



Leading Edge Technology Q4 2011

Top 10 Tips for Disaster Recovery Planning

Essentially, the key to Disaster Recovery success is having a realistic and well understood set of objectives that are based on the business needs. This involves planning and preparation, from the business impact analysis, to understanding and quantifying risks, to classifying and prioritising applications and data for recoverability.

Additionally, there is the need for preparing systems to be able to recover, and then documenting everything, especially the Disaster Recovery plan. Another factor for success is to make Disaster Recovery less than an exception by integrating Disaster Recovery hardware components into production. The dynamic nature of IT requires continuous review and updates of the process and the plan. It must be part of the day-to-day operations.

Finally, investing in a solid technology basis is critical. An organisation must leverage newer technologies that provide higher performance at lower cost where possible, and at a minimum it must ensure that data backups are functioning well and kept offsite.

1. *Business and IT need to be linked*

Creating a Disaster Recovery plan is a compromise and while people are aware of best practices, they face issues related to cost. When best practices are pitted against cost, cost needs to be the second and not first priority. Even more important though, is that capabilities need to be matched to expectations. Responding to a disaster is an exception, but preparing for it should not be a burden but integrated with day-to-day priorities.

2. *There needs to be a Disaster Recovery plan*

The Disaster Recovery plan needs to represent all functional areas within IT prior to, during, and after a disaster. It needs to include applications, networks, servers & storage.

Contingencies, such as "what-if" scenarios should be considered as part of planning process. Decisions need to be made regarding levels of disruption that will constitute a disaster, downtime and loss tolerances.

3. *Keep the Disaster Recovery Plan current*

Disaster Recovery planning needs to be part of the day-to-day operations of the IT environment and even though it is an exception, it should always be at the forefront of



Leading Edge Technology Q4 2011

people's minds. Once the Disaster Recovery plan is created, it needs to be maintained and updated every time an element within the IT environment changes. The dynamic nature of IT environment ensures that the Disaster Recovery plan will fail if the management of the plan is not part of change management.

4. ***Test the Disaster Recovery Plan***

The Disaster Recovery plan needs to be tested regularly to ensure the business can recover the operation successfully and in a timely fashion. Disaster Recovery testing is a major challenge for most IT departments, but if recovery has not been tested all the way to the application level, it is very likely that problems will occur.

Even though a Disaster Recovery test is a major operational disruption it shouldn't be treated as a pro forma exercise but needs to include true end-to-end testing all the way to production. The focus needs to be on recovering applications rather than servers since with today's complex applications, client server and web-based multi-tier applications, the components reside on multiple servers thus there are interdependencies between these. If disaster recovery has not been tested all the way to the application level, it is very likely that problems will occur.

The philosophy for Disaster Recovery testing needs to change. Basically the approach used for software quality testing should be adopted, where finding bugs is a positive thing. Finding problems in Disaster Recovery is equally positive as long as these issues are resolved to eliminate problems during a real disaster.

5. ***Set realistic recovery objectives***

Frequently, organisations have established objectives and prioritised servers and applications in accordance with Disaster Recovery policies. However, upon an objective examination of Disaster Recovery capabilities and resources, it turns out that these goals are not attainable. Thus it is important to set realistic Recovery Point Objectives (RPO) and Recovery Time Objectives (RTO).

In regards to the RPO when does the clock start ticking and what tolerance is permissible for an outage. As for the RTO how current is the data prior to the disaster. These are the key matrix items that need to be determined and supported. It is important to examine whether the infrastructure can support the goals.



Leading Edge Technology Q4 2011

6. ***Disaster Recovery Responsibilities***

Disaster Recovery roles and responsibilities need to be clearly defined. In the case of a disaster, who will be there to recover the data and initiate the Disaster Recovery plan? With disasters like Sep 11, there was a clear demonstration of the risk of staff not being available to perform recovery. Even in situations where tragedy is not the issue, it might simply be a case of not being able to physically reach Disaster Recovery sites. Any Disaster Recovery planning scenario must consider redundancy of roles to ensure that people are available to cover various responsibilities in the process.

This highlights the need for comprehensive documentation and training. Large organisations with distributed IT expertise are in the best shape as far as this is concerned, because they can leverage resources in multiple locations. There is also the possibility of contracting and enlisting third-party service companies to help in the planning and preparation process.

Disaster recovery requires organisation, coordination, and execution. Perhaps the best profile for a Disaster Recovery Manager is that of a military commander. Executing a Disaster Recovery plan is analogous to a military operation. It requires that each participant understands his or her job, who they have to interact with and, most importantly, the proper chain of command. As in these circumstances, chaos is a given, being able to react to new and changing circumstances quickly and confidently is key.

Some of the factors that need to be considered are how and when a disaster is declared, time to notify and position people at Disaster Recovery sites, equipment logistics, recovery initiation, and the overall execution process for recovery.

7. ***Disaster Recovery Risk***

The Disaster Recovery plan needs to address the right risks. Disaster recovery is essentially an insurance policy. How much and what kind of insurance is needed? What sort of risks is the organisation willing to take? The definition of what constitutes a disaster that is covered by the plan has to be considered. Many recent disasters were floods but various kinds of other weather activity and fires need to be considered as well. There are elements within the organisation's environment that need to be considered from the standpoint of what constitutes a disaster. A site outage, application outage, or even a server outage could constitute a disaster for an organisation.

8. ***Good Backups***



Leading Edge Technology Q4 2011

What happens when the backups don't work? For many companies tape backup is still the primary medium for disaster recovery, certainly for off-site disaster recovery. As an alternative, replication across a WAN is growing, but it might be too costly an option for some businesses. Application recoverability must be validated through the recovery of backups to the application level.

9. *Alternative Recovery Services*

It needs to be clearly defined who - in the case of a disaster - will be there to recover operations and initiate the Disaster Recovery plan. While this is an uncomfortable consideration it needs to be considered nonetheless. Disasters like September 11 clearly highlighted the risk of staff not being available to perform recovery. Some of the organisations affected had a backup copy of their data offsite, however it was only a short distance away from the World Trade Centre site and staff couldn't access the site for weeks caused by the exclusion zone set up around Ground Zero. Even in situations where tragedy is not the issue, it might simply be a case of not being able to physically reach Disaster Recovery sites.

10. *Disaster Recovery Cost Consideration*

Data protection and recovery requirements may seem too expensive and Disaster Recovery is considered a particularly heavy expense, one that most organisations have a great deal of difficulty absorbing. It returns to the gap between the ideal and the practical. Being able to address the IT cost for Disaster Recovery is an issue of integrating Disaster Recovery into standard operations as much as possible. Ideally, the Disaster Recovery resources and equipment are not viewed as technologies that are sitting idle. Ultimately, this comes down to making an informed decision of either spending money or accepting risk. Newer technologies are emerging that make this more cost effective. Regardless, Disaster Recovery needs to be treated as an investment. It is an insurance policy.



Leading Edge Technology Q4 2011

For further information on any of our content, contact Leading Edge Technology.

08456 44 79 49

www.leadingedge.uk.net