sample list. Based on your location these may change.

List of potential disaster threats in order of likelihood of occurring:

1. System software failure
2. System hardware failure
3. Electrical power failure (longer than UPS life)
4. Air conditioning or other environmental failure (filtration, excess pollutants)
5. Telecommunications or network failure
6. Water Damage (sprinkler system failure, air conditioner, flood)
7. Fire or smoke damage
8. Building related issue (occupation IE: protestors, legal, environmentalists)
9. Toxic material spill
10. Civil disorder, riots, threats
11. Vandalism, sabotage or other direct damage
12. Accidents or acts of nature that damage buildings, equipment or supplies.

Now you should consolidate your hardware information and organize it so it follows the list of previously identified priorities. This will come in extremely handy when you need to deal with a damage assessment and the decisions for acquiring new hardware if needed. While you are doing this consider any potential for consolidation. If you can replace three lost servers with one, you should consider it at this stage. You shouldn't put your mail daemon on your firewall server, but you certainly could consolidate a couple of file servers into one.

Now outline potential levels of plan activation. In this area you could start with something simple like a failed hard drive and progress through to a complete site relocate. The degrees in between are something that will differ for every company. If your building is located beside or close to a chemical manufacturer you would need to include a response level to a chemical leak or explosion. Ideally this is based on the previously formulated list of the likelihood of certain disasters occurring.

Next you need to determine at what point you will activate your plan, and to what degree. This can be a very subjective outline, and certainly not exempt from modification should the need arise. This outline can take several approaches. One is based on expected outage time where you act on assumptions regarding when you will be able to get back into your existing building. If the outage time is 72 hours you proceed to one point, if the time will be seven to ten days you proceed in another manner. You also need to know who has the responsibility for approving the activation. This should be someone in a senior position with the ability to make decisions affecting the organization as a whole. A General Manager, Vice President, or Chief Operating Officer would be good choices. And you should have more than one person designated so there is no confusion as to who can make the decision if the primary person is unavailable for any reason. This information should also be explicitly outlined.

Name (listed in order of contact priority)	Position	Home phone	Cell phone or pager	Contacted (Y/N)	Date / Time
Bob Smith	**SR. VP OPS**	**(222) 222-2222**	**(222) 222-2211**		
Alice Green	**C.O.O.**	**(222) 227-2122**	**(222) 384-4578**		
Buck Rogers	**C.I.O**	**(222) 123-5847**	**(222) 123-6912**		
Jimmy Dean	**C.F.O.**	**(213) 458-6821**	**(213) 456-9821**		

After an event, but prior to the activation of your plan you must assess the situation and if deemed necessary determine at what level you need to proceed. A significant amount of information gathering will need to be done in the first few hours. Defining the situation and establishing an overall status and the path forward is key. In some situations the needed action will be obvious, but in most cases further information will be required prior to formalizing a decision.

A great number of your external contacts, as well as building and area security, law enforcement, and even government departments may play a role in helping you define where you stand and your short term course of action. This will help in generating a damage assessment to assist in outlining a path forward.

Based on the damage assessment your Executive Team will need to make the decision on whether to declare an emergency (this is separate from any other body declaring one) and invoke the Disaster Recovery / Business Resumption Plan at a certain level.

Obviously the damage assessment is a very important factor in the process, and forms or other ways of documenting the incoming information should be in place. In Appendix "A" there a couple of sample forms which can be adapted to your specific needs or simply used to guide the creation of your own.

External Contact Information

Company/Org	Contact Name	Type	Contact Number

Telephone Company	Business Office	Office	(222) 222-2222
ISP	Bob Smith		(222) 221-2121
Compaq	Jim Jones	Office	(421) 769-1111
Building Management	Chuck E. Cheese	Office	(123) 456-7890
Police	Desk Sgt.	Precinct Office	(123) 789-0123
Fire	District Chief	Shared Cell	(213) 456-7823
Government hotline	Gov't employee	Office	(401) 528-9631
FEMA	Billy Bob	State Office	(402) 268-7894

Once a determination has been made, your Disaster Recovery/BRP may come into effect. Certain items will need to be reviewed regularly such as the status of your employee notification process. Needs must be defined and approved such as overtime, capital purchases, and other related items. You may also need to define shifts or schedules for recovery work. It is very helpful to have forms and documents in hand to manage this process as well.

