

A Practical Guide to Disaster Recovery Planning: The basics to getting started.

Brace Rennels, Business Continuity published: March 2006

Executive Summary

When you think about your disaster recovery plan, does your tape backup system come to mind? Does the mere mention of disaster recovery make you a bit nervous? If so, you're not alone. Many businesses risk grave losses due to failures and disasters yet continue to depend on their tape backups to help them recover successfully should a major outage occur. The thought of implementing a more appropriate disaster recovery plan can be daunting; to the point which many simply push it off until later. Unfortunately 'later' often ends up being after the business has suffered a major loss from which it could not recover.

This paper is intended to help simplify the process of starting a disaster recovery plan so as not to be so overwhelming. Through some basic steps, businesses can better protect themselves against data loss while working toward a more complete business continuity plan.

This whitepaper will cover some basic steps to help your business be better prepared to withstand failures and outages.

- The need for a DR plan – Why you are at risk?
- Getting started – Your business is ready to be protected
- Defining what is right for your company – One size does not fit all
- Potholes to avoid – Learning from other's mistakes
- The planning process – Small steps make a huge difference

If you're already thinking that this process is just too big, relax. I'll walk you through some simple ways to help improve your company's resiliency against outages to maintain user and business productivity during adverse situations.

The Need

Hurricanes, tornados, floods, malicious acts, or simple mistakes. Unfortunately, unplanned outages do happen. Whether it is a severe weather incident that shuts down a city or region or a simple mistake like kicking a power cord loose causing a server to halt, every business is susceptible to some form of outage or disaster. And there is not likely any business that can simply afford to just be down for days or even hours without suffering pains of some sort. At best one could expect to incur some financial losses and have to smooth things over with some unhappy customers, but at worst, and far too often this is the case, businesses are unable to recover and are forced to close.

The statistics show some staggering results when the need to plan for disaster is not realized and implemented. By implementing a few short- and long-term solutions, you can help to keep your business from being one of these statistics.

Do any of these apply to your company? Let's look at a simple example that resonates with just about any company. One of the most critical applications for businesses today is email; without it, day-to-day operations can not run, or at best will slow to a crawl. Consider the impact to your company when email goes down. Productivity is likely to slow drastically or even stop completely. For better or worse, we are heavily dependent on our email systems for performing our jobs and running the business. Consider for a moment the impact of your email system being unavailable. Most employees would notice within minutes or even seconds and there would be an immediate work stoppage as everyone asks 'is email down?' and then proceed to continue trying until they realize there really is a problem. Even a small amount of downtime for just one application can be very costly.

40% of all SMBs will go out of business if they cannot get to their data in the first 24 hours after a crisis. -- Gartner

43% of companies never resume business following a major fire. Another 35% are out of business within 3 years.
-- U.S. National Fire Protection Agency

"Small companies often spend more time planning their company picnics than for an event that could put them out of business." -- Katherine Heaviside, Epoch 5

The productivity dollars add up quickly, and this does not account for the business and legal implications of lost data that could result in fines and even imprisonment. The need to protect systems and data is readily apparent.

Getting Started

The biggest hurdle many businesses face when it comes to implementing a disaster recovery or business continuity plan is simply getting started. Breaking things down into less formidable steps can simplify the process to get it completed more efficiently. You will have a solid basis from which to begin.

The most important resource for any business to consider is its people. Property can be replaced, people cannot. Be sure to have a viable evacuation plan to ensure the safety of all employees before starting anything else. Consider that a major disaster to your business may very well have a serious impact on the personal lives of your employees. Plan on and account for the fact that your employees may have to tend to personal issues during a disaster and may not be available to assist in recovering the business. Think about the people first and foremost.

As for the rest of your business, here are some considerations for creating your plan.

1. Understand what keeps your business going.

Identify those systems and resources that are absolutely critical to run the business and focus on protecting those first. Not all systems require the same levels of protection; in fact some may not need protecting at all. A cost-effective and efficient business continuity plan sets priorities to help bring the business back online as rapidly as possible.

