Comprehensive Consulting Solutions, Inc. – “Business Savvy. IT Smart.”®

Disaster Recovery Planning – An Overview

White Paper

Published: March 1999 (with revisions)

An overview of the Disaster Recovery Planning Process - From Start to Finish

Contents

Preface

Disasters happen. They can be small and straightforward to deal with, or if you’re unlucky – you can be faced with a full-blown catastrophe. We can’t always avoid disaster, but through diligent planning and preparation we can minimize downtime and data loss. If your company relies on its IT systems to stay in business, then this white paper and the rest of the series on Disaster Recovery and Business Continuity Planning are a must-read for you! You can find those white papers at http://www.Comp-Soln.com/whitepapers/.

This white paper describes, at a high level, some of the many areas to address during the creation of a Disaster Recovery (DR) Plan. It is not all-inclusive, but is intended to provide insight into the overall process and our approach.

Overview

Most businesses stay very busy working on projects that support the growth of that business. Many companies do not have a Disaster Recovery Plan (DRP). Often there is a desire for a DRP, but the level of effort and/or cost required to create a DRP can cause this project to have a low priority relative to other more immediate projects. A DRP is viewed as "nice to have" or "just insurance that will not be used", and not as a critical business component.

That is, until there is a failure that causes a significant outage or loss of data (often at a significant cost to the business). It is our opinion that every company could benefit from both a Disaster Recovery Plan and a Business Continuity Plan (BCP). Companies purchase insurance to protect their business. Investing in a DRP and BCP is just as important for most businesses in our opinion.

Are you able to quantify the cost of downtime for mission critical systems? Does this figure include lost sales and/or lost customers? Does it include the cost of wages for people unable to perform their primary job function while the system is down, as well as the amount of time required to get caught up once the system is available? Once a company quantifies the cost of unscheduled downtime the business case justification for a DRP usually becomes easy.

So, now that you have decided to go forward with this type of project, what next? Where do you start? What needs to be addressed? How will you know that the plan *really works*? Do you need to find external expertise for this type of project? If so, exactly what type of expertise is required?

Before we go any further it is important to mention a few things. A DRP first needs to be created, then tested and refined, and finally implemented and tested on a periodic basis. While this can be an expensive and time-consuming effort, it can prove to be a bargain in the long run if some type of disaster occurs. Most plans will experience some type of failure during their first execution so it is very important to test the plan. Systems and personnel change, so it is also important to retest the plan on a periodic basis, ideally rotating staff.

Using experienced Consultants to help develop the process and then later audit and refine the process is usually idea sound investment. They will often identify gaps or ambiguities that might have been missed by someone who has more familiarity with the systems, processes, and procedures in use. It is also important to find a team that will build plans based on how your business and systems work, and not try to make your business fit into a predefined template. Every business is different, and every system being recovered has its own nuances. Being able to capture that knowledge is critical to success.

It’s not just Computer Systems!

It is also important to have a Business Continuity Plan. A BCP should address infrastructure related items that are often taken for granted. For example, where will people sit to do their job if there is a catastrophe? Where will mail be delivered? How will your customers find you? What type of workstation and software will be required? Are there phones, voice mail and e-mail? How will the outside world reach you? How will your site communicate with remote groups? Are there any special requirements required for day-to-day operations (e.g., websites, specialized machinery, secure remote access, broadband, etc.)? If this is a multi-site location, what is the plan if more than one site has a failure at the same time? These are all very important issues that need to be addressed for a ***comprehensive*** Disaster Recovery Plan. Please see our white paper on this subject for more information.

Another related topic is Emergency Management and Communication. This deals with issues such as physical security of site, medical care, and coordination with Government Emergency Management teams, and communication with your management team, employees and vendors.

Typical Approaches to Disaster Recovery

Once a company recognizes the value of Disaster Recovery, the next question is generally “how do we do it?” They may try it themselves at a remote facility with redundant equipment (a “hot site”). They may secure the services of a DR facilities and services provider (generally a multi-year agreement that often starts at a cost of $250,000+ per year). Or, if they are very lucky and have computer facilities located in several geographic areas, they may try to implement some type of SAN (storage area network) or data replication mechanism. That is often the most expensive solution, but also can provide the fastest recovery time (shortest recovery time objective, or RTO) with the least amount of data loss (recovery point objective, or RPO), resulting in the lowest overall system recovery objective (SRO – or the point where the “systems” are ready to do real work).

