Table of Contents

1 Backups 1
1.1 Why do backups 1
1.2 When to do backups 1
1.3 Where to store backups 1
1.4 How to create backups 2
2 Planning your backup strategy 3
2.1 Know your software 3
2.2 Organize your filesystem 3
2.3 Understand the volatility of your data 4
2.4 Ask when you might want to restore 4
2.5 Review your hardware requirements 4
2.6 Make a plan 5
3 Some software options 5
3.1 Acronis TrueImage 5
3.2 Nero BackItUp 5
3.3 Symantec Norton Ghost 5
3.4 Synctoy 6
3.5 GoodSync 6
3.6 OopsBackup 6
3.7 Backup4All Pro 6
3.8 AJC Active Backup 7
3.9 Western Digital My Passport Series Hard drive 7
3.10 IDrive 7
3.11 IDrive Portable 8
3.12 FreeOTFE 8
3.13 Choose your software 8
3.14 Cost your backup strategy – is the effort and cost worth it 8
4 A case study 9
4.1 On-site backups 9
4.1.1 Duplicate synchronized copies - SyncToy 9
4.1.2 Backup versions on external hardware - OopsBackup 9
4.1.3 Immediate versions of changing open files – AJC Active Backup 9
4.2 Off-site online backups - IDrive 9
4.3 Risk assessment 10
5 Configuring OopsBackup 10

Copywrite - Ken Wakefield

5.1 First 10
5.2 Catering for Volatile data 10
5.2.1 Change the frequency at which backups are taken 10
5.2.2 Change the file size & time frame for which Deltas are taken 11
5.2.3 Invoke automatic purging for large files 11
5.2.4 Invoke the use of Windows Shadow Copy for opened files 12

Copywrite - Ken Wakefield

1 Backups

1.1 Why do backups

There is something wrong with the computer, and you seem to be having trouble opening some documents, and what is that, the hard drive seems to be making more noise than it used to.

Or you are half way through the day in a small retail business environment when the disc suddenly crashes after you've entered one or two hundred cash sales. Or maybe you're an author and having just got over writers block and poured out the creative juices all morning……BOOM! What good is a nightly sync copy going to be to you now?

Suddenly you can't get at all your files, and finally you can't even start the computer. What a nightmare.

Yes, you've heard about backups and their importance, but being human, you never think your computer will crash. After all, it has been working fine without a missed beat for years now.

Not to mention that you have no idea really how to perform backups, and it costs money to buy backup software, and then which one would you buy anyway, there seems to be so many of them when you Google 'backup software', so it all went in the too hard basket, and now it looks like it's too late.

The computer is D E A D !

All the files are gone!!!!

1.2 When to do backups

You have to think about your usage of the computer, and design a backup strategy that suits that usage.

Yes, it is a bit of work, initially.

A backup strategy must provide for some fundamentals, such as a copy of your data, but is that enough?

The fine detail in this is down to how you work, what programs you use and how they work. It's all down to how much effort you'd have to redo to get from the last backup taken to where the file was when it was lost or corrupted, as well as do you have a backup copy at all.

If you are making changes regularly, such as entering cash sales and invoices as they arrive and the computer is on all day and the accounts program is running all day, you want frequent backups during the day. If you're a writer painfully and creatively structuring every single sentence as you write it, you want even more frequent copies taken during this process.

If on the other hand, you come home at night, have dinner and then sit down and enter the days expenses into your accounts and this takes 10 to 15 minutes, then you will only need a backup to be performed once a day.

If you are just storing pictures and video by the gallon each day, which aren't being then edited by photo software, then you probably only want to do a backup once a week especially if the pictures are still in the camera. However, doing one once a day spreads the load on the computer across the days of the week, and so the backup process has less of an impact on the normal performance of the computer. You need to take these sort of considerations into account as well.

1.3 Where to store backups

You have a workstation in the office running the accounts software all day, and have a laptop that you take home, so the backups are made to the laptop, a strategy which also offers some offsite protection. If the business is broken into overnight or the office burns down, You can start up the next morning straight away with the laptop.

