An *IT Briefing* produced by SearchStorage.com

10 Reasons Why Your Disaster Recovery Plan May Fail

10 Reasons Why Your Disaster Recovery Plan May Fail

By James Damoulakis

BIO

James Damoulakis is CTO at GlassHouse Technologies. He brings 20 years of experience in systems, storage, backup/recovery, and DR, with a strong focus on architecting and implementing highly available enterprise storage solutions. He has spoken on storage issues in a number of venues and is a frequent contributor to key industry publications like *Storage Magazine*. Before joining GlassHouse, Mr. Damoulakis was Director of Implementation Services at CNT/Articulent in Hopkinton, MA, where he managed a team of senior technical consultants focused on SAN design and implementation, enterprise storage management, backup/recovery, and high availability. Previously, he was Director of Technical Services at Invincible Technologies Corporation, where he was responsible for technical support and professional services around ITC's highly available, networked, and attached storage products. He has also held a variety of management and technical positions with Digital Equipment Corporation, FTP Software, NEC Technologies, and Apple Computer. Mr. Damoulakis holds a Bachelors degree from Boston University and a Masters Degree from Northwestern University. He received his MBA from Northeastern University.

This *IT Briefing* is based on an XOsoft/TechTarget Webcast, "10 Reasons Why Your Disaster Recovery Plan May Fail." To view this Webcast online, please click the link.

This TechTarget *IT Briefing* covers the following topics:

About TechTarget *IT Briefings*

TechTarget *IT Briefings* provide the pertinent information that senior-level IT executives and managers need to make educated purchasing decisions. Originating from our industry-leading Vendor Connection and Expert Webcasts, TechTarget-produced *IT Briefings* turn Webcasts into easy-to-follow technical briefs, similar to white papers.

For inquiries and additional information, contact:
Dennis Shiao
Director of Product Management, Webcasts
dshiao@techtarget.com

10 Reasons Why Your Disaster Recovery Plan May Fail

Executive Introduction

This document contains a 10-item list to use as a guide when developing or evaluating a disaster recovery (DR) plan. Each item provides a helpful hint in formulating or fine-tuning a DR Plan. The list of 10 items is somewhat arbitrary, in that it is not prioritized, not necessarily sequential, and the level of effort for resolving or achieving each goal varies. However, the overall goal is to identify some topics for an honest assessment of DR capability. Making even small changes in a number of these areas would improve DR capability significantly.

1. Business and IT Are Not Linked

Whenever tragedy strikes, the importance of disaster recovery is underscored. With 9/11 and recent events in the Gulf, the challenges of DR are being more greatly emphasized.

Ideal Vision

Ideally, DR would include elements as if money were no object. Being prepared to handle all categories of disaster requires having clearly documented policies and procedures, well-understood roles, responsibilities, goals, and priorities that tie together business goals with IT capabilities. Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) must be clearly defined and understood. The list of the relevant applications and supporting servers that would need to be recovered in an affected environment would be carefully prioritized and classified and there would be tools to allow quick recovery in an automated fashion. In a perfect DR plan, there would be documentation regarding who, what, why, and how the plan will be accomplished; these elements are understood and capable of being executed. Unfortunately, the reality of DR plans is somewhat different.

Creating a DR plan is a compromise. People are aware of best practices, but face issues related to cost. When best practices are pitted against cost, cost usually wins. Even more serious, though, is capabilities versus expectations. What is it that people think IT is capable of delivering versus what IT can actually deliver? This is one of the biggest challenges. DR requires performing activities that are rarely done and handling situations under the worst possible circumstances. Planning and testing is typically very limited, so building the necessary expertise is a challenge. In general, because responding to a disaster is an exception, preparing for it becomes a burden on day-to-day priorities. Successful disaster recoveries involve IT performing Herculean efforts to get the job done.

Disaster recovery planning requires a lot of decision-making and, in fact, it is one component of a larger recovery undertaking. To be successful, it is important to take into account all sorts of requirements, drivers, interdependencies, contingencies, risks, and pitfalls associated with those activities. Within organizations, to create an understanding of how DR policies are set, a recent survey by Veritas indicated that in 71% of companies only the IT staff is involved in DR strategy. This is surprising given the weight and the impact of disaster recovery. Considering business continuity (BC) versus disaster recovery, in that survey by Veritas only 38% of companies have integrated their BC and DR plans. This can lead to the problem of misalignment of expectations versus capabilities. The challenge is being able to act and understand what those actual business requirements are, work with the appropriate people within the business organization to establish those requirements, and then set and meet realistic expectations. This balancing act brings into closer alignment the ability to meet critical needs and to have those needs understood in advance.