The overall coordination of this process must be centralized. People will need to know where to call, where to go, and the most likely place to contact someone with the authority to make decisions. Depending on the severity of the disaster it may be possible that only some aspects of your plan are needed. Be prepared for ongoing and detailed assessment of the situation. Throughout this initial assessment you need to keep your teams apprised of the status of the situation and ensure they are prepared for any eventuality. Remember, telephone communication is always the first priority for recovery.

After you have completed this stage of your plan you need to begin to define the teams you feel you need. Once this is done, you need to assign people to these teams.

Using your assessment of your people, and taking into account their specialized skills begin to assign them to teams based on the roles you feel you need. This information should be documented along with contact information. A sample table is below.

Team Name	Name	Home phone	Cell phone or pager	Contacted	Date / Time
(Exec) Mgmt Team	**Bob Smith**	**(222) 222-2222**	**(222) 222-2211**		
Mgmt Team	**Alice Green**	**(222) 227-2122**	**(222) 384-4578**		
Alternate Site Team	**Jim Jones**	**(222) 123-5847**	**(222) 123-6912**		
Offsite Storage Team	**Jane Black**	**(213) 458-6821**	**(213) 456-9821**		
Software Team					
Hardware Team					
Applications Team					
Network Team					
Operations Team					
Salvage Team					
New Hardware Team					
Database / Security Team					
User Liaison Team					
Supply Procurement Team					

This process will begin to divide up the responsibilities and tasks needed to be undertaken should your plan be activated.

Team tasks need to be outlined and fully communicated to all members. As indicated above the teams should be comprised of those who are the most knowledgeable or proficient at a task. In a worst case scenario ensure at least one member on the team has the requisite knowledge. Tasks can still get accomplished with one person coaching or overseeing others. You may also wish to combine teams, depending on the available manpower. The offsite and software teams could be combined as could the hardware and network. Every business and situation will be different in this regard so ensure you plan for what you need.
The team functions and tasks in Appendix "B" are examples. You can choose to make them significantly more detailed, or keep it relatively neutral and rely upon specific delegations during an incident. The more you have documented, the smoother things may run, but flexibility is the key.
Now the teams will be assigned specific tasks. The easiest way to accomplish this is to outline what needs to be done in various stages of your plan. Then assign a team to be responsible for the task. For example, if you experience a disaster you need to accomplish several things fairly quickly:

- Secure telephone communication ability
- Verify the whereabouts of all staff and their status
- Confirm the nature of the event
- Allow staff to contact their families
- Begin damage assessment

Based on these five items your plan should define who will get the telephones available and working, who starts trying to contact all staff and maintain a list of who has been contacted, their status and location. Also who will be managing incoming telephone calls, and who will be responsible for contacting or providing the ability for employees to contact family. And finally who makes the inquiries to building management, authorities, or emergency workers to begin establishing the status of the event and who oversees the compilation of the damage assessment.

At this point you have designated teams, assigned priority tasks and outlined team responsibilities. These may also include retrieving offsite backups, ordering hardware, and communicating tasks and duties to staff. You may also need to reassign teams or team members as your plan progresses. For example, if the event does not entail relocation then your alternate site implementation team could be used elsewhere.

Also, designate someone to act as an anti virus contact. Define a policy that absolutely no diskettes or network access is approved until all equipment has current virus scanning software installed and all media is scanned. The likelihood is that someone somewhere will be attempting to get themselves, or their area functional independent of the overall effort. Should they happen to bring in diskettes or other files which are infected with a virus you will end up with double the disaster. Unfortunately if you experience a disaster, sooner or later people find out and you will become a target so security is a significant concern.

You also need to deal with returning to your previous location when it is possible to do so, or how you would go about moving to a new permanent location. This will take a little more work, and much may be unknown but a reasonable baseline plan could be designed. This area has room to maneuver as your time scales will be less restrictive and you will have the benefit of time to plan.

