

WHAT IS DISASTER RECOVERY

The definition of 'Disaster Recovery' tends to vary widely from company to company and is a difficult term to define because it changes and is so varied in each situation. And in fact its use and definition should change, vary and adjust for each situation, each company's business needs and applications, as well as each point in time. Although 'Disaster Recovery' is often viewed as a function of the IT (Information Technology) arena, it really has its roots in the Business needs of the company that is applying it for the intended purpose of ensuring that the Business functions can continue and the livelihood, continuation and survivability of the company remains intact.

Disaster Recovery is not just an ability to restore the IT functions after some unfortunate incident. Although that may be the ultimate goal that we technologists hope we will never have to activate, Disaster Recovery is actually a continuous process of analyzing the business needs and planning the technology needed to restore business functions. Disaster Recovery also includes the continuous improvement, refinement, and expansion of the capabilities to react to unforeseen, unknown and unexpected situations.

To continue this discussion we will establish some very high level distinctions regarding a few basic terms. For this document we will assume;

Disaster Recovery is the processes, plan, technology, etc. needed to recover from an unforeseen incident at a Data Center. Business Resumption is the processes, plan, technology, etc. needed to recover from an unforeseen incident at a Business User's location, i.e. work area, Call Center, etc.

Business Continuity is the overall philosophy including Disaster Recovery, Business Resumption, Carrier redundancy, workload balancing, personnel training, emergency acquisitions, etc.

We will also assume that a 'Disaster' can be caused by a very wide variety of incidents and situations ranging from the traditional fire/flood/tornado that can/may destroy a building and its contents to more subtle incidents where the building and contents are intact but the authorities will not allow personnel into the building or area. Causes of a Disaster can also include events that we can not foresee, plan for, or even expect in some cases and might include civil issues, political upheaval, national or regional health, or terrorist actions.

Although the balance of this paper may appear to be oriented towards the technology, it is due to the target audience and should not be viewed as a departure from the theme that Disaster Recovery needs to be driven by the Business in the direction that the Business needs dictate.

Business Impact Analysis

Before anybody, Business or Technology, can start to develop a Recovery Plan they need to know what functions need to be recovered, how quickly, how much (capacity), and why. A Business Impact Analysis (BIA), including a Risk Analysis,

needs to be performed to investigate the potential impacts and determine what compensating actions should be taken. This step is primarily done within the Business unit but with the IT organizations involvement and assistance.

Most Business units do not have a good understanding of the impacts on themselves should a significant outage occur. Understanding these impacts on the Business and their significance is the first step in deciding what actions need to be planned. The impacts of an outage will vary from company to company and even between departments within a given company. Some companies or departments may suffer substantial losses or be at risk immediately with an outage of their IT systems. An organization that transfers large sums of money in near real-time or with information that is time critical to people's health or safety are examples. These businesses most likely have a greater need for recovery in a timely manner than does an accounts payable area where your vendors would understand and tolerate receiving a payment a few days late, or a records archival department that could perform their function next week or next month with little or no impact to the overall business.

Once a Business or department has analyzed their functions, processes, and criticality to continuation, then they need to assess the cost impacts and risks of suffering through an extended outage. Again, transferring large sums of money may be very costly to a company that can not do so for an extended period or not being able to provide health or safety information may have a high degree of risk and even legal exposure. On the other hand, not being able to achieve last month's records to optical disk for long term storage may not have a significant cost impact for a long period.

With the cost impacts and risks in hand the Business can then move forward with identifying how long they can be without a system before significant impacts start to mount. This may be almost immediately in some situations and a substantial time in other situations. Additionally they will need to review their needs to recover as of a point in time compared to the failure. In other words, when the system is recovered does it need to be restored to the point in time of the failure or can they recover back to the prior day or weekend and then manually recreate any updates up to the point of failure. This information will allow the Business to start making logical decisions regarding what systems need to be recoverable in what timeframes, at what point in time compared to the outage they need to be recovered to, and what monies they are willing to spend to do so.

Facilities

Decisions on facilities, or location, to recover to will vary depending on the BIA, the company, locations of their Data Center and Business Unit, and many other factors. General guidelines are that the Recovery location should be at least 5-15 miles away from the main Production facility to prevent or at least reduce the chances of losing both facilities in a common incident such as fire, tornado, etc. Many organizations extend this distance to further reduce the risk and to take into account other situations such as hurricane, wide spread power outages, civil or terrorist actions, etc. Increasing the

distance generally helps to reduce risk, but also tends to increase ongoing costs associated with travel for testing, network connectivity, etc.

The facility chosen and its associated features and capabilities will vary substantially from company to company. One approach is to obtain use of a fully functional site already populated with all the needed equipment, software, connectivity, etc. This approach is often referred to as a 'hot site'. Although generally more expensive this approach does allow for a faster recovery, thorough testing abilities, and is often obtained from companies that specialize in Disaster Recovery/Business Continuity. This approach also lends itself to data redundancy on the local system at the 'hot site' as discussed below. Depending on the needed recovery timeframe a 'cold-site' approach may also be considered where a shell location (computer room with environmental already in place) is obtained with the plan to obtain the necessary equipment and software at the time of the failure. Although less costly this approach is normally only used for Businesses that can endure a fairly long period until their systems are restored and are willing to risk not being able to test their plan periodically. Some organizations take an approach that is a combination of these two examples by subscribing to a fully functional location that they can have immediate use of for a limited period of time and another nearby 'cold-site' that they can then populate and eventually move into.

Other factors that need to be considered in selecting a facility include its availability should you need to use it. Many firms have multiple subscribers to their facilities which raises the concern of a single disaster causing multiple customers to need the use of a common facility at the same time. General capabilities, growth capacity, network connectivity (discussed below), location, ease of access, travel, anonymity, security, surrounding support facilities and many other items that may be unique to a particular Business also need to be considered in the location selection process.

