

# Disaster Recovery and Small Business

## Introduction

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

## Business Data

Most businesses have now become reliant on computers and digital data for their operation. Loss of the business data can have disastrous consequences with typical small businesses not being able to operate if important information is lost, for example:

- Customer, billing and stock databases
- Accounting databases – wages, taxation
- Online presence – web pages and databases
- Access logons for suppliers, banking etc
- Business templates – invoices, contracts, orders etc

Even if some of this information can be rebuilt, your business may be out of action for many days and affected for months afterwards.

## What are the risks?

There are many common sources of risk to your business 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

When disaster strikes, it tends to strike at the worst time and often in the worst way. How much important information would you lose if your computer equipment was stolen today? You could buy a new computer, but what then?

## 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 average small business.

On a limited budget and without giving the issues too much thought, the business owner 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 properly secured. Generally, the information that is important to your business is also of interest to others that don't have your best interest at heart. Would your customers be happy if someone found your USB-key containing customer details including credit card information on it?
- The procedures for archiving information offsite are often beyond the capabilities of the average small business operator.
- 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 and eventually fail, resulting in the loss 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 online. Your business may be liable to litigation if your customer's trusted information becomes compromised; at the very least, your business reputation will suffer.

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 your business with secure storage may have access to your confidential business 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 and business information may be bought and sold as a commodity?

*The only way to ensure that your sensitive business 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 protect your important business information whilst ensuring that it remains private:

*You must use strong encryption to protect your business 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 business information. The Cobar™ product suite, when combined with the provision of online storage, is the ideal backup and disaster recovery solution for small businesses.

The Cobar™ product suite meets all of the essential criteria for a backup and disaster recovery scheme that is suitable for 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 you are not vulnerable to common disasters.
- ✓ **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.
- ✓ **Compression.** Cobar™ products automatically compress your information so that it takes less time to upload and uses less space in your online storage. Databases can typically be compressed to less than 10% of their original size. Compression ultimately saves you money.

## Additional Considerations

While Cobar™ will protect your business from loss of important information, the following additional security vulnerabilities need to be addressed by the small business owner:

- ✓ Files can be accessible on the local computer systems – if a computer is stolen or lost then your information may be vulnerable.
- ✓ There are Trojans and viruses that have been designed to steal your personal information such as logins for services like online-banking and credit card details.

You must ensure that you are also protected from these vulnerabilities. Suggested preventative measures include:

- ✓ Local encryption of sensitive information.
- ✓ You must have an up-to-date virus scanner installed and running.
- ✓ You should seriously consider keeping up-to-date with operating systems vulnerability patches through the Windows Update service.
- ✓ Your computer systems must be fire-walled from the Internet.

## 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	<a href="http://www.capstoneblack.com">http://www.capstoneblack.com</a>
Email	<a href="mailto:info@capstoneblack.com">info@capstoneblack.com</a>
Phone	+61 (0)2 6258-0181
Fax	+61 (0)2 6292-1568
Mail	GPO Box 2387 Canberra ACT 2601 AUSTRALIA

Cobar™ is a Trade Mark of CapstoneBlack Pty Ltd