2. There Is No DR Plan

Disaster recovery requires teamwork in creating and executing the plan. The DR plan needs to represent the playbook for all the functional areas within IT prior to, during, and after a disaster. It needs to encompass applications, databases, networks, servers, clients, and storage. At a high level, it should guide employees on how to communicate where they

need to go and what they need to do to keep doing their jobs. Detailing who the owners are and the key contacts for each activity is also extremely important. Another important aspect is identifying dependencies and prioritization of tasks. This would include validation activities and application activation processes. All of these should be included within the DR plan. There should be the consideration of contingencies. Those contingencies contain "what if" scenarios and alternate responsibilities or roles when key individuals are not available. Decisions need to be made regarding levels of disruption that will constitute a disaster, downtime tolerances, loss tolerances, and steps required to resume normal operations. Another aspect is where is the plan? Do people know where it is? Is it kept in multiple locations? How can people find it when they need it? The DR plan needs to be a living document that is kept current to ensure that people know what to do in the case of a disaster.

3. How to Keep the DR Plan Current

There is a fundamental problem with DR because it exists outside the day-to-day operations of the IT environment. Because it is an exception, it is not at the forefront of people's minds. As soon as the DR plan is created, it almost immediately becomes outdated. The dynamic nature of IT environment ensures that your DR plan will fail if the management of the plan is not integrated as a rigorously enforced part of change management. As new applications are introduced and brought online, the priority and impact, with respect to DR from a resource and interdependency perspective, needs to be considered.

If the initial investment is made in developing a comprehensive DR plan that prioritizes servers and applications, identifies interdependencies, and documents recovery in detail, adding additional elements can be managed by simply updating the plan appropriately and providing notifications to necessary groups. Major infrastructure changes require more comprehensive plan updates. It is critical to examine DR backup within your change management process.

4. Testing the DR Plan

Typically, the DR plan is not tested or, if it is, it is not tested for the right things. DR testing is a major challenge for most IT shops. It is often done on a yearly or bi-yearly basis. Not only is it a major operational disruption; all too often it ends up being treated simply as a pro forma exercise. One significant weakness with many DR tests is the lack of true end-to-end testing all the way to production. The focus is often on recovering servers rather than application recovery. This is problematic. In today's complex applications, client server and web-based multi-tier applications, the components reside on multiple servers. There are interdependencies between these. If recovery has not been tested all the way to the application level, it is very likely that problems will occur.

Site Considerations

It is important to consider the degree of testing that can be performed based on site considerations. Whether it is a hot site, warm site, or cold site effects the times and degree of testing that can be done. DR testing often is not viewed as it should be, which is as a quality improvement exercise. Instead, it often is treated as a final exam, a test where the slightest hint of failure is to be avoided at all costs. Unfortunately, this can lead to somewhat perverse behaviors such as limiting recovery to safe or pre-tested recovery components to avoid embarrassment. The philosophy for DR testing needs to change. Essentially, it would be best to adopt an approach similar to software quality testing, where finding bugs is a good thing. Finding problems in DR is a good thing as long as those problems are addressed to diminish problems during a real disaster.

5. Pie-in-the-Sky Recovery Goals

An unrealistic recovery goal that cannot be achieved relates strongly to business and IT alignment, the very first item in the document. Frequently, organizations have established objectives and prioritized or classified servers and applications in accordance with the policies. However, upon an objective examination of DR capabilities and resources, it turns out that these goals are not attainable. It is important to set realistic Recovery Time Objectives (RTO). When does the clock start in a disaster? What is the tolerance for that outage? In Recovery Point Objective (RPO), 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.

Recovery Time Objective Timeline

A recovery goal of less than a day simply cannot be realistically obtained. If the DR facility is a cold site or depends heavily on tape-based recovery, those options and capabilities need to be reviewed and matched to goal setting. In Figure 1, there is an RTO timeline from a real environment that uses tape-based recovery. The realistic RTO in this environment is six days. This should not be viewed as a recommendation or a standard that tape-based recovery takes six days. It is an example in a particular environment.