Hardware/Software

The type of hardware and software needed at a Recovery site will be determined by the standards normally used within a particular company to reduce costs, complexity, ensure common file formats and support, testing ability, etc. The quantity or capacity needed at the Recovery site will be determined by the BIA and identifying what systems and capacities are needed in a recovery situation. Most organizations will replicate their Production Environments as closely as possible although they may use smaller hardware platforms if less capacity is needed.

Monitoring of the environment needs to be almost continuous as any change in the Production Environment needs to be reviewed and may require changes at the Recovery site. This process needs to include general growth/capacity increases, Business changes, both hardware and software upgrades, Application enhancements, and even general procedural changes. Most organizations realize the importance of this monitoring and will adjust their Change Management processes to include a review of their D.R. environment.

Communications

Communication connectivity for a Recovery site can be the most challenging and expensive portion of a Recovery Plan depending on the extent and complexity of the network as decided in the BIA. Some organizations will need to support the immediate needs of numerous large and/or international locations with large bandwidth, while others will find a small, simple network adequate for their limited needs during a Recovery situation. The Network connectivity to the Recovery site needs to be designed in such a manner as to;

- Provide Business connectivity and capacity in the timeframe needed after a Disaster
- Minimize ongoing expense, complexity, support needs
- Minimize impacts on the normal Production Network
- Be monitorable and able to support periodic testing

Most organizations also take this opportunity to review the potential issues that could surface with their carriers in the Network (outside the Data Center or Business location). Many companies do not realize how dependent their Business is on the Carriers and such items as reliance on a single Central Office (CO), a single Carrier, or even a single entrance cable to the customer's location. In general Carriers incorporate a high degree of redundancy into their networks, CO's, back-up systems, strong infrastructure, security, etc. But no amount of planning can provide total assurance that there will never be a major failure, particularly in situations where the key components traverse long distances in various physical forms through various environments and political settings.

Data Recovery Methodology

Data Recovery methodologies vary widely from company to company, business to business, and should be determined primarily on the results of the BIA. The needs of the Business regarding how quickly they need to recover after a disaster and as of what point in time will determine greatly what methodologies can be used to capture data and subsequently restore it to a Recovery system.

If the Business need is to recover almost immediately after a disaster and to recover as of the point in time of the disaster, then a methodology of duplicate and/or synchronized databases between sites may be employed. This approach maintains current and up to date information at the recovery site and can be supported with redundant systems that can take over the processing virtually immediately. Obviously the significant costs and complexities will be a major decision factor in using this approach as it has impacts on hardware, software, communication needs, support complexity, as well as affecting how the normal Production environment operates. A

factor to consider in this approach that is often overlooked is that any database integrity issues or concerns caused by viruses will also be replicated almost immediately.

Many organizations will find the BIA indicates their recovery needs to be within 24-48 hours of a disaster and the database can be restored as of the night before the disaster. This need can be more easily met with methodologies such as nightly back-ups that are taken off-site for storage, movement of these back-ups to the Recovery site when needed and restoring the database onto awaiting equipment. Although this methodology is less complex and costly than synchronized databases, it does require the Business have some way to re-apply activity from the time of the last back-up to the time of the disaster. Approaches to this range from simple retention of source documents (paper) for a period of time to off-site replication of log files which is still fairly simple compared to duplicating and synchronizing an entire database.

Variations of these approaches may include SANs or remote tape technologies that can provide database copies ranging from real-time to previous night back-ups.

Business Resumption

As mentioned before, Business Resumption for this discussion is defined as the ability to recover from a significant event at the Business User location. This normally entails recovery to another location where the Business User can have access to space with desktop PC's, phones, and connectivity to both their customer and their IT systems/data. Additional non-IT business related tools (business machines, scales, etc.) also need to be considered by the Business in many instances.

Business locations ranging from Branch Offices, Contact Centers to Corporate Headquarters are also likely to experience disaster type situations that significantly impair or prevent them from continuing their normal business. Although these locations may not be viewed by some with the same significance as the Corporate Data Center, they still use some similar technologies these days and are still a vital link in the overall flow of information and handling of customers and business functions.

Most business areas depend heavily on technology that needs to be replicated and available for the continuation of these functions. This includes PC's, Servers, LAN, phones, PBX, and connectivity to data and voice Networks and Carriers. As with Data Centers, some companies specialize in and can be engaged to provide these services, or an organization may be able to provide their own internal capacity in the form of other remote locations, Training areas, etc.

Ongoing

Any organization that commits the time, resources and money to analyzing their business needs and developing a Business Continuity plan will also need to continue that commitment going forward to maintain the plan and ensure that it is still executable.

Business Continuity is not an experience that you can go through once, place it on the shelf and expect it to be viable without ongoing attention and commitment.

Ongoing support and activities need to include;

- Periodic testing - Needs to be conducted to ensure proper operation, completeness of planning, training of staff and to turn up shortcomings and changes. Testing should be conducted at least every 6 months with variations between partial and full tests, planned and unannounced tests.

- Personal training – Unfortunately a disaster may remove some, many, or most of the key personnel along with the IT or Business capability. Broadening the B.C. experience base across personnel is critical along with documenting processes in such a thorough and simplistic manner that even an outsider could follow and execute the procedures.

- Changes – Business functions and IT systems seldom remain static for very long. New systems are always being added, capacities, business needs, legal requirements, etc. continue to change. All changes in IT Production environments need to be reviewed for impacts to the Recovery environment and all Business function/process changes need to be reviewed with an eye towards changed requirements to the BIA.

Authored by Ralph Acito