



Disaster Recovery, Continuity Planning and Backup Strategies for Small Businesses

[April 2010]

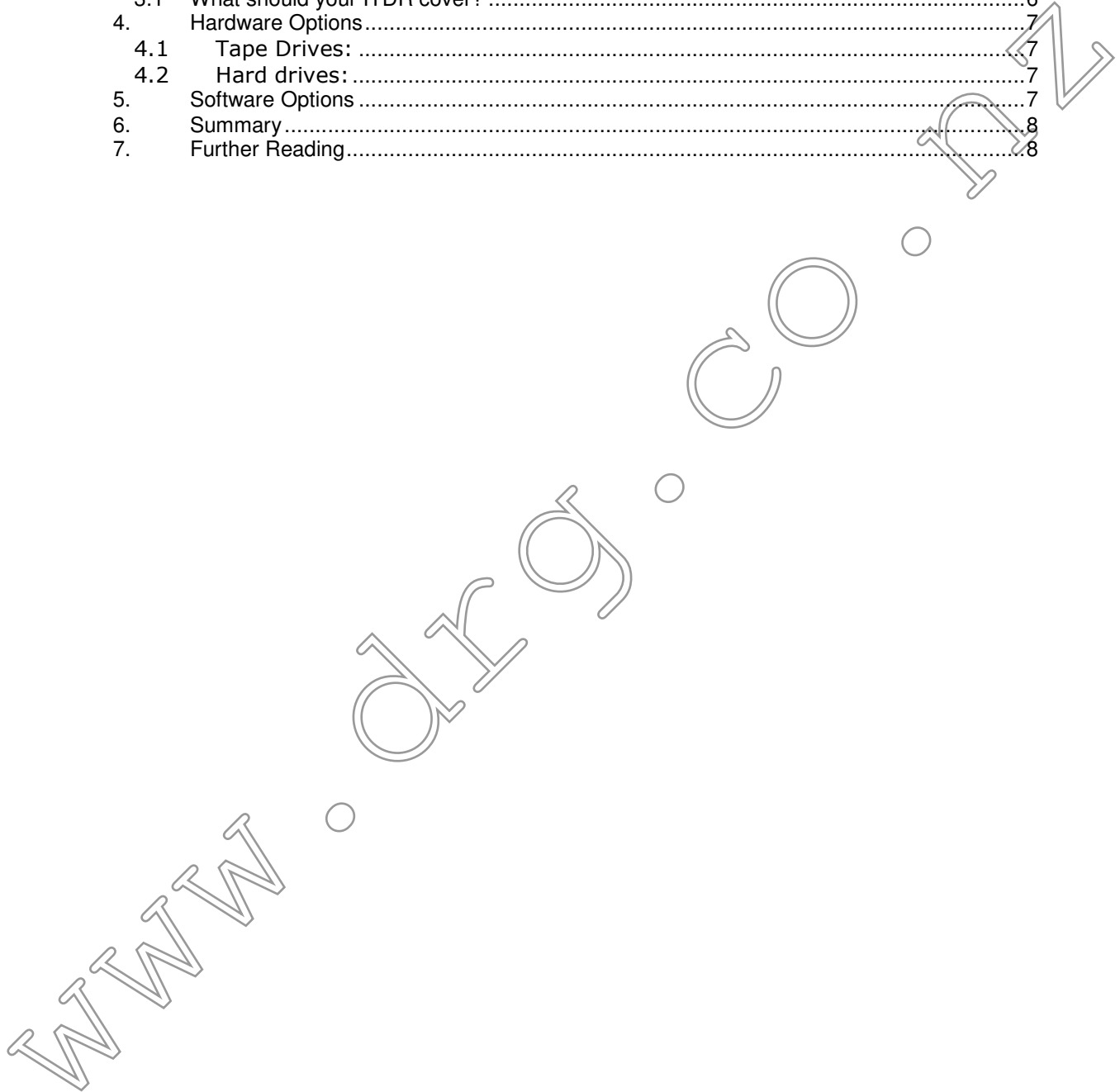
DRG Technology

Paul Röllin

Director

Contents

1.	Introduction.....	3
1.1	What is Business Continuity?.....	3
1.2	What things should be in a Business Continuity Plan?.....	3
1.2.1	Business Impact Analysis	3
1.2.2	Risk Assessment.....	4
1.3	What Does This Document Cover?	4
2.	What do we mean by disaster recovery in IT?	4
3.	IT disaster recovery strategies for SME's	5
3.1	What should your ITDR cover?	6
4.	Hardware Options.....	7
4.1	Tape Drives:	7
4.2	Hard drives:.....	7
5.	Software Options	7
6.	Summary	8
7.	Further Reading.....	8



1. Introduction

If disaster struck today, would you be ready?

