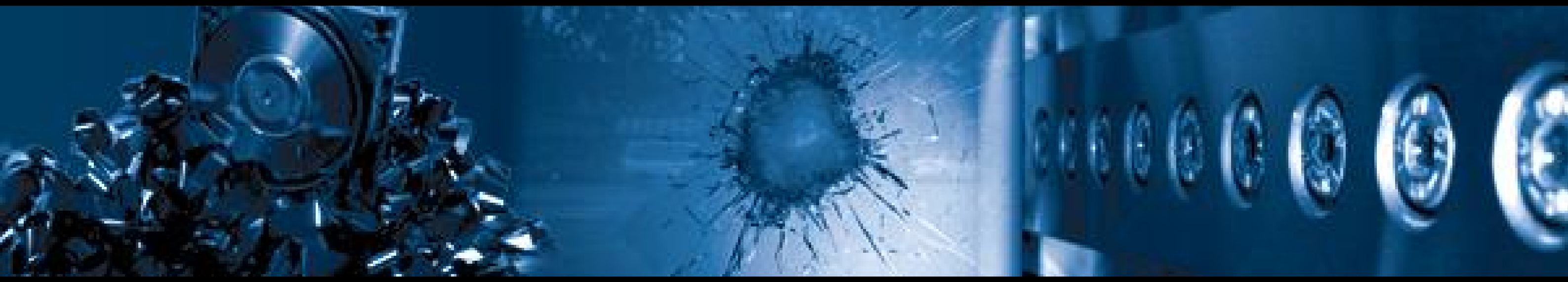
Success Blueprint

The 7 critical steps to...

A BULLET-PROOF BACKUP SYSTEM



“This is your definitive guide on how to avoid being a statistic”

***43 %** of companies that experience a severe data loss disaster, and that have no recovery plan in place, never re-open.*

***70 %** of companies that suffer serious data loss go out of business within 12 months.*

*Loss of data cost US businesses in excess of **22 billion dollars** in 2004.*

Cortex I.T.

Introduction

Imagine this - you arrive one morning to find that a faulty read-write head has crashed your server's hard disk overnight, rendering it useless. Or a small electrical fire has destroyed part of your office, including your server. This server was used to store customer lists, payroll details, accounting details, purchase orders, inventories and other data vital to the running of your business, built up after years of operation and growth.

You find that you were seriously ill-prepared to deal with such a disaster. Virtually all of your business' data had resided in this one location. No copies were made. You are faced with the fact that many years' worth of data has been lost forever.

Insurance will replace materials, equipment and office space, but will that be enough to get your business up and running again? Your vital business data can't be claimed on insurance and it can't be replaced with money alone. Would your business survive after significant data loss? Unless you have a good backup system already in place, the statistics are grim. Just as the costs of fire damage can't be covered by insurance bought after the event, the costs of data loss can't be avoided by acting after the loss has occurred. It is vitally important that data is backed up before encountering hard disk failure, viruses, malicious software, mistakes by employees or other causes of lost data.

It takes 19 days and costs US$17,000 to manually retype 20 megabytes of sales data. The same volume of accounting data takes 21 days and costs US$19,000.

The 7 critical steps essential for the protection of important data...

1. Central storage of data on the network

The first step in setting up a backup system is deciding what needs to be backed up. Ask yourself, what can I afford to lose? For example, the latest Windows Service pack can be downloaded again, so there is little need to protect it; your customer database cannot so easily be replaced. Once you have identified the information you need to back up, you need to know where it is stored. Although it might seem counter-intuitive at first, as much of your critical data as possible should reside in one place on the network. It is far simpler and easier to backup, restore and protect one machine than several. As a side benefit, physical and network access to that machine (and therefore to critical and perhaps sensitive data) can more easily be restricted, improving security.

2. Multiple backups

You don't want to have all your eggs in one basket. There are many reasons why your company should have access to several full system backups.

- A single backup could fail. Tapes, CDs and hard drives all wear out eventually, so you shouldn't rely 100% on a single backup to store your data. The more copies you have, the less likely you are to lose all of your data to wear, fire damage, water damage, etc.
- In the case of accidental deletion, most people only notice data loss days after it occured, which means that if your only backup is from last night, you have no way of retrieving the data.
- Restoring files that were deliberately deleted months or even years ago, when you thought you would never need them again, can often be of great benefit.

The 7 critical steps essential for the protection of important data (cont)...

3. Off-site backups

If your office burns down, you don't want all your backups to burn with it, so it's important to physically move some of your backups off-site. We recommend that any weekly, monthly, quarterly and yearly backups are stored off-site at a secure location.

4. On-site backups

While it is important to have some backups off-site, you don't want to have to travel back and forth whenever you need to retrieve a file. For this reason it's useful to have recent daily backups available on-site to allow for quick recovery of files. These backups are still important, and for reasons of security and reliability it is best to store them in a secure place such as a fireproof safe, rather than next to the server or on the System Administrator’s desk.

5. Monitoring

If you need to restore a file or a whole system, you want to be sure that all backups completely successfully. It would be disastrous to learn that your backups had failed only when you attempt to perform a restoration. One way to ensure that each backup has been performed successfully is to check the backup logs each day. An easier method is to acquire backup software that notifies you daily of the backup status and can alert you to any problems.

6. Follow the plan

If you are using tapes, disks or removable hard drives for backing up, you will need to remember to change these regularly depending on the backup scheme you are using. Neglecting to do this could cause the backup to fail or could result in an important previous backup being overwritten. It is also important that you insert the right device, as having the 4th-of-June backup data on the 1st-of-January tape would make the right data very difficult to find.

7. Regular file list updating

As you install new programs, add hard drives and create new files, it is important to know that all new data is also protected. Of course, if you are backing up the whole C: drive, for example, any new files or programs on that drive will also be backed up automatically. However, if you are only backing up specific, important files, it is vital that you keep this list up to date, or you risk losing valuable data.

How do you ensure that you have a BULLET-PROOF BACKUP SYSTEM?

Keep in mind that the average failure rate of a hard disk is 100%, as every drive will fail eventually. Make sure you stay in business by following the seven points listed above.

How do you do that? Well, that's where a backup program such as **BackupAssist™** can help. Data protection need not require a full time IT professional; it can be done by almost anyone with a bare minimum of time to spare - all you need is the right tool. An application such as BackupAssist™ can automate much of the process, and also provide an easy-to-use interface for setup and maintainence.

BackupAssist™ implements industry standard schemes that allow you to schedule daily backups that can remain on-site, and weekly, monthly and yearly backups that can be stored offsite. BackupAssist™ will verify the accuracy of each backup and notify you of successes and failures via email, so you also know when problems arise. This simple-to-use program will also email you or your secretary/office assistant with a reminder to insert a new tape, drive or disk, to minimize the chance of human errors hindering your backup scheme. With steps two to six covered by BackupAssist™, protecting your data is a breeze.

Success Blueprint

The 7 critical steps to...

A BULLET-PROOF BACKUP SYSTEM

BackupAssist™ Windows® Backup Made Easy!

Cortex I.T.

Level 4, Whitehorse Tower
991, Whitehorse Road
Box Hill 3128
Victoria
Australia

p: +61 3 9899 4681
f: +61 3 8080 1606

w: www.BackupAssist.com
e: sales@BackupAssist.com
e: support@BackupAssist.com