2. Get the data out of the building

This is the quickest and easiest way to help ensure that the business can be recovered should it suffer a loss or outage. If a failure or loss of data occurs you need to be able to recover it. Even if it requires being restored to a different location, at least your data will be available.

3. Calculate the cost of downtime

This will help in setting priorities as to which areas of the business get protected and to what levels. Note that while some systems may not have a large dollar value associated with them being down, there may be legal ramifications should they not be available or recoverable. Cost is not just lost revenue, but the overall impact on the data has on enabling the business to meet employee, customer, legal, and financial obligations.

4. Think beyond tape

While tape is probably the most common method for protecting and recovering data, it may not be appropriate or sufficient for all of your applications. Tape is acceptable for long-term archival and recovery, however, it can be a lengthy process to rebuild a system from tape. After determining the Recovery Point Objective (RPO) and Recovery Time Objective (RTO) for each of your systems, consider appropriate enhancements to tape solutions such as host-based replication. Other solutions like data replication can provide near-zero data loss and disk-to-disk recovery options for a rapid return to productivity.

5. Continue to build and test the plan – continuously!

Be sure that your plan accounts for the various types of outages that could affect each business location including a simple disk or hardware failure, a building outage, a regional power failure, environmental disasters, and natural disasters such as hurricanes and earthquakes. Check that the necessary procedures are documented and available for everyone to read and understand. Everyone in your company has an important role should an emergency arise. Whether their role is to get themselves safely out of the building or to help in the rebuilding process, it is important for them to know exactly what is expected of them during a crisis.

Business Continuity Planning

A disaster recovery plan is sometimes referred to as a business continuity plan. However the difference between these two plans should not be confused. A disaster recovery plan is often characterized as being specifically for IT systems within a specific location or maybe a few locations. A business continuity plan can be considered the all-encompassing corporate plan that describes the processes and procedures an organization puts in place to ensure all aspects of business can resume and be recovered should a disruption occur. A business continuity plan covers more than just computer systems and data at a few physical sites. Critical areas such as employee safety, relocation plans, communication systems and others are covered in a business continuity plan.

Business continuity planning seeks to prevent interruption of business-critical services, and to re-establish business operations to an acceptable level as swiftly and smoothly as possible. A complete business continuity plan should account for your employees first and foremost with an evacuation plan that ensures everyone's safety. Other resources to cover include relocation, temporary offices, telecommunications, remote access, customer and business activities, disaster recovery of systems and data, and all other necessities to return to business as usual, even in the event that an entire location is not accessible.

Creating a business continuity plan can take upwards of 6-9 months during which time the appropriate disaster recovery solutions should be implemented to provide adequate protection of your data to prevent a major business interruption. As this document is not intended to cover complete business continuity planning, further information should be gathered with regard to starting a business continuity planning project. While your long-term goals may warrant a complete business continuity plan, the concepts covered in this whitepaper should help you to get started on the disaster recovery portion to protect your data and applications.

Disaster Recovery Planning

Unfortunately there is not a magic formula for developing a disaster recovery plan for every business. Every business has unique needs due to different customers, geographic locations, applications, etc. What others can withstand, your business may not, and vice versa. Your disaster recovery plan should be customized to meet the requirements of your business and the values you place on your data. Performing a business impact analysis and risk assessment can help to identify the real needs of the business and direct the creation of the disaster recovery plan. Information on these is readily available in addition to resources for assisting with or performing the actual analysis.

Clearly define what constitutes the different levels of a disaster, as different situations will likely invoke different procedures. For instance, a system failure would invoke different recovery procedures than a fire that destroys the entire building.

Don't Wait

Do not wait until you have a complete DR plan to start protecting your business. The quickest and easiest way to protect your critical systems is to get the data offsite to a different geographic location. Maintaining a copy of your data at a remote facility will enable you to recover and regain productivity. You likely perform tape backups already, so the easiest and quickest process may likely be to ensure these are stored offsite at a secure location, readily accessible in case a recovery is necessary.

Is a tape-based data protection solution enough? While it may be for some of your systems, it is probably not sufficient by itself for all of them.