Then one day you put the laptop on the car roof while you put an armload of stuff in the boot, hop in the car and drive home. Oops!, forgot about the Laptop on the roof!. Or it disappears from the passenger seat while you pop into the local store for milk and bread!! Oh well, we'll get a new one later in the week.

Copywrite. Ken Wakefield

That night, the paint shop next door burns the whole block down. Where's your data now, in some drugie's bedroom, down a storm drain, or in the ashes?

The bottom line is that backups need to be stored in two places, first on a separate storage device, i.e. another hard drive, and second, a building other than where the computer is located…the further away the better, i.e. off-site.

1.4 How to create backups

Backups are about three things:

1. Protecting your data from hardware failure, including hard drive crashes, lost or stolen equipment
2. Protecting against tragedy such as fire, or a jumbo jet crashing onto the office destroying ALL hardware and data on site
3. Protecting against human or software error, where for one reason or another you need to go back to a point of time in the past, undoing recent work performed that was incorrectly done or not done satisfactorily, or restoring a very recent version to overcome a corrupted file situation.

To achieve this requires more than just a photo copy of the PC's files onto an external hard drive done once a night.

A good backup strategy needs versioning, offsite storage of backups as well as synchronized copying to another piece of hardware and different files being covered by differing backup frequencies.

Versioning is where previous copies of changed files are not just overwritten with the changed file, but where the new version of the file is somehow stored in addition to the old version within the backup, and you can therefore go back and get (restore) either of the versions which are copies of the data from different points in time. Versioning gives you protection against file corruptions, or human errors because it allows you to go back in time.

Offsite means taking those copies to another location such as home, a bank vault, or an on-line storage that is itself backed up safely by an on-line storage service provider. Off site copies protects you from tragic events like fire.

Synchronized copying gives you the easiest and quickest access to your data in the event of dramatic hardware failure or loss.

Then you will want to take a version of your word documents every time you hit the save button, or the accounts files every 10 minutes, but that big email file may only need backing up every hour, or even only once every day.

A good strategy requires software to do it for you, and it should do it seamlessly with as little human intervention as possible.

Choosing the right backup program is a key factor in success. You may have to put together a couple of tools, but once configured, a good working backup process should then never have to be touched again till it is needed to restore a file.

Now a note here about on-line offsite storage. This is very dependent on internet connection speed.

It is certainly not an option over dialup. It is also highly unlikely to be a solution without managed refinements with ADSL 1, where we have different upload and download speeds, and uploading is much slower. So if you're in Australia, and you're in the country, this is impossibly slow, and can only be achieved with very limited amounts of data. Offsite storage is probably only going to be achieved by physical transportation

copywrite - Ken Wakefield

2 Planning your backup strategy

2.1 Know your software

It is important to understand the programs you use in terms of:

- what files they keep to hold your data, and
- whether those files are still accessible to a backup program when it opens them.

For example, you use Quicken, and when you start the Quicken program and select File->Open, you select a file such as MyAccounts.QDF

You must use Windows Explorer to look at the files stored on the computer. You will see that in fact, there are many files stored with the name MyAccounts but of different types (file extensions). There's a QDF, a QCN, a QPH and so on, so in fact to backup the Quicken file, you have to backup all these files and there might be 7 or 8 of them depending on the version of Quicken and the features you use, plus they all need to be copied at the exact same point in time.

Let's take another example. You are creating your own on-line shopping website using ShopFactory. You start the ShopFactory program and create a new website called MyShop.

Again, use Windows Explorer to look at the files stored on the computer. You see in fact that ShopFactory creates a folder called MyShop to hold the files it uses to build your website, and under it there are other subfolders and all up in excess of 750 files associated with what the software presents to you through it's screens, as one file called MyShop.

You would never keep track of all these files individually, so it's important that if you want to be able to rollback to a past point in time, your backup software allows you to easily restore all files as at a time in the past and effectively retrieves the latest version of every file as at that point in time for you.

You must know what files your software keeps and know where it stores them.