There are steps that need to be taken in order to perform the recovery from wherever the tapes are being vaulted, whether it is Iron Mountain or some other location. The equipment provisioning process can be somewhat lengthy. When multiple applications need to be recovered, some applications will be recovered in less than the three days that are indicated in Figure 1, but overall the expectation is three days for the set of applications. Then there is the actual application recovery process.

One important thing to remember is the fact that RTO is the total time from the outage to the point where users get access to the application and the data, not simply the time that the data is recovered from site backups. In this example, allowing a full additional three days for the application team is a pretty lengthy timeframe and one that could be outside the business requirements for many applications in many organizations.

Recovery Point Objective

With Recovery Point Objective (RPO) there is a similar timeline in terms of a tape-based scenario and what is required to send tapes off site. In the case of nightly backups, the best case RPO scenario is one day. Figure 2 shows the process and the steps that need to be completed in order to send things off site in that one day. When tapes are sent off site on a weekly basis, then the RPO is in reality seven days, not one day.

Figure 3 is an example of RPO and RTO classification from a major financial services company. Multiple application recovery tiers are defined. The table defines RPOs and RTOs for each of those tiers, an indication of the categories of technology needed and an approximation of the relative cost. The cost could be exponential, it could exist in much closer bands, but even in the 24–72 hour range, asynchronous