When using a DR Facilities provider there are many issues to consider. It is likely that the equipment provided for recovery during a test or an actual disaster is not identical to the equipment used in production. There may be availability issues if the company has many customers in a single geographic area. There may be phone and network bandwidth issues if more than one customer declares a disaster at a single time. Does the company have multiple hot sites that you can use? Where are they located? How long would it take to assemble a recovery team at each site? (This affects the RTO) How often can you test the plan (twice a year is ideal), and how long will you have to test the plan (24-72 hours is typical)? What is ***their*** DR plan? How committed are they to your success? (Tip: a good contract will address service level agreements (SLAs), preparation before your team arrives, and the level of assistance your team will have recovering systems).

Where do you start?

The first step is to create a DR team. This includes an executive sponsor, a DR Coordinator, Team Leads (there will be several groups and possibly sub-groups), and team members. People should be designated as either primary or backup for a position, with every position (with the possible exception of the Executive Sponsor) having more than one person assigned. This is to minimize people as a "single point of failure." The goal is to have representatives from each business or technical area that have the expertise to help develop the various recovery procedures, and are committed to the success of the overall effort.

The next step is to define business goals. The goals should address items such as what functional areas need to be recovered (lines of business, locations, functionality, etc.), what length of time is acceptable for recovery, and what amount of data loss is acceptable (some data loss is almost inevitable unless you are very lucky or are using a SAN / real-time replication to a remote site). This often involves prioritization and a cost-benefit analysis (often initially based on assumptions, not fact) to determine the worth of recovery – something that may be premature at this phase of the project.

Understand the Business Goals and Objectives

You know what is expected (i.e., the scope of this effort); now find out what that really entails. What are the critical systems? What are the key processes and applications? What are the dependencies on other systems? This includes data transfers, manual processes, and remote processing. Document these processes, their interaction with and dependencies on other systems and user interfaces, and the sensitivity of the data (time sensitive and confidential information are two examples).

Once the systems have been identified, attempt to quantify their impact relative to the overall business goals. This will help be essential with the prioritization efforts for system recovery. If there are good estimates on the cost of downtime, this information can be used to complete an accurate cost – benefit analysis as well.

Identify Specific Requirements

Are there any specific business or legal requirements? This could include adherence to standards such as ISO 17799 and/or NFPA 1600, or regulations such as HIPAA, Gramm-Leach-Bliley Act, Sarbanes-Oxley Act, etc. It is very helpful to know this information up-front in able to ensure compliance on an ongoing basis. Please see or compliance white paper for more information in this area.

It is important that issues such as these be defined in the overall scope of the effort. Everyone involved with this effort (including Upper Management within a company) needs to have a single vision of "what success looks like." Without this you risk wasting time and money on a plan that may be viewed as a failure.

Identify Key Personnel

These people may not be part of the DR Team, but are important. For example, who has the authority to declare a disaster? That information should be well known, and contact information for those people should be readily available. This list should be maintained both by name and by role. It should be validated and updated frequently.

Identify Single Points of Failure

The overall goal of this step is to mitigate unnecessary risk. The scope of this effort includes people, software, equipment, and infrastructure. It is important to look at the "big picture", which includes:

- impact of the failure
- probability of failure
- estimated incidents (failures) per year
- annualized loss expectancy
- cost of mitigation

Preparing to Develop the DRP

You know what needs to be accomplished – in detail. You are preparing a project plan to develop the Disaster Recovery Plan. Now is the time to step back and make a sanity check. Have you really addressed everything? This is especially difficult to know if this is your first DRP. The following contains tips on what critical functional and technical areas to address for a comprehensive DRP.

Are you ready to begin yet? It is important to have a document management system in place to track versions of plans, work in progress, and work that is scheduled but not started (e.g., detailed specifications for a specific task). This information needs to be backed-up and saved in a format that does not rely on the underlying systems being recovered (for obvious reasons). We have used secure e-rooms that are hosted by an external vendor for some of our projects. We also recommend that the plans be archived on portable media such as DVD, with copies kept with key people and at various "safe" locations.

This information is too valuable to be without, and it also too valuable to let out to unauthorized resources. The issues of availability and confidentiality are important to consider when defining the document management plan. It is also important to provided updated copies of the documentation at a periodic basis (usually quarterly or semi-annually).

The DRP should address 3 main functional areas

1. Recovery: Once the infrastructure is in place it will be necessary to recover production data. Since recovery may not be up to the point of failure, it is important to identify any processing that needs to be redone. Can all of the data feeds to the system be identified? How many of them can be redone with 100% certainty of success? It is important to minimize "holes" in data (especially in a distributed processing environment where one step could be dependent on one or more predecessor steps or actions), and then to identify the action to be taken when data inconsistencies are detected. There should be an audit trail for all work performed during this phase. Once the data is recovered there should be some type of validation process (discussed in more detail below) to ensure that the recovery was complete, leaving a consistent work environment.