Secondly, it's important to understand that some programs works differently with different types of files.

When a program opens a file, it may do so in such a way that other programs, like backup programs, cannot open it at the same time, and therefore cannot take a copy at the time specified to create a backup. In this case, the backup program will not be able to take a copy until the original program, that is Quicken or ShopFactory, is exited and releases its files so other programs can then use them. Also, where there are a large number of files that must be copied as at a specific time, something must ensure that they are all copied at that same time.

Some backup programs get over these issues by using a technology called *Windows Shadow Copy*. This is very complicated technology within the windows operating system so many backup programs do not use it.

A good backup program will allow you to use Windows Shadow Copy, but use it selectively for files that will probably be opened when you definitely want to have a backup copy taken because you run programs that lock their files for long periods of time or manage a large number of files simultaneously.

Whether you need this facility or not is your choice, and paramount in choosing a backup software product for your needs. Do you sit at the computer hours at a time building a website or writing a word document, or does your accounts program run all day and never close till the end of the day?

2.2 Organize your filesystem

To make configuring backups and restoration easy, you must have a well organized filesystem.

Not all programs apply the same principles in deciding where to store files.

Generally when you ask a program to create a new file, the standard is to initially offer 'My Documents' as the location to store the file to be created, but some older software like older versions of Quicken, offer some fairly varied alternatives.

Copywrite - Ken Wakefield

But this is not enough. NO file should ever be just stored directly under 'My Documents'. Imagine the mess if every tool in the shed was all just put on the top of the work bench. (Oh My! I can hear the laughter from here, yes it might be easy if you are very familiar with every tool, are you that familiar with every file on your computer?)

First, if the program has not created a program related subfolder under 'My Documents', create one. ShopFactory does this nicely, it creates the folder 'ShopFactory V8 Websites' under 'My Documents' and offers this folder as the location for all newly created ShopFactory projects.

Quicken on the other hand does not. It is recommended that under 'My Documents', you create a subfolder called Quicken and store all Quicken files under here. If you are keeping books for multiple clients, you may create further subfolders under that Quicken subfolder, for each individual clients files.

This organization of your filesystem means that you can easily locate data related to certain programs and projects, and moreover, subject to similar usage. Now you will be able to easily configure you backup program to treat program related folders appropriately according to the way those programs work and the way you use them.

With this knowledge and organization of your filesystem, you will know where to find backups which will be stored in a similar structure, and also where to restore them to if a restore is required.

Knowledge of your filesystem is paramount. Learn how to navigate your filesystem.

2.3 Understand the volatility of your data

You need to work out what files are changing..

- during the day
- every day
- only occasionally
- rarely
- never after being stored

to configure your backup software for the best performance. If you've organized your filesystem as recommended, you should have volatile data in different folders to large amounts of non volatile data.

2.4 Ask when you might want to restore

The important question here is whether your activity on the computer might require you to be able to go back and recover a file / files as at some specific point in time during the period you were working with a program like an accounts program, as opposed to yesterday, the day before that, etc.

In other words, consider you are building a website or writing a very long word document and you are sitting at the computer all day. Suddenly you have a light bulb event, and realize the changes you've made over the last hour are crap!, or the software simply crashes and corrupts the file.

Do you think there might be occasions when you might want to be able to reverse an hours work, and go back to the way the file was an hour ago?

If the answer is yes, then for these types of files need more frequent backing up and need a backup program that can take a copy while you are working with the file open, if the program locks its files.

If you only work for short periods and are happy for a backup to occur after you have closed the program you were using, then there are a wider range of backup programs and tools available to you.

2.5 Review your hardware requirements

All backups require an external drive whether it be a pocket sized portable USB drive, massive desktop storage or another computer.

If it is another computer, be aware that that computer will have to be switched on all the time you are working on the first computer, or backups will not occur.

Copywrite - Ken Wakefield

If you are going to get an external hard drive, for backup purposes it does not have to be the latest SATA / RAID technology, but needs to be reliable, and needs to have power saving features so that it powers itself down when your computer is turned off.