Once you have documented all the details into a cohesive plan you will also need to provide copies to everyone who was involved in the planning for their review and input. You should then finalize your plan and present it to management. A thorough review and sign off from them is necessary. The key factor here is that senior management has the ultimate responsibility for this plan.
After this process is finalized you then need to communicate the plan to all staff. Awareness is valuable in this process, and staff will appreciate the fact that they have been involved and that the company is prepared to deal with situations of this nature. Some of the information they may already know such as the designated external meeting place for staff in the event of an emergency, or who oversees the evacuation of disabled employees in an emergency.
All key players should have a copy of the non secure portion of the plan and understand what their responsibilities are. Regular reviews of the plan are an absolute must and they should include the accommodation of new hardware, personnel changes, location moves, and anything else which could impact the execution of the plan.
Your plan should be stored in your secure offsite storage with your backups and other disaster recovery information. One important fact here is that your plan will contain some very sensitive information. In most situations you should structure your plan in such a way as to separate sensitive information from publicly available information. Limited copies of the sensitive material should be released, and those entrusted with these should be documented. In most cases there should be one copy of this information in secure offsite storage, and second copy with a senior corporate official such as your Chief Operating Officer or equivalent. It is highly unlikely and more than this will ever be needed.
Testing your plan can be significantly more difficult, but not impossible. The main issue here is will management support the time and effort that will be needed to test the process. There will be some planning and preparation needed to test the process, and everyone needs to be on side. You will need to develop a script and you may also want to let everyone know about the test, lest you should attract authorities under the assumption it is the real thing.

In Conclusion

The overall process of producing a Business Resumption Plan is a significant undertaking. This paper has expanded on certain critical areas which need to be dealt with during the process, but by no means is this all inclusive. Each organization will have different priorities, needs, available resources, and reasons for Business Resumption Planning. Business Resumption Planning isn't simply dealing with the computers and electronic infrastructure, but the overall process of ensuring your organization can continue to function in the event of a disaster.
During your information collection stage the breadth of this process will become

evidently clear as departments assess what they would need to have access to in order to continue to function at a minimally required level of operations.

There are many approaches to Business Resumption Planning, and in some instances it may well be valuable to contract consultants to manage the process for you. After completion your plan can be updated and managed internally. A search of the internet will provide you with many options, and a good deal of information. If you are considering hiring consultants to oversee the process ask business associates or colleagues if they have any recommendations or referrals. You should spend some time researching information available free online and get a good understanding and idea of the process and what it encompasses. You will then be better prepared to understand what a consultant can offer in relation to what you need, and you will be able to make a well informed decision and recommendation to senior management.

You will also need to do some pre planning and assessment of your own before you call in the consultants. Determine what level of recovery your firm can afford. You will be wasting money if your consultants present you with multiple plans for recovery using a hot site, buddy site, and cold site when your budget completely eliminates any prospect of having a hot site and you know using a cold site would be preferred over a buddy site. Focus them on what you need and can afford, ensuring they work inside your specifications.

Should you decide to undertake Business Resumption Planning internally there are lots of great references and guides available on the internet. There are also software packages available to assist in the initial documentation and the ongoing maintenance of your plan. But most importantly do not overlook the resources found within your organization as they will play a key role in your efforts, now and in the future.

Bibliography

1. Syong, Gan Chee. "Introduction to Business Continuity Planning" SANS Reading Room, October 1, 2001 http://rr.sans.org/recovery/continuity.php

2. Information Security Forum "The Forum's Standard of Good Practice – The Standard for Information Security" (November 2000, pg. 86) (http://www.isfsecuritystandard.com/pdf/FSOGP_2000.pdf

3. Government of Canada "Business Resumption Planning: A Guide" http://www.epc-pcc.gc.ca/publicinfo/self_help_ad/booklets/book_busi.html

4. University of Massachusetts Business Continuity and Planning Guidelines http://www.umassp.edu/policy/data/busines/append3.html

5. "MIT Business Continuity Plan", Massachusetts Institute of Technology, 1995 http://web.mit.edu/security/www/pubplan.htm

6. Government of Canada, Informatics Disaster Recovery, "Level 1 IDR Plan", last reviewed and updated June 2001. (Information related to this reference has been drawn from the unprotected areas of this document. Information specifics have been sanitized where deemed necessary)

7. National Institute of Standards and Technology "Preparing for Contingencies and Disasters" http://csrc.nist.gov/publications/nistbul/csl95-09.txt

8. Information Security Management Handbook, Volume 2, Fourth Edition, Tipton, Harold F., Krause, Micki (2001)

9. The CISSP Study Group online Discussion Board.

Appendix A[6]

EQUIPMENT DAMAGE ASSESSMENT FORM

Team: _____

R#	Equipment	Condition	Salvage	Comments
1				
2				
3				
4				
5				
6				
7				
8				
9				

Legend

Condition: OK - Undamaged; Salvage: Y/N
DBU - Damaged, but usable;
DS - Damaged, requires salvage before use;
D - Destroyed, requires reconstruction.