2. Restoring / Sustaining Business Operations: Critical business processing (which may not encompass all application systems) will need to be supported. All processing requirements and service level agreements need to be defined and documented. Dependencies between processes also need to be defined. It is important to document the existing process and then build the plan accordingly. Anything that ran before (in production) will probably need to run again (at the hot site), so scheduling and dependency information is critical. Remember that routine maintenance (including backups) should still be performed at the hot site (it too is an asset that requires protection).

3. Transferring Data back to Production Machines: This is one area that is generally omitted from a DRP, but we feel that it is very important. Eventually production will need to shift from a "hot site" back to a permanent location. A process needs to be defined to manage this migration. Often the Client will elect to execute the DRP on the production machines in order to synchronize the machines to a specific point in time. It should also be noted that this is one of the more difficult tasks to test.

The DRP should address 3 main technical areas

1. Hardware Issues: This includes machine type (especially an issue when using equipment that is older or not as popular), configuration (disk capacity, peripheral devices, device names, RAM, file systems and volume groups, OS users, etc.) and operating system version and patch level (hopefully it is a current version in case vendor support is required). Another issue is deciding whether to use an existing pre-configured machine or to completely configure a machine (load the OS, initialize and configure disks, TCP/IP configuration, SCSI addresses, everything). There are pros and cons to each scenario. Our recommendation is to plan for the worst case (i.e., the complete rebuild). Note: It may be possible to reconstruct the production machine on a new machine using a tape backup. This method does not leave much room for flexibility relative to hardware configuration, but is very fast when compared to a manual system reconstruction.

The key to success is to ensure that DRP machines have at least as much capacity as the production machines that they are replacing, that they are compatible architectures, and that "someone" has the installation media for the OS load. These machines usually either reside at a remote location (in which case they can be pre-configured) or are provided as-needed by a company that specializes in providing facilities and equipment.

2. <u>Networking Issues:</u> What part of the production system must be replicated for the DRP? This environment most likely consists of several machines, and there is a good chance that the environment is not homogenous. Is any special type of LAN or VPN software required? How do the machines communicate with one another? (Probably TCP/IP) Do applications connect to machines using hostnames (which is preferable) or hard-coded IP Addresses? What other configuration information is required? Are there requirements for connections to an external network (WAN, Internet, Extranet)? Are there requirements for dial-in access? Is there any other type of Client/Server or *n-tier* activity that will need to be supported? All networking requirements and issues need to be identified, documented, and then addressed in the DRP. What about bandwidth?

3. <u>Software Issues:</u> This is a very broad area that encompasses many things. Software includes the Operating System, user written applications, and third party software (RDBMS, report writers, GUI products, backup/recovery products, scheduling software, etc.). A comprehensive inventory of currently used software, including current version, license information, and support contact information is essential. <u>This is what runs your business. Working hardware and an accessible network is worthless if your critical applications are not working!</u>

   Whenever possible it is preferable to be using current versions of the products in production (for improved product support). It is also desirable to have the installation media, installation guide/notes, licensing information, support information, and current configuration information available for these products (all of which is critical for rebuilding the installation). Regarding custom applications, it is desirable to have the source code, libraries, and "make" files in addition to the executable code. There is always the chance that the application will need to be recompiled due to version incompatibilities, bad executables, path changes, etc.

Creating the Procedures that Support the Plan

<u>When the DRP is created it should not assume anything!</u> There should be an *excruciating* amount of detail for each recovery procedure, including instructions listing each and every command to be executed. Nothing should be assumed or left to chance. It should anticipate problems and provide a structured means of troubleshooting. Design the procedures with the goal of a semi-experienced person who may not be familiar with your operations executing the procedure.

Execution of the plan will be stressful and people may forget simple, everyday things. Also, resources/staffing may change and the people assigned to execute the DRP may not be familiar with it. The use of checklists is very desirable. These lists should have sections for a timestamp, initials of the person doing the work, and room for comments. This information will be critical if a problem is found downstream. A single person should be identified as a DR Coordinator, with a backup person identified to fill-in if necessary. That person will be responsible for monitoring each phase of the DRP, coordinating with the various groups involved with executing the DRP, and providing status information to the "outside world" during DRP execution. Resources should be identified as being responsible for each and every task and procedure, and they should know exactly what is expected of them. Again, nothing should be left to chance!