For personal computers rather than multi networked computer environments in a small business, you are better off with a USB drive that is powered via the USB cable and therefore comes on and is turned off, with your computer and is relatively power efficient and does not require its own power supply. It is also easily disconnected and carried with you as an option for satisfying offsite storage requirements to some degree.

2.6 Make a plan

Sit down with pen and paper, and draw a diagram representing your backup strategy, and ask whether you can be bothered unplugging the USB drive and taking it with you when you leave the house.

Decide what is practical and what is not, and make sure the plan will work seamlessly and not be inconvenient because if it has any inconvenience, it will inevitably fail.

Do this before you look at backup program options.

Now read the next chapter on some different programs available, what they can do and offer, then review your plan and enter into it what programs you will use to achieve each part of it. You can also research the internet for additional options.

3 Some software options

3.1 Acronis TrueImage

Licence – Commercial, about $US 50

Acronis TrueImage is a highly regarded and published software package, which includes a module called NonStop backup

It really is a disk management and system recovery tool for disk imaging needs as opposed to a data backup tool, although Acronis would deny this categorization.

NonStop provides Versioning based on 5 minute time intervals, but does NOT use Windows Shadow Copying and requires the Acronis product to be installed to recover files from the backup repository. Acronis disk imaging does use Windows Shadow Copy, but this is a very difficult medium to work with.

I personally found it problematic and would not recommend it at all, despite its prominence in reviews on the internat.

3.2 Nero BackItUp

Licence – Commercial, about $US 50

A very neat and simple interface, but not really supported by quality support. I found it had a number of problems, and did not use Windows Shadow Copy. I also felt that it had sociability problems with other software on my PC, and would not recommend it.

3.3 Symantec Norton Ghost

Licence – Commercial, about $US 80

A competitor for Acronis TrueImage, and the original of its type. It is again really a disk imaging and system recovery product rather than a data backup product

Despite the media, not recommended for our purposes.

Copywrite - Ken Wakefield

3.4 Synctoy

Licence – Free

SyncToy is a free program from within Microsoft, written and available free from Microsoft downloads, and is designed to synchronize two folders, and does so very efficiently.

Synchronizing two folders means it looks at the files/folders in each of the folders being synchronized, and copies from one to the other as required to make them the same, i.e. replicate changes in one to the other.

This is often used to align the versions of the same files that are updated on both a desktop computer, and a laptop computer when the operator is mobile, however it offers three type of synchronization, two being 'Echo' and 'Contribute' which operate only in one direction.

Using it in 'Echo' or 'Contribute' mode therefore effectively achieve a copy and as such can be used as a primitive backup solution where synchronized copying only is an acceptable solution. A disadvantage is it must be run manually by the average user.

3.5 GoodSync

Licence – commercial, about $US30

A very comprehensive synchronization tool with considerable automation

3.6 OopsBackup

Licence – commercial, about $US40

A solution that offers automation, Versioning, Windows Shadow Copy, and even without the program, the latest and some historical versions can be retrieved with just Windows Explorer.

It has been developed to be efficient and not degrade the performance of the computer on which it is running and so is not full of fancy options, but powerful with what it has. As such, it has a simple and intuitive interface.

In fact its simplicity is one of it's main features. Just about anyone should be able to setup and run OopsBackup, because it is so simple. OopsBackup can be operational very quickly, or can be configured to achieve the backup needs of continually operating software like Quicken and ShopFactory, with very little effort and configuration.

It watches file related events on your computer and then copies the latest version at the scheduled time. The schedule automatically slides if the computer is not on at the time of the next scheduled backup, so backups are never missed.

It does not require setting up different backup jobs for Full, Differential and Incremental backups and timing these to interact appropriately or understanding these and their impact. Oops backup has it's own differential methodology called Reverse Deltas, and applies these automatically in order to save space in the backup repository as it provides for the restoration of older versions.

For the Home or small business user, this program is highly recommended

3.7 Backup4All Pro

Licence – commercial, about $US50

Been around a while and is a comprehensive and well supported product. Comes in various versions, Pro being the 'have everything' version, and at the cost difference, would only get the top level version as it includes encryption and incremental backups.

This is a very good program and has all the bells and whistles. However it is much more difficult for the uninitiated to set up and run.

It has compression, encryption, Windows Shadow Copy (Backup Open Files) and scheduling. It creates and runs backup jobs, each being one of the familiar Full, differential or Incremental type of backup,

Copyright - Ken Wakefield

which are scheduled to run at specific times rather than watching your activity and backing up files as you change them.

There are no negatives for this product, other than it's complexity for the uninitiated and the effort required to set up backup jobs. If you use compression and encryption though, it will be very slow.

3.8 AJC Active Backup

Licence – commercial, about $US30

This is a very neat little program, but it is architecturally archaic.

It has the advantage that it takes a backup version as soon as a file is saved (provided windows shadow copy is not needed) or closed rather than at a preconfigured time.

It does not use Windows Shadow Copy, but then this is not needed for all programs. Windows Shadow Copy is not needed to backup a copy of an opened Word document for instance. AJC will take a backup copy every time you hit the save button while editing a word or excel or text document.

I wouldn't suggest this product as a full backup strategy as its future is uncertain at the moment and there are some things it cannot achieve which programs like OopsBackup can, but it's a good model of the sort of 'watching' backup program as opposed to 'time slice' backups.

However, I'd certainly recommend it as a good adjunct to OopsBackup for users who spend most of their day writing documents with Word, or developing Excel spreadsheets, as it will keep versions of these as at saves between OopsBackup Scheduled backups, and can then be set to purge these in a couple of days when the documents will then be covered by OopsBackup scheduled backups.

You really don't want your main backup software saving for prosperity 100's of versions taken every time you hit the save button, but having these versions taken and saved for a couple of days by AJC Active Backup as you work can be really handy in case of software glitches and crashes for example.

3.9 Western Digital My Passport Series Hard drive

This is a hardware option. However, it comes with integrated backup software and password locked encryption.

These products offers you an easy way to have an encrypted portable USB drive which is also security in case of stolen hardware, if security is an important issue.

The Western Digital backup software called Smartware does versioning, but does not use Windows Shadow Copy, but it does watch your computer as you work, and takes backup copies as you close a file.

The 'Editor' suggests this is worth considering if you have to buy an external hard drive to implement your backup strategy as backup software and encryption are included, but it may be an inflexible solution for more general needs.

What's more, if you have a home network with multiple computers on it and an Ethernet router (ADSL modem with multiple Ethernet ports), there is a 'World' version of the passport series that can plug into the modem and be available when any computer on the network is turned on, and will automatically back them all up.

3.10 IDrive

Licence – Free for the basic account which allows 2GB storage – more than enough for ADSL 1 connection.

IDrive is an online backup service provider in the USA, and remarkably offers a free account option for storage of up to 2GB. Over that you can have up to 150GB for $US 5.00 per month.

I find it very useful for backing up a limited set of extremely important files, and after the initial backup which took 4-5 hours to load 400MB, now updates that repository in 3-10 minutes. This would not change much if I could upload my other 130GB as most of it is pictures and video which will never be changed, but I can't upload it with my broadband limitations.

Copywrite - Ken Wakefield

However, they have an interesting concept called IDrive Portable, see following paragraph, which as well as offering a way around this problem, the free program used can be downloaded and installed on any external hard drive, and so could be considered in lieu of OopsBackup.

IDrive and IDrive Portable offer Windows Shadow Copy, limited versioning, and limited scheduling. They only store up to a specific number of versions but do use incremental backup technology for storage efficiency, but this is suitable for most purposes.