To determine where a higher level of protection is needed, identify and prioritize the resources and infrastructure that must be available to enable critical business functions to resume. What keeps your business going? Email? Databases? Web servers? Prioritize your data and protect the most critical first, if they cannot all be done at the same time.

Two key factors to consider when determining priorities are Recovery Point Objective (RPO) and Recovery Time Objective (RTO). RPO defines the amount of data, in time, which your business can afford to lose for a particular system. For some applications, recovering data from yesterday or even last week may be ok – in this case, the RPO would be days or weeks. Other applications and data, for which any loss is not acceptable, you may choose to have a RPO of minutes or less. While RPO defines how much data is protected, RTO defines how long it takes to recover that data. RTO is the amount of time the application can be down and not available to users or customers. Can your business survive without a particular application for a few minutes? How about a few days? These factors will help to set appropriate priorities for recovering systems and data and determine the right solution for each.

Do not assume that your tape backups are sufficient. They are not likely suitable for meeting the RPO and RTO of all of your systems. With tape, the recovery point is back to the time of the last backup - typically a day or more. Recovery Time with tape is generally a day at best because tapes must be retrieved and the data must be restored from them. For most businesses, these are not acceptable levels for all of systems.

Beyond Tape

Where tape is deemed insufficient, consider other alternatives such as real-time replication to augment your tape backup solution. Replication solutions can provide for near-zero data loss and allow for immediate system and data availability for recovery and user access. There are various options in the replication arena that vary in cost and complexity. Some of the options include host-based or hardware-based solutions with synchronous or asynchronous replication. Host-based replication is often more cost effective and the most flexible as it can work with heterogeneous storage and can tightly integrate with your applications to provide excellent disaster recovery and high availability solutions. Hardware-based solutions tend to be expensive and proprietary, working only with that particular vendor's storage devices, which limits flexibility now and when choosing hardware in the future.

Project Planning

A documented project plan can help to expedite the implementation of your disaster recovery procedures by identifying and coordinating pre-requisite tasks, responsibilities and resources for each task. Pre-planning allows for many questions to be answered before the actual work begins, preventing delays and redesign during the implementation. A project plan allows for the breakdown of tasks into more manageable chunks so that the overall project is not as overwhelming. The project plan helps to define and validate the solutions, and more importantly help you manage and coordinate the rollout. Consider your options and be sure to account for the protection of your applications and systems as well as infrastructure and human resources.

Although you likely have many systems and applications running throughout your company, they are not likely all of the same importance to the success of the business. Determine and document what systems and data are critical and focus on those first. Some systems can probably be down without adversely impacting the business while others are more critical and must be brought back online quickly to prevent losses. Simply applying the same levels of protection to everything can leave some systems insufficiently protected or prevent the plan from ever being implemented as costs and complexity will be insurmountable barriers. Your project plan will be a living document, continuously reviewed, updated, and modified as the implementation progresses.

Strategic Planning Assumption

75 percent of large enterprises will combine data replication and tape technology for rapid application recovery (0.7 probability).

Bottom Line : Organizations that are running 24x7 operations and are confronting shrinking backup windows, or that foresee an inability to meet service-level agreements, should plan and budget for deploying data replication technologies.

Avoiding the Potholes

There is a lot to consider when planning for the unplanned, but with a systematic approach you are more likely to be successful in designing and implementing the solutions that will prove successful if ever needed during a disaster.

With all the details to consider and the myriad of options available, errors and mistakes are likely unavoidable. This is one area where we can learn and benefit from other's experiences. Avoiding or at least minimizing mistakes throughout the entire process will lead to a quicker and smoother deployment and result in a better protected business, not to mention a less stressful design and implementation process for those involved.

Lack of planning, resources, and time

We all have plenty of day-to-day tasks to consume our time. Making time to work on what amounts to an insurance policy for your business, your DR plan, is often pushed off for more urgent matters that need immediate attention. Unfortunately, tactical activities are easier to justify spending our time on than strategic activities. To help prevent this project from being pushed off for other tasks, get buy-in for this project from the necessary decision makers and make it a priority with allocated time and resources to bring it to fruition. The risk analysis and business impact assessments can serve as excellent resources for getting management support.