For business a disaster doesn't just include the obvious: fire, flood, earthquake etc. What about a hard drive crash? The accidental deletion of last months accounts? Theft of your main computer?

Being ready for a disaster means planning.

1.1 What is Business Continuity?

Business Continuity Planning is the creation and validation of a Business Continuity Plan (BCP) describing how your business will recover and restore partially or completely interrupted critical functions within a predetermined time after a disaster or extended disruption.

That is, a BCP covers how to stay in business in the event of disaster. BCP includes disaster recovery which can cover all types of disaster from major to isolated minor issues (e.g. fire through to a hard drive failure).

When developing a BCP it is important to fully understand the critical areas of your business. For modern business, IT is no longer a nice thing to have – it is critical to how you manage you clients, staff, stock and accounts. All business have a reliance on technology such as email for contacting clients, online transactions for dealing with suppliers, banks etc, and electronic accounts.

1.2 What things should be in a Business Continuity Plan?

1.2.1 Business Impact Analysis

The Business Impact Analysis is the foundation on which the BCP is developed. It identifies, quantifies and qualifies the business impacts of a loss, interruption or disruption of business processes so that management can determine at what point in time these become intolerable (after an interruption). This is called the 'Maximum Tolerable Period of Disruption'. It therefore provides the data from which appropriate continuity strategies can be determined.

The main things to consider are:

- What is critical to my business?
- What can I afford to lose?
- How long can I trade after a major disaster?
- How will I recover my data?
- What will happen to my customers?

The answers to these questions will vary greatly from business to business – for example, in a major natural disaster will all your clients be equally affected and therefore the importance of continuity in the short to medium term greatly reduced?

1.2.2 Risk Assessment

In the context of BCP, a Risk Assessment looks at the probability and impact of a variety of specific threats that could cause a business interruption. Risk Assessment activity should be focussed on the most urgent business functions identified during the Business Impact Analysis process.

For Small to Medium sized businesses it may be difficult to quantify the risk of a given event, but it is still important to understand what risks the business faces and which are the most likely.

Some risks that you should consider include (but are not limited to):

- Fire
- Flood
- Theft
- Hard drive crash
- Deletion of data
- Network equipment failure

1.3 What Does This Document Cover?

This document will concentrate on disaster recover and continuity of your IT systems.

Planning for disasters is not just for major corporations – many Small to Medium Enterprises (SME) will equally face disasters over the time they operate; if they want to be successful after a disaster then planning is critical.

The cost of data loss can be huge. In fact, 20 megabytes of accounting data takes 21 days and costs \$19,000 to reproduce. Among companies who lose data in a disaster, 50% never re-open and 90% are out of business within two years!

Source: The Cost of Data Loss: By Harald Anderson (<http://ezinearticles.com/?The-Cost-of-Data-Loss&id=7111>)

2. What do we mean by disaster recovery in IT?

With regard to a business' IT system, a disaster can range from small, isolated events to major regional catastrophes.

What is a small isolated disaster? A good example of this would be a staff member accidentally (or possibly maliciously) deleting a business critical file from the server. Other possibilities include hardware failure in a critical machine, small isolated fire in one part of the building, etc.