Go to www.idrive.com and create an account, download the program. It can be scheduled to run automatically at certain times, but not more often than once per day. I have it running at 3am, and have a TV card to ensure the computer starts up and is ready at 3am for the program to run. The program is configured to shutdown after an automatic backup, and so the computer is back off by 3:10am

Why a TV card? Because Windows itself can only wake a computer from standby or hibernate, but the hardware PCI TV card can wake the computer from a cold boot to make a scheduled TV recording. You can see here some of the other issues that can come into play in activating a good and seamless backup strategy

3.11 IDrive Portable

Licence – Free but is based on the purchase of an external HD from them, but can be used on any external HD

This is an additional product from IDrive, that is meant to allow you to first backup to a portable USB drive, which you then mail to them and they copy the files to your online repository, thus getting around the limitations of your broadband quota and speed.

It can also be used in the reverse direction to get your files back.

The advantage is that you know your files are forever safe, but you pay the monthly fee to store them.

However you can still download the program and use it on any local external hard drive you have, and may provide a free strategy, but as such would be totally unsupported. It is limited in scheduling and versioning and automation, but does provide encryption so your data is safe from exposure if the USB portable drive is stolen, which OopsBackup does not at this stage.

3.12 FreeOTFE

Licence – Free

For a description, please see www.freeotfe.org

Basically, this allows you to prepare and use a portable storage device like a USB drive or memory stick, so that it is then password protected and all data is encrypted.

You could use this with OopsBackup at the moment to get around that products lack of encryption.

This could be an important issue if carrying sensitive information around on a portable drive as part of your off-site strategy.

It does however require time and skills, and takes some hours to prepare the drive before use. It's not for the average person.

However, if password protection and encryption of your portable drive is a significant issue, I'd recommend you look at purchasing a portable USB drive from Western Digital, whose My Passport range of external drives now come configured for just this purpose with it's own Backup Software solution.

3.13 Choose your software

Go back now to the plan we discussed in '2.6 Make a plan' and add your software selections to achieve it.

3.14 Cost your backup strategy – is the effort and cost worth it

Only you can answer this, go back and review Chapter 1 and ask yourself this question again.

Copywrite - Ken Wakefield

4 A case study

4.1 On-site backups

I have two USB external hard drives, one 1TB desktop drive, and another 160MB portable drive. The portable drive has been prepared and encrypted using FreeOTFE so it is password protected and safe from prying eyes, and can be easily unplugged and taken with me in the brief case.

4.1.1 Duplicate synchronized copies - SyncToy

I use the free SyncToy to daily update synchronized copies of all files on my data drives to both the ITB desktop storage also used by OopsBackup, and a portable USB drive which can be disconnected and taken with me as part of offsite storage. This synchronized copy using SyncToy is done at 2:32 am in the morning while I am asleep by using a SyncToy commandline utility that is run as a windows scheduled task.

This synchronized copy adds simple duplicity for added insurance plus a portable copy for protection against tragic events.

If I am going away for an 'at risk' period, I just unplug the portable drive and take it with me in the brief case. This portable drive has been prepared with FreeOTFE and so is encrypted and password protected.

4.1.2 Backup versions on external hardware - OopsBackup

The 1TB external drive permanently attached to the computer holds an OopsBackup archive in addition to a SyncToy copy. All data drives are backed up to it as well using OopsBackup.

OopsBackup backs up different folders at different frequencies chosen according to their usage, with some using Window Shadow Copy depending on the programs using the files. Historical versions allow the restoration of versions of the files from points in the past. It is configured to use Windows Shadow Copy on Quicken and Outlook files.

This achieves hardware failure and human error protection with synchronized copying and versioning for the restoration of files from timelines in the past.

The chosen software has automation features that both ensure backups are always taken even if the PC has been turned off, and mean that no human intervention is required at anytime once configured.

4.1.3 Immediate versions of changing open files – AJC Active Backup

One computer on the network is predominantly used with Microsoft Word. AJC Active Backup watches these documents as they are edited, and takes a copy each time the Save button is selected, or the document is closed.

Given the intensive activity with document development with word, this extra protection has been installed on that machine against software and human 'glitches'.

4.2 Off-site online backups - IDrive

My computer is woken up again at 3:30 and at 3:32, IDrive updates the online repository with changed sensitive files. It takes approx 4-10 minutes across a 1500/256 ADSL 1 connection. The computer shuts down again on completion of the online backup, the results of which are logged in an email to me as part of the backup.

This provides off-site protection in addition to the portable USB drive. It is however limited because of the broadband bandwidth, and therefore does not cover all files on the computer.

Copywrite - Ken Wakefield

4.3 Risk assessment

The biggest at risk element of this strategy, is total destruction by tragedy of both external drives, while both on site.

The solution is to use IDrive via its IDrive Portable product at $US65 for one of their portable drives and $US5 per month for the storage.

Alternatively I could just buy a second portable USB drive locally, and use it one night for the duplication process, and post it to parents or children to put in their bottom draw till needed, swapping with the one being used nightly every now and again.

5 Configuring OopsBackup

5.1 First

The simple approach is to install the program and accept the default settings and run with that.

Default settings will in general be suitable for the majority of cases, and therefore will continue to cover the majority of all backups.

The default settings are fine for all non-volatile data, it's only when you have volatile data that you might need to do more.

If you don't feel you are up to considering the issues any further and refining settings for specific cases and creating special folders, then just run with the defaults. You will not be at risk of not being covered by backups, but some situations may grow your backup repository faster than it could be configured to do so, or you may find some backups occur later than you thought.

But the program will work, and you will be covered for 99.5% of restoration needs of the average user, and the other 0.5% will not cause the average user any real problems.

The only recommendation is to buy as big a capacity portable external drive that you can afford. Storage is fairly cheap these days.

5.2 Catering for Volatile data

Volatile data is files that are changed frequently and/or kept open for long periods by the programs you use. This means files that may be changed continually throughout the day, or just changed regularly on a daily or weekly basis.

Examples of volatile data are the files of your accounting programs where you run your accounting programs every day, or even all day, and enter considerable amounts of financial transactions, or if you use an email program and have a number of communications daily, your email programs files are volatile data.

Another example would be the files of any development software, for example the files of ShopFactory if you were developing an online shop website, where the developer spends lengthy periods with the development software running and the files open.

For volatile data, you may want to enhance OopsBackup behaviour in one or more ways as follows, and this is done by creating OopsBackup special folders, which allows tailored settings to be specified for specific folders on your filesystem including all files and subfolders within it.

5.2.1 Change the frequency at which backups are taken

If you are running a program all day continually adding data and making changes to the files it uses, then you may want to increase the frequency at which backups are taken so that in the event of failure, you do not have to go back so far before re-entering transactions again.

Copywrite - Ken Wakefield

For example, if you're selling something at the rate of some every 10 minutes and these go into your accounts software as the sale occurs, you wouldn't want to have to go all the way back to last nights backup and start from there to re-enter the sales if the system crashes at 4pm

Based on your usage, you need to choose a frequency that suits you. If you think you can recall and re-enter the transactions over the last half hour without much inconvenience but not for what has happened over the last hour, then set the frequency to 29 minutes.

If you regularly sit there staring at the accounts and bank statements and make amendments to reconcile accounts and adjust/assign expense categories and project tags, then you might want to reduce that to 10 minutes, so that if you make a mess of it or an error occurs, you can restore to a point not so long ago.

On the other hand, you must remember that more frequent backups means more disk space is required for the backup repository. Another example is you have a large 1 GB file, added to daily by a single import in the evening, and this adds large backups to the repository expanding it unnecessarily. You may decide to only backup this file up once a week so that only 52 revisions are added to the repository a year instead of 365, because it is easy to re-import the daily files received over the last week. This is an example of managing your backup repository so it doesn't grow too big, as opposed to managing the time at which backups are done so you can restore to a recent timeframe that is convenient.

So, based on the effort required to manually restore to the current time from the last backup as against the storage space required for frequent backups in the backup repository, for volatile data you either increase or decrease the frequency at which backups are taken.

5.2.2 Change the file size & time frame for which Deltas are taken

Another way of controlling the growth of your backup repository, is to use Deltas for large files. There is a setting that can be modified for the defaults or for individual special folders which sets a maximum size for files above which a backup just stores a delta rather than the whole file.