COMPLETED BY: _____ DATE/TIME: _____

FILE AND WORK IN PROGRESS ASSESSMENT FORM

Recovery Team: _____

R#	Files / Work (Itemize)	Condition	Salvage	Comments
1				
2				
3				
4				
5				
6				

7				
8				
9				

Legend

Condition: OK - Undamaged; Salvage: Y/N
DBU - Damaged, but usable;
DS - Damaged, requires salvage before use;
D - Destroyed, requires reconstruction.

COMPLETED BY: _____ DATE/TIME: _____

INCIDENT ACTION PLAN

This is the recommended format.

Who	What	TIME DONE	DATE DONE

Appendix B[6]

TEAM NAME	FUNCTIONAL MANDATE	TYPICAL DUTIES	MEMBERS
Executive Team	Responsible for: • management of the crisis and process.	• decision to implement the plan • confirms alternate site availability • approves damage assessment • media contact • give strategic direction • approves major equipment purchases • secures financial backing as required • approve all actions not preplanned • resolve issues of priority	• Executive Management/ Division Managers • IT Manager • DR/BRP Manager
Management Team	Responsible for: • the overall coordination of the disaster recovery implementation .	• in conjunction with Executive Team, initiate plan • manage response • strategic direction • inform and update Executive Team • Facilitate recovery team requirements • assist in decision making process with Executive team • resolve issues of priority	• DR/BRP Manager • DR/BRP Team Leaders

TEAM NAME	FUNCTIONAL MANDATE	TYPICAL DUTIES	MEMBERS

Alternate Site Team (Note: this team is typically only used in a catastrophic outage where large staff and workload relocation to an alternate site must occur)	Responsible for: • the overall coordination of the disaster recovery implementation at the alternate site.	• manage response • strategic direction • inform and update Executive • Facilitate recovery team requirements • assist in decision making process with Executive team • resolve issues of priority	• SEE LIST

TEAM NAME	FUNCTIONAL MANDATE	TYPICAL DUTIES	MEMBERS
Off-Site Storage Team	Responsible for: • management of all backup tapes off or on-site. • securing the correct tapes for transport to, and restoration at the alternate site • Establishing an alternative off-site service at the backup site	• inventory and select correct tapes • transport to the backup site • establish secure storage at the backup site • inventory all tapes at the backup site	See List
Software Team	Responsible for: • restoring the software at the alternate site	• confirm the system file backups • load the system files • load the configuration files • bring up the operating system • test the software • validate system recovery process • support service at alternate site	See List

TEAM NAME	FUNCTIONAL MANDATE	TYPICAL DUTIES	MEMBERS
Hardware Team	Responsible for: • restoring the system hardware environment at the alternate site	• conducts damage assessment • makes repair/replace recommendations • bring up the hardware system • test the hardware • hardware support service at backup site	See List
Applications Team	Responsible for: • restoring the applications individually or all together at the alternate site	• restore to as current a version as possible • work with users to verify the system • monitor processing • help restore tape backup	See List

TEAM NAME	FUNCTIONAL MANDATE	TYPICAL DUTIES	MEMBERS
Network Team	Responsible for: • Reroute and activate network communications to the alternate site	• determine requirements • install the network, including lines, modems, and all communications gear • test the network • operate the backup network • determine damage to the primary site network • order replacements	See List
Operations Team	Responsible for: • restoring an operational environment and processing the scheduled workload	• assist other teams • establish a schedule with assistance from the users • run the daily schedule • perform backups	See List