Proper planning helps ensure that important details are not left unaccounted for and prevents having to go back and revisit entire sections. It is much better for your business to be proactive with its DR plan rather than reactive during or after an outage or catastrophe.

Lack of knowledge or expertise

Not sure you have the know-how in-house to build a DR solution? Do not let this stand in the way of protecting your business. There are plenty of resources available to help with this project. If you have a thorough knowledge of your technology, it may still prove beneficial to seek outside assistance with thorough knowledge of disaster recovery planning and rollouts. Even if it is just to help draft or review your plans to be sure something was not overlooked, you will have justified the expense. Remember, you don't know what you don't know. There are many who have done this hundreds of times and could be of great value in designing and even implementing your solutions.

Unrealistic deadlines

While speed is of the essence to remove the risk to your business, moving too fast can result in mistakes that will further extend the completion date. Being able to prioritize your tasks and identify those that are interdependent will help facilitate a smooth implementation of critical controls. This is where listing pre-requisite tasks in your project plan will pay dividends. Set appropriate milestones that account for delays and setbacks so as not to have to rush to meet unrealistic deadlines. It is better to make mistakes early in the project when you have accounted for enough time resolve it, rather than rushing and discovering it at a more critical time.

Lack of practice

Practice...practice...practice... This cannot be stressed enough. A plan is only as good as it is when it is executed. Once your plan is complete, and even throughout the design process, it is crucial that it be tested thoroughly to ensure that, should it need to be executed for real, it will work.

Testing the businesses continuity and disaster recovery plans provides an excellent training vehicle for everyone in your company. People at all levels throughout the company need to know what to do in an emergency and be aware of the role they may play in the recovery process. The last thing you want is for your first test to be when you have an actual outage. That would not be a good time to discover an oversight or a design or implementation flaw.

After the initial plan is complete and successfully tested, schedule quarterly or semi-annual tests to be sure changes to your business and your environment have not rendered part or all of the plan ineffective. Continuous testing will help to ensure that any new personnel are up to date and knowledgeable on the disaster recovery procedures should they ever need to be put into practice.

If someone asks if you have a viable disaster recovery and business continuity plan, you will be able to affirm with the utmost confidence.

Summary

Ready to get started? You now have the basics for building a disaster recovery plan for your business. The key is to remember that while the complete business continuity plan can get a bit overwhelming, there are interim things that can be done to implement a solid disaster recovery plan for protecting your business from data loss and application downtime. Do not wait for the corporate business continuity plan to be completed before instituting a solid DR plan, do them in parallel. The DR plan is a piece of the overall BC plan. Do not leave your systems and business at risk during the BC planning process; protect them immediately.

Seek assistance and advice from those who have experience in this area. For over 10 years, Double-Takel® Software has been providing the products, services, and support to help you be successful in protecting your most critical applications. When losing data is not an option, your only option is Double-Take®.

About Double-Take® Software

Double-Take® Software, formerly known as NSI Software, Inc. provides the world's most relied upon solution for accessible data protection for Microsoft® Windows® applications. The Double-Take product is the standard in data replication, enabling customers to protect business-critical data that resides throughout their enterprise. With its partner programs and professional services, Double-Take delivers unparalleled data protection, centralized back-up, high availability, and recoverability. It's the solution of choice for thousands of customers, from SMEs to the Fortune 500 in the banking, finance, legal services, retail, manufacturing, government, education and healthcare markets. Double-Take is an integral part of their disaster recovery, business continuity and overall storage strategies. Double-Take Software is privately held and headquartered in Southborough, MA. For more information, please visit www.doubletake.com.

© 2006 Double-Take® Software, Inc. All rights reserved.

Double-Take® and GeoCluster® are registered trademarks Double-Take® Software, Inc. Microsoft, Windows and the Windows logo are trademarks, or registered trademarks of Microsoft Corporation in the United States and/or other countries. All other trademarks are properties of their respective Companies.

For more information on Double-Take® Software products and services please contact us.

Sunbelt Software USA
www.sunbelt-software.com
Tel 727-562-0101

Sunbelt Software HQ France
www.sunbelt-software.com
+33-(0)1 47 77 05 00