Detailed test plans should be developed prior to execution and should address all critical functional areas of the DRP. Data should be gathered during testing (e.g., reports, screen prints, transaction logs, etc.) and saved for future review. In the event of problems that data may help the team make a root cause determination regarding the problem so that it can be corrected. If everything goes right it provides the necessary documentation to support an external validation effort of the DRP exercise. The only way to really know if "everything worked" is to know what "everything" is, and then to be able to demonstrate that the necessary tasks were completed successfully!

Testing and Refining the Plan

The final issue with executing the DRP is to determine if the test is designed to validate the process, or if it is to simulate a true disaster. While it may seem that the two issues are the same, they really are not. For example, assume that the target "disaster date" is Friday July 21st, 2006. If there were some unforeseen problem with the backups (e.g., bad media), there would be two options available. The first option would be to use backups from an alternative test date (for example, Friday July 7th, 2006). This option would be used to *test the process.* The second option would be to recover from the next most recent backup (probably Thursday July 20th in this example) and then redo the work up to the point of failure (i.e., the original target date). This option more closely simulates a true disaster, and is more consistent with the stated RPO. There are pros and cons to each of these options. The determining factor is usually available time and/or cost. The first option generally identifies correctable deficiencies in the process. The second option is generally much more expensive and time consuming but most closely simulates a true disaster. Therefore, the ultimate goal should be to simulate recovery after an actual disaster.

A common problem that we see is that plans are developed, but they are never tested, or are tested once and forgotten. A plan that is not continuously refined and validated is almost worthless. In order to maximize the chance for success in the event of a real disaster it is essential that the DRP be executed on a regular basis (semi-annually is recommended). Specific recovery procedures can generally be tested in-house on a more frequent basis. Staff should be rotated as much as possible, thus providing a more comprehensive test of the process and the plan, and providing trained resources in the event that they are ever needed.

A Project Management Approach

The practice of professional project management can really help drive the Disaster Recovery Planning effort. Someone with experience and proven expertise (such as a PMI certified Project Management Professional, or PMP) who understands how to decompose a complex process into manageable components and coordinate activity is invaluable. Has all work been accounted for? Are the right people working on the right pieces at the right time? Are there dependencies between tasks? Is Risk being managed? Is there effective communication and documentation? Again, this is a best practice for any large effort, especially one as critical as Disaster Recovery or Business Continuity.

This also creates an opportunity for Independent Validation & Verification, a process that utilizes outside expertise to validate that the planning and efforts are complete and will deliver the desired results. Expertise from various areas is usually leveraged to not only look at what is being done, but also how it is being done. This can save time and money if problems are identified early, and will provide an additional level of comfort for Management.

A good Project Manager will also document important events, such as detailed meeting minutes that include information about issues, positions and opinions, decisions made, etc. This type of supporting and historical information can prove invaluable when recovering from a disaster, especially if key members of the team are no longer available to provide their insight and knowledge.

Summary

It is important to define the true purpose of the DRP & BCP, define the specific requirements (as opposed to goals) and what constitutes success during execution (many sites consider anything less than 100% restoration and continuation to be a failure), and then develop a plan that addresses all of those requirements.

We create a “Critical Success Factors” spreadsheet that is weighted by the criticality of the system, utilizes dependencies to factor-in the downstream impact of a failure, and creates a “score” based on the recovery. This is a tangible way to track progress and identify key deficiencies in the overall Disaster Recovery Plan.

Remember, the DRP is a "living" document that is refined over several iterations and updated over time. No matter how good it is it probably will fail during the first execution. The key is to continue to improve the plan so that it will work if and when it is ever needed. Please see our other white papers on Disaster Recovery at http://www.comp-soln.com/whitepapers.

Click here to view a slide presentation on this topic from a conference presentation.

About the Author

Chip Nickolett, MBA, PMP is the President of Comprehensive Solutions. His first disaster recovery project was in 1994 for a large insurance company, and he has been actively engaged in disaster recovery projects since then, establishing a BC/DR practice area within Comprehensive Solutions. For more information please see http://www.Comp-Soln.com/chipn.html.

Let Us Help You Succeed!

Call today to discuss ways that Comprehensive Solutions can help your organization save money and achieve better results with your IT projects. We provide the ***confidence*** that you want and deliver the ***results*** that you need.

View our "Disaster Recovery" Brochure

Back to White Papers
Back to Services

Comprehensive Solutions
4040 N. Calhoun Road
Suite 105
Brookfield, WI 53005
U.S.A.

Phone: (262) 544-9954
Fax: (262) 544-1236

This document is provided for informational purposes only, and the information herein is subject to change without notice. Please report any errors herein to Comprehensive Consulting Solutions. Comprehensive Consulting Solutions, Inc. does not provide any warranties covering and specifically disclaims any liability in connection with this document.