TEAM NAME	FUNCTIONAL MANDATE	TYPICAL DUTIES	MEMBERS
Salvage Team	Responsible for: • mitigating damage at the primary site. This depends on prompt realization of what is salvageable and what is not. Repair and replacement orders will be filled for what is not in operational condition.	• assist in the immediate damage assessment/ salvage operation • inventory damaged and undamaged items • salvage equipment and supplies • settle property claims • settle extra expense claims	See List
New Hardware Team	Responsible for: • ordering replacement hardware for the equipment damaged in the disaster. Hardware orders may not be a one-for-one replacement, since this may be the best time for an upgrade, consolidation, etc.	• develop a list of damaged and destroyed equipment based on input from damage assessment team • decide on new hardware • order new hardware	See List

TEAM NAME	FUNCTIONAL MANDATE	TYPICAL DUTIES	MEMBERS
Database and Security Team	Responsible for: • verifying that control mechanisms are providing data integrity regardless of the emergency. Of particular concern is the condition of the databases that are recovered on the backup computer.	• review procedures used to recover databases • recover databases • audit databases and prove they are recovered • audit data security	See List

User Liaison Team	Responsible for: • coordinating all user activities with respect to the technical recovery teams. Particularly, all priority issues will be resolved. This team will serve as a conduit for all communications to and from the technical staff	• communicate problems between technical teams • assist in establishing operations schedule • update status and progress	See List

Last Updated: October 23rd, 2017

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Seattle 2017	Seattle, WAUS	Oct 30, 2017 - Nov 04, 2017	Live Event
SANS Gulf Region 2017	Dubai, AE	Nov 04, 2017 - Nov 16, 2017	Live Event
SANS Amsterdam 2017	Amsterdam, NL	Nov 06, 2017 - Nov 11, 2017	Live Event
SANS Milan November 2017	Milan, IT	Nov 06, 2017 - Nov 11, 2017	Live Event
SANS Miami 2017	Miami, FLUS	Nov 06, 2017 - Nov 11, 2017	Live Event
SANS Paris November 2017	Paris, FR	Nov 13, 2017 - Nov 18, 2017	Live Event
Pen Test Hackfest Summit & Training 2017	Bethesda, MDUS	Nov 13, 2017 - Nov 20, 2017	Live Event
SANS Sydney 2017	Sydney, AU	Nov 13, 2017 - Nov 25, 2017	Live Event
GridEx IV 2017	Online,	Nov 15, 2017 - Nov 16, 2017	Live Event
SANS San Francisco Winter 2017	San Francisco, CAUS	Nov 27, 2017 - Dec 02, 2017	Live Event
SANS London November 2017	London, GB	Nov 27, 2017 - Dec 02, 2017	Live Event
SIEM & Tactical Analytics Summit & Training	Scottsdale, AZUS	Nov 28, 2017 - Dec 05, 2017	Live Event
SANS Khobar 2017	Khobar, SA	Dec 02, 2017 - Dec 07, 2017	Live Event
SANS Austin Winter 2017	Austin, TXUS	Dec 04, 2017 - Dec 09, 2017	Live Event
SANS Munich December 2017	Munich, DE	Dec 04, 2017 - Dec 09, 2017	Live Event
European Security Awareness Summit & Training 2017	London, GB	Dec 04, 2017 - Dec 07, 2017	Live Event
SANS Bangalore 2017	Bangalore, IN	Dec 11, 2017 - Dec 16, 2017	Live Event
SANS Frankfurt 2017	Frankfurt, DE	Dec 11, 2017 - Dec 16, 2017	Live Event
SANS Cyber Defense Initiative 2017	Washington, DCUS	Dec 12, 2017 - Dec 19, 2017	Live Event
SANS Security East 2018	New Orleans, LAUS	Jan 08, 2018 - Jan 13, 2018	Live Event
SANS SEC460: Enterprise Threat Beta	San Diego, CAUS	Jan 08, 2018 - Jan 13, 2018	Live Event
SANS Amsterdam January 2018	Amsterdam, NL	Jan 15, 2018 - Jan 20, 2018	Live Event
Northern VA Winter - Reston 2018	Reston, VAUS	Jan 15, 2018 - Jan 20, 2018	Live Event
SEC599: Defeat Advanced Adversaries	San Francisco, CAUS	Jan 15, 2018 - Jan 20, 2018	Live Event
SANS San Diego 2017	OnlineCAUS	Oct 30, 2017 - Nov 04, 2017	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced