A Disaster Recovery Plan - does my business need one?

Often when business owners consider the concept of protecting their business against unforeseen circumstances they see Business Continuity Planning and Disaster Recovery as the same thing but the two should not be confused. This article concentrates on the latter and identifies some of the basic steps to help your business become better prepared to withstand data disasters.

Business Continuity Planning

A business continuity plan identifies a company's exposure to internal and external threats, and puts in place the means with which to provide effective prevention and recovery for a business, whilst improving its competitive advantage and system integrity.

Disaster Recovery Planning

A disaster recovery plan is often characterised as being specifically for IT systems within a specific location or maybe a few locations. There is no magic formula for developing a disaster recovery plan because every business has unique needs due to different customers, geographic locations and IT applications. It's necessary to clearly define what constitutes the different levels of a disaster, as different situations will probably invoke different procedures. For instance, a system failure would invoke different recovery procedures than a fire that destroys the entire building.

Why do I need one?

Unplanned power failures do happen, whether it's a severe storm or the cleaner unplugging the server to do the vacuuming. Every business is susceptible to some form of disaster and no business can simply afford to just be down for days or even hours without suffering some sort of pain, be it inconvenience or financial. Servers can fail leaving you without access to key company data.

By implementing a few short and long term solutions, you can help to keep your business from being one of those companies that never fully recover from a disaster. Consider the impact on your company if the email system goes down, because every business is heavily dependent on its email systems for performing basic tasks and running the business.

Developing the plan

Consider your people to be the most important part of the plan. Assume that your employees may have to tend to personal issues during a disaster and may not be available to assist in recovering the business. For the rest of your business, here are ten considerations for creating your plan:

1.) Start immediately

The quickest and easiest way to protect your critical systems is to get the data offsite to a different location. Maintaining a copy of your data at a remote facility will enable you to recover and regain productivity. You should already perform tape backups, so the easiest and quickest process may likely be to ensure these are stored offsite at a secure location. To determine where a higher level of protection is needed, identify and prioritise the resources and infrastructure that must be available to enable critical business functions to resume.

Identify 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 sufficient or it could be days or weeks. Ascertain the amount of time an application can be down and not available to users or customers. Can your business survive without a particular application for a few minutes or several days?

2.) Data security is more than just 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. Other solutions like data replication can provide near-zero data loss and disk-to-disk recovery options for a rapid return to productivity.

3.) Fully understand what drives your business

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 and 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.

4.) Plan the project

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.

5.) Calculate the cost of downtime

This will help in setting priorities as to which areas of the business get protected and to what levels. While some systems may not have a large cost 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.

6.) Set realistic deadlines

Moving too fast can result in mistakes that will further extend the completion date. Being able to prioritise your tasks and identify those that are interdependent will help facilitate a smooth implementation of critical controls. 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 to resolve it, rather than rushing and discovering it at a more critical time.

7.) Preparation

To help prevent this project from being pushed off for other tasks, get buy-in for the 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.

8.) Lack of knowledge or expertise

Even if you haven't prepared a plan before, don't put it off as there are plenty of resources available to help and even 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 implementation.

9.) Avoiding the potholes

With all the details to consider and the myriad of options available, errors and mistakes are probably unavoidable, so learn and benefit from other's experiences. Avoiding or at least minimising 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.

10.) Continuously develop and test the plan

A plan is only as good as it is when it is executed so it's crucial that it is 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 a real disaster. That would not be a good time to discover an oversight or a design or implementation flaw. 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.

REMEMBER!!!

The Companies Act 2006 has dramatically changed the responsibility, duty and liability of Directors to the extent that unless they can show evidence that they have considered and taken reasonable steps, to protect the company and its value from all risks that could critically affect a business's ability to trade, and as a result the company's stakeholders, the community or the environment suffer loss or damage, the Directors can be held liable to unlimited damages. Can you afford not to have a Disaster Recovery Plan?