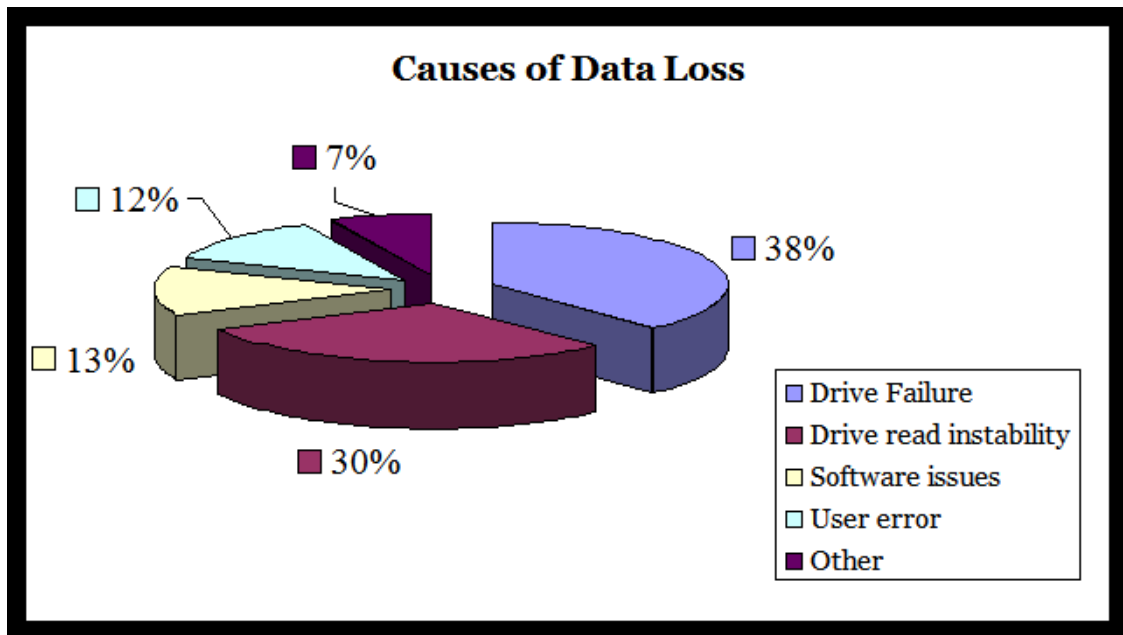


Figure 1: Causes of Data Loss.

(Source: a survey of 50 data recovery firms across 14 countries, DeepSpar Data Recovery Systems, "A Survey of Data Recovery Issues & Causes," *Unpublished working paper*, (2007).)

From figure 1 it is clear that hardware failure is the main cause of data loss. Major disasters account for only a small proportion of the risk – far greater is the likelihood of a hard drive failing, a PC being stolen or the accidental deletion of a file.

A major disaster could be a significant fire in your building or something more widespread such as flooding, volcanic activity, earthquakes or major storms.

For large organisations IT disaster recovery (ITDR) planning will include redundant systems to take over in the event of failure of the main system – often in a different city!

Such a level of continuity planning is beyond businesses in the SME space. For these businesses redundancy on this scale is not available due to cost. For them the best way to plan for disaster is to make sure that all critical systems are backed up. If systems are continuously backed up then deleted files can be quickly recovered, business critical machines quickly replaced and disruption from the minor disaster is greatly reduced. If backups are kept off-site, then even major disasters (major fire or flood) are recoverable.

3. IT disaster recovery strategies for SME's

Backing up your data is the most critical part of your ITDR planning. If your data is safe – so is your business.

Remember – you can't recover what you haven't kept!

3.1 What should your ITDR cover?

We believe that a DR plan should answer the following questions:

- What data is critical?
- How long do we need to store the data for?
- How much data can we afford to lose?
- What machines are 'business critical'?
- What machines can be replaced quickly vs specialised hardware that may not be easy to replace?
- How long can we function without that machine or data?

The answer to these questions will be different for every business and can only be answered by people intimately involved in the business.

Data backups must form the main part of any DR planning. Redundant systems are beyond the budgets of SME's but good backups stored safely can remove the need for such costly systems.

For the majority of businesses there will be at least 1 business critical machine, the loss of which will stop all or most work immediately. This machine is generally a server controlling file storage, emails, internet access and some centralised applications (e.g. accounts, CRM etc) and therefore needs to be at the centre of any Disaster Planning.

For small to medium businesses finding the right backup solution can be difficult. There is a large market for backing up single PC's with numerous products aimed at the home user (or single PC business) and there are a similar number of options for large corporate organisations.

But for the SME market (here defined as 3 to 30 PC's + 1 or more servers) the range of products and offerings is noticeably smaller. Such businesses are too large for the single PC options to be effective and too small to afford the large corporate solutions.

DRG Technology has found that a large number of clients are experiencing significant growth in data volumes needing to be backed up, this means that they now need a solution that is:

- Flexible
- Scalable
- Easy to manage
- Automatic
- Includes some level of redundancy

Any DR plan must also include ways to test the system. Backup audits should be undertaken regularly to ensure that the backups are usable in an emergency.

4. Hardware Options

There are basically two options when it comes to backup hardware: Tape or Hard drive. Both have their pros and cons, with some people swearing tapes are best, while others insist on hard drives.

4.1 Tape Drives:

Tape drives have been the main hardware for backups for several decades. Originally they were significantly cheaper than other options and can be more flexible in terms of storage, rotation etc. Tapes lend themselves to simple off site storage, easy rotation (different tapes for different days/weeks/months) and simple archiving.

However, writing to and reading from tapes can be very slow, the life span of tapes can be relatively short (a few hundred writes), although for archiving they will last decades. They can also become obsolete over time, making recovery from old archives difficult if the organisation has not kept their original tape drives.

4.2 Hard drives:

Hard drive technology has advanced rapidly over the last decade and Terabyte sized drives are now available for low cost. Hard drive prices per megabytes have now reached the region of a few cents making them a very cost effective way to store data. If stored in a safe environment a hard drive should remain readable over many decades and the technology is not proprietary so less likely to become obsolete in the way tapes may.

There are two main ways of connecting a hard drive to a computer for backing up – Direct Attached Storage (DAS) and Network Attached Storage (NAS). DAS drives include things such as internal drives and USB drives plugged directly into a PC. NAS drives sit on the network, connected to the LAN and so are available to all systems to use for backup. NAS units allow for the use of RAID to provide for redundancy. For example a 2Tb NAS will contain 2 x 2Tb drives using RAID 1 for mirroring. This means that if one of the drives fails no data is lost.

Hard drives also provide a greater degree of flexibility and scalability than tape drives. It is generally a simple job to add a new, larger hard drive, to a NAS or replace a USB drive with a larger version. If the maximum capacity of a tape drive is reached the only options are to span backups over several tapes (which can cause management problems) or to replace the whole tape drive and all tapes with higher capacity ones.

5. Software Options

There is a wide variety of backup software on the market. They generally fall into two categories:

1. Imaging software, e.g. ShadowProtect, Acronis True Image, Kaseya BUDR
2. File copy software, e.g. NT Backup, Symantic Backup Exec

Imaging software creates a complete image of the hard drive being backed-up, this includes all program files, windows settings and data. Disk images can be mounted like a hard drive when required (useful for getting back a file when needed) and they can also be used for a bare-metal recovery – that is where the original hardware needs to be completely replaced and you are starting with an empty system. In the case of Kaseya BUDR and ShadowProtect this bare-metal recovery can be carried out on non-matching hardware, i.e. it does not matter if the original image was of an HP system and the new one is a Dell – the recovery will still work.

Imaging software requires hard drives for the backup media – they generally do not work with tape drives.

File copy software creates a copy of the data and can be set to copy everything on the hard drive or just a few data folders. This type of software is generally used with tape drives but can also be used with hard drive backup hardware. The stored data is a copy in the same structure as the original and can be brought back at any time following a disaster. Generally such backups do not allow for a bare-metal recovery but can be copied back once the new system is up and running. Also file copy software does not allow for hardware independent recovery.

6. Summary

Every business from small 'one-man bands' to multinationals need a Business Continuity Plan to ensure that they will be able to carry on after a disaster – no matter how small or large that disaster is.

The plan should include:

1. A business risk assessment
2. An impact analysis
3. IT system summary
4. Backup and recovery plan for critical data
5. Recovery/replacement plan for critical plant/equipment

Get Ready – Get Through!

7. Further Reading

WikiHow: How to Create a Business Continuity Plan

<http://www.wikihow.com/Create-a-Business-Continuity-Plan>

Best Practices in Business Continuity – AT&T Best Practices

<http://www.continuitycentral.com/bestpractices.pdf>

Best Practices: Backup and Recovery Strategies – CA

http://ca.com/files/whitepapers/backup_recov_wp.pdf

Business Continuity Institute

<http://www.thebci.org/>