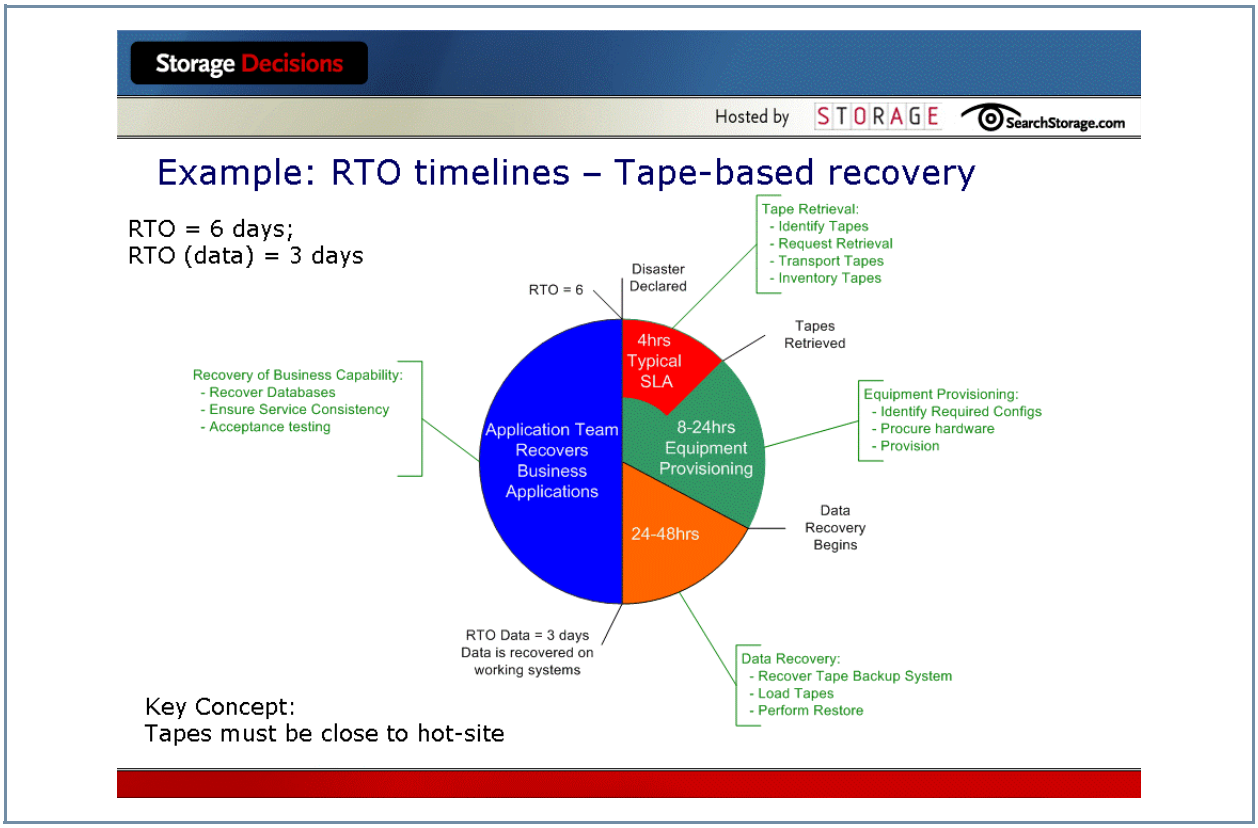

Figure 1

Storage Decisions

Hosted by STORAGE SearchStorage.com

Example: Tape-based DR - RPO=1 day

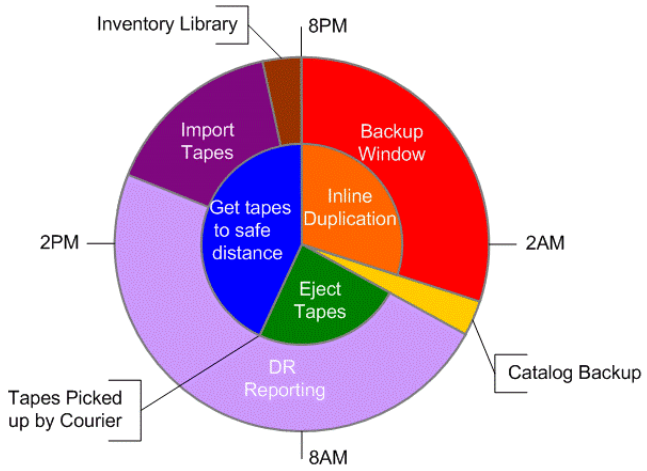

Figure 2

Storage Decisions

Hosted by STORAGE SearchStorage.com

RPO & RTO Classification Example From Major Financial Services Company				
Application Recovery Tier	**Recovery Point Objective**	**Recovery Time Objective**	**Technology Needed**	**Relative Cost**
AAA	No data loss.	No downtime	Synchronous Storage Replication; HA clustering; Application-based replication; Hot failover h/w	$$$$$
AA	Less than one hour data loss.	Up to four hours	Synchronous (cascade) or Asynchronous Storage Replication; AAM automated failover; Hot failover h/w	$$$$
A	Less than four hours data loss.	Same day recovery	Asynchronous Storage Replication; AAM automated failover; manual failover process; Hot failover h/w	$$$
B	Less than 12 hours data loss.	Up to 24 hours	Asynchronous Storage Replication; Manual failover process; Warm failover h/w	$$
C	Less than 24 hours data loss.	24 hours to 72 hours	Asynchronous Storage Replication; Tape-based data replication; Manual failover; Cold failover h/w	$
D	Less than 24 hours data loss.	72 hours plus	Tape-based data replication; Manual failover; Cold failover h/w	$

Figure 3

replication is part of the mix. It does not go fully to a tape-based mix until 72 hours into the plan.

6. DR Roles and Responsibilities

There is often a lack of clearly defined DR roles and responsibilities. Disaster recovery demands organization, coordination, and execution. Perhaps the best profile for a DR Manager is that of a battlefield commander. Executing a DR 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. In these circumstances, chaos is a given; therefore, 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 DR sites, equipment logistics, recovery initiation, and the overall execution process for recovery. Figure 4 gives a list from the IBM DR Redbook of possible DR teams or core groups that may need to be included within a DR scenario.

This should not be viewed as a definitive list that requires every one of these teams in place, but there are roles and responsibilities that need to be considered when planning the DR team to ensure that items are covered appropriately.

7. DR Plan Risks

Another topic for consideration is when the DR plan does not 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 organization willing to take? The definition of what constitutes a disaster that is covered by the plan has to be considered. FEMA has declared 33 major disasters as of September 1, 2005. Most of these disasters are floods but various kinds of other weather activity and fires are considered as well. There are elements within the organization'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 organization.

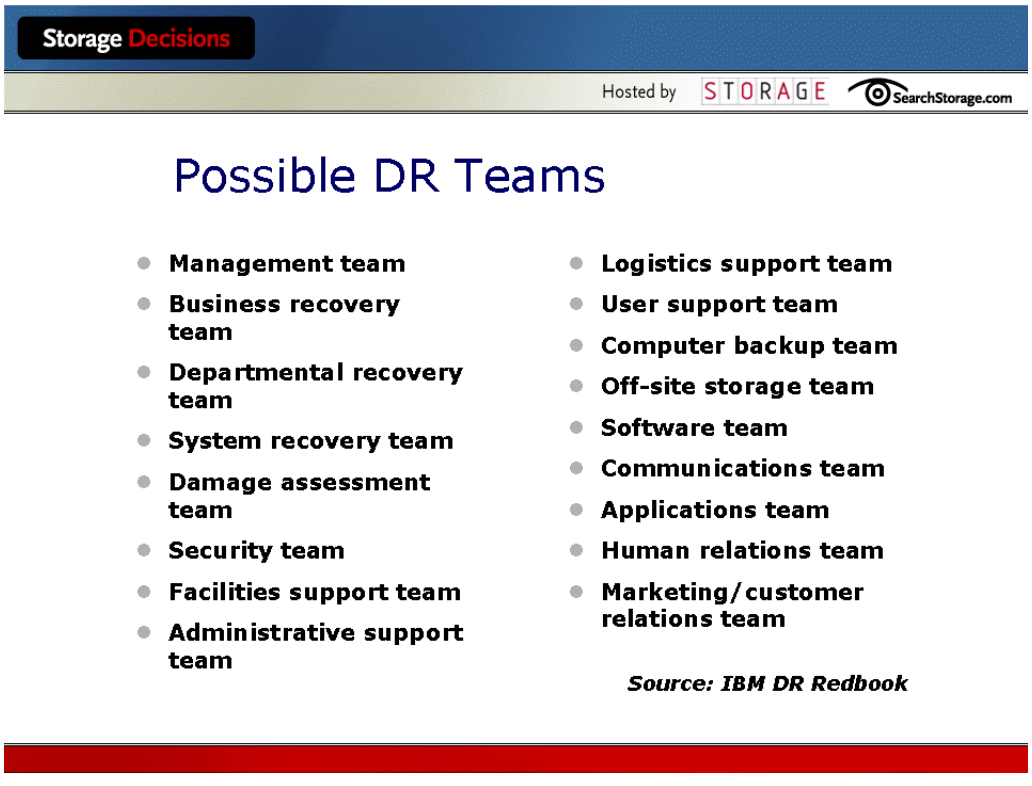

Figure 4

Internal Risks

Some of the other items to consider are internal problems such as vandalism and data corruption that could potentially cause catastrophic events within the operation of the business. A key step in assessing this is to conduct a business impact analysis. This analysis would develop an understanding of the categories; weigh the risks and the probability of the risks versus the cost and the impact. One danger is that often people buy the amount of insurance they can afford instead of the amount required. This is not ideal for business. Ensuring a full understanding of the risks and what is required to address them is critical.

8. Bad Backups

What happens when the backups do not work? This is technically related to the earlier topic of testing, but it is worth underscoring the point. For many companies, tape backup is still the primary medium for disaster recovery, certainly for off-site disaster recovery. As an alternative, a wide area of data replication is growing and is used in many environments, but it might be too costly an option for some businesses. Fundamentally, the DR plan is only as good as the tape restoration capabilities and the effectiveness of the off-site tape management processes. Bad backup tapes mean no recovery is possible.

Backup Tape Concerns to Consider

Some of the things that need to be considered in terms of backup are nightly failures. Are the backups completing successfully? What are the tape management practices that are in place? How are tapes being handled with off-site media production? Many environments lack the resources to duplicate tapes to send off site. Newer technologies like virtual tape libraries can help. In a cold or a warm site, bare metal recovery should have strong capabilities, particularly when depending on backups for recoveries. Bare-metal recovery capability should be tested very carefully.

Application Recoverability

Application recoverability must be validated through the recovery of backups to the application level. Consider a scenario where multiple servers make up a given application. Those multiple servers are backed up at different points throughout the night. Recovering each of those backups may be successful independently, but whether the application is sufficiently synchronized to be recovered completely needs to be reviewed through monitoring and testing. If there is not solid reporting on the success of backups, then the ability to recover in a DR scenario is questionable. It is important to ascertain that backups are completing at the application level and that the data on the medium is good.

Technology Options

Technology options can help, because they would reduce Recovery Point and Recovery Time Objectives which would evolve to a point of being less dependent on backups. The current best practice is replication. Replication can take place at the storage level, the network level, or even the host or application level, greatly reducing the currency of data, the RPO, and the time it takes to reach RTO. Replication is the key. Disk-space backup technologies are also great enablers to improving DR capabilities.

Virtual tape libraries (VTLs) or other disk solutions can be used in combination with replication and remote vaulting. VTLs can greatly ease the DR burden and free up resources that can be deployed to provide higher levels of recovery. Virtualization through VTLs or virtual servers such as VMWare, being able to abstract the hardware environment and reduce dependencies on specific hardware configurations, makes recovery less painful.

One area that is not often considered is archiving. DR is concerned primarily with current data, getting back the current data that you need to run the business and the applications associated with that data. Reducing the amount of current data that needs to be recovered to adjust the current data set will create a smoother recovery. A strong archiving capability enables quicker and more reliable DR. Finally, continuous data protection helps dramatically reduce both RTO and RPO and tends to do so at a cost that is less than traditional replication.

9. Alternative Recovery Services

In the case of a disaster, who will be there to recover the data and initiate the DR plan? This is an uncomfortable factor that needs to be considered. It is the toughest topic of all of these items. With disasters like 9/11, 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 DR sites.

Redundancy of Roles

Any DR planning scenario must consider redundancy of roles to ensure that people are available to cover various responsibilities in the process. This goes well beyond DR to business continuance, including issues such as chain of succession within the executive levels of the company. Which people will be there to run the business and the critical business functions needs to be considered. It underscores the need for comprehensive documentation and training. Large organizations with distributed IT expertise in multiple data centers 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.

10. DR Cost Consideration

Data protection and recovery requirements may seem too expensive. This is the crux of the DR problem. DR is a particularly taxing expense, one that most organizations have a great deal of difficulty absorbing. It returns to the gap between the ideal and the practical. It is a matter of ensuring that realistic capabilities are set and ensuring that the expectations are well known and well publicized within the environment. There should not be a huge gap between what the business thinks IT is capable of delivering and what IT is capable of delivering. Being able to address the IT cost for DR is an issue of integrating DR into standard operations as much as possible. Ideally, the DR resources and equipment are not viewed as technologies that are sitting idle. One solution is multiple data centers that can serve as fill-over points to one another with some additional capacity, so that these pieces of technology are being used to help ease the cost. Ultimately, this comes down to making an informed decision of either spending money or accepting risk. There is no easy solution. Newer technologies are emerging that make this more cost effective. Regardless, DR is an investment. It is an insurance policy.

Additional Considerations

There are considerations in addition to the 10 items in this document. Some of these considerations include how long can you operate in your DR mode? Hurricane Katrina is underscoring that aspect. Many people think about DR and assume a few days, maybe a week at the outside for operations before returning to normal. What happens if it is months or even longer that you will need to operate in DR mode? Does the plan support that? What is the DR plan for the DR site? When operating in the DR site for a long period of time, steps need to be taken to ensure that the data is appropriately protected. Typically, during a disaster the business is in a vulnerable situation. What things need to be done to mitigate that risk? Finally, what is the plan to return to normal? How do you get back? How do you maintain business operations and return to your primary site? These are things that need to be weighed in the entire DR equation.

Executive Summary

There are a number of recurring themes in these checklist items. Essentially, the keys to DR success are having a realistic and well understood set of objectives that are based on the actual needs of the business. This involves planning and preparation from the business impact analysis to understanding and quantifying risks, to classifying and prioritizing applications and data for recoverability. Additionally, there is the need for preparing systems and other technology to be able to recover, and then documenting everything, especially the DR plan. Another factor for success is to make DR less than an exception by integrating DR hardware components into production. The dynamic nature of IT requires continuous review and updates of the process and the plan. It is not something that can be contemplated once or twice a year. It must be part of the day-to-day operations of the IT environment. It requires practice developing confidence by having well understood roles and responsibilities, regular testing to demonstrate competency, and being able to know that recovery can be performed when necessary. Finally, investing in a solid technology basis is critical. An organization must leverage newer technologies that provide higher performance at lower cost where possible, and at a minimum it must ensure that backups are functioning well. The references and resources in the table on the next page will assist in starting DR planning and providing additional checklists and guidance.

Reference or Resource	Internet address
Dynamic Markets, "Veritas DR Research 2004"	eval.veritas.com/mktginfo/products/White_Papers/High_Availability/dynamic_markets_executive_summary.pdf
DR Institute	www.drii.org
DR Journal	www.drj.com
Disaster-Resource.com	www.disaster-resource.com
IBM TotalStorage Solutions for DR	www.redbooks.ibm.com/redbooks/pdfs/sg246547.pdf