Disaster Recovery and the Home User

Introduction

This white-paper provides the reader with an overview of the problems and risks faced by the home-user when protecting important information and will show how the Cobar™ product suite addresses those issues.

Why do I need it? What are the risks?

If you are like the majority of users, the digital age is impacting your home. The digital revolution is bringing you many benefits, the most common being email messaging, digital photos and other multimedia. Many homes now include a personal computer that is used to access the Internet and for home-office/work use.

If you are like most of us, it is not until you have lost everything at least once that you begin to understand the importance of having your valuable information backed-up securely. Many home computer users are oblivious of the significant risks to their information, including:

- Equipment failure – hard-disk, media
- Natural disasters – fire, flood, earthquake etc
- Theft of equipment and media
- Loss of data due to virus and/or user error

Generally, the biggest impact is the loss of irreplaceable information such as digital photos and home movies but many uses will feel a significant impact due to the loss of unique works such as university assignments, business proposals, client lists, PIN numbers and access codes, home inventory data and even email archives.

When disaster strikes, it tends to strike at the worst time and often in the worst way. How much important information or memories would you lose if your home burnt to the ground today? What if you have important assignments or business proposals that are due by Friday?

Traditional approaches

It is pretty clear that some sort of protection is required against these risks. While there are sophisticated backup solutions used by large organisations, they are out of the range of the home user. On a limited budget and without giving the issues too much thought, the home user may try one or more of the following schemes:

Scheme #1	Important files are saved to CD-R / DVD-R / USB key
Scheme #2	Important files are saved to another computer

The most significant failings with these schemes are:

- The user must manually burn the files to CD or copy them to another media / computer. Users, even sophisticated IT professionals, will not keep the backups up-to-date if it requires them to do it manually each time.
- The information is not secured. Generally, the information that is important to you is also personal and private information. Would you be happy if someone found your USB-key with all of your personal and private information on it?
- The processes for archiving information offsite are often beyond the capabilities of the home-user.
- If the backed-up information is not stored offsite then you still risk losing it all to fires, floods, theft etc.
- USB Keys are often misplaced, or occasionally fail, resulting in the loss of any of the valuable backed-up information.

To be successful, a backup or disaster recovery scheme must have the following characteristics:

- ✓ *It must be automated.*
- ✓ *It must be off-site.*
- ✓ *It must be secure.*
- ✓ *It must be simple.*
- ✓ *It must be affordable*

Why security and what flavour?

The information that you consider important enough to take measures to ensure that you don't lose, is also generally sensitive and private information. You will want to ensure that only you (or those that you authorise) can 'read' or 'view' the information that you store.

There are a number of products that advertise themselves as 'secure' offsite storage but they fail the 'security' test on a number of fronts:

- Your information is securely transmitted to the storage site but then stored with little or no protection.
- If it is secured, then often only a simple login username and password is required to access your data.

These failing mean that the people that are paid to provide you with secure storage have access to your personal and private information. Even if you form a good impression of the storage provider's ethics, consider if the storage is through an outsource provider in a foreign country where personal information may be bought and sold as a commodity?

> *The only way to ensure that your sensitive information remains private is to make sure that no-one can access it once it leaves your computer.*
>
> *If it isn't encrypted before it leaves your computer, then unauthorised people may be able to access your private information.*

Encryption is a process that converts information into a form that no-one else can 'read' unless the reader has a 'key' to the information. 'Strong' encryption methods exist that allow you to keep your information secure – even from corporations with super-computers at their disposal. These methods have been mathematically analysed for weaknesses over many years to 'prove' that they maintain your privacy.

So, it becomes clear, that in order to maintain your privacy while also ensuring that you don't lose important information:

> *You must use strong encryption to protect your information before it leaves your computer.*

Because you are now the only one that has a 'key' to your protected information, it really doesn't matter a lot that someone else may have access to it. If they cannot 'read' the information then it is of no use to them! All you have to do is to ensure that the 'key' remains private.

Cobar™ - Secure Online Data Storage

The Cobar™ suite of products has been designed and developed to address the shortfalls in the existing systems for storing your valuable information. The Cobar™ product suite, when combined with the provision of online storage, is the disaster recovery solution for home users and small business.

The Cobar™ product suite meets the essential criteria for a backup and disaster recover scheme that is suitable for home and small business users:

- ✓ **Automated**. Cobar™ Backup allows you to identify the files and folders that contain important information and *automatically* secure and copy them to an online storage location.
- ✓ **Off-site.** Cobar™ products are linked with online storage providers to ensure that 'your eggs are not all in one basket'.
- ✓ **Secure**. Cobar™ products use strong commercial grades of encryption such as AES and Blowfish to encrypt your information before it leaves your computer.
- ✓ **Simple.** Cobar™ has been designed from the ground up to be very easy to use. Field trials have shown that average users can install and use the product within 2 minutes of downloading Cobar™ software.

  Cobar™ provides a familiar 'Explorer' style of interface featuring drag & drop, combined with extensive use of guiding 'wizards' to ensure that less experienced users are not overwhelmed.
- ✓ **Affordable.** The Cobar™ product range, whether bundled with online storage or bought outright, are attractively priced to be easily within reach of those on a tight budget.

CapstoneBlack

CapstoneBlack is a solutions development company established to develop and support innovative applications with a focus on secure communications and storage products.

The CapstoneBlack head-office is located in Canberra, Australia:

Website	http://www.capstoneblack.com
Email	info@capstoneblack.com
Phone	+61 (0)2 6258-0181
Fax	+61 (0)2 6292-1568
Mail	GPO Box 2387 Canberra ACT 2601 AUSTRALIA