A delta is the difference between the file as of the backup, and the file as of the previous version and is much smaller than the full copy being only the differences. Instead of keeping the full copy of the previous version in the backup repository, it is replaced with the much smaller delta when a new and later version is added. To get back to the previous version, the delta, that is the differences, are applied to the later full version to produce the earlier version. This can be done over many versions applying more and more deltas to the earlier versions as they are produced, till you eventually produce the older version required.

Of course, the further you have to go back, the more work the computer has to do to go back combining more and more deltas, and eventually this takes too long to be practical.

So, as well as specifying when deltas are to be stored instead of full copies, you also set another setting to say how many deltas are to be kept before another full version is kept instead of a delta, and so to go back beyond that, you are then again only applying a few deltas to an older full copy.

A recommendation is that a practical value for the number deltas to be kept between full versions, is of the order of 20-40, although just about any can be set. With a value of 999 though, you'd probably never get your very old version if required.

It takes a bit of assessment to work out when you should apply deltas, so again take the defaults, and use them till you are aware of an extreme case that is growing the repository size too much, and then refine the backups of the folder that contains the relevant large files.

5.2.3 Invoke automatic purging for large files

Still on the subject of managing the size of your backup repository, it must be remembered that the concept of backups is to provide restoration of lost or changed data as required.

You really need to assess if very old backups of a large file, are really ever likely to be used.

Copyright Ken Wakefield

Remember, that the latest version is never deleted unless you delete the file itself from the computer being backed up.

In that case also, the last Latest Version becomes the latest history version, and is never deleted by the automatic purging option, and so is always restorable from the backup repository if you decide you should not have deleted the file in the first place.

Where large volatile files are continually adding to the backup repository and you assess that the older versions beyond a certain age are never likely to be of any use, then setup a special folder if one does not already exist, and set automatic purging to occur beyond a date at which the file version is deemed of no value.

5.2.4 Invoke the use of Windows Shadow Copy for opened files

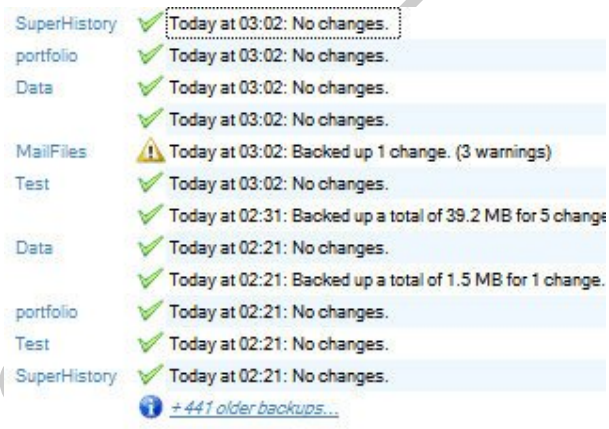
Having setup all your special folders and chosen suitable frequencies so that backups occur at time intervals you want, there is one final consideration. Can the backup program take a copy if the frequencies you have chosen have backups occurring while the program that uses the files, is running. In other words, can it backup Open Files?

You must check that the backup program will be able to take it's copies, and if not, switch on Windows Shadow Copying. This should not be just switched on for all files, as it is a very resource intensive process and will 'bog down' your backup program. Also, it really shouldn't be switched on for special folders covering the whole computer and multiple drives.

A sure way to check if it is needed is to open the file with the program, and while opened, try to copy and paste the file in windows explorer. If you get a sharing violation error, then you will need Windows Shadow Copy to allow the file to be backed up while it is opened.

Alternatively, Review the OopsBackup Backup History reports. A limited list of these is shown on the Dashboard displayed immediately you open the 'Manage' screen, click on the link at the bottom of that limited list or click the Reports button on the Dashboard and select Backup History, for the complete list of all Backup History reports.

Now, look for any reports that resulted in warnings as indicated by the warnings icon, as in the following screenshot..



Notice the additional information indicating there were three warnings when the backup at 3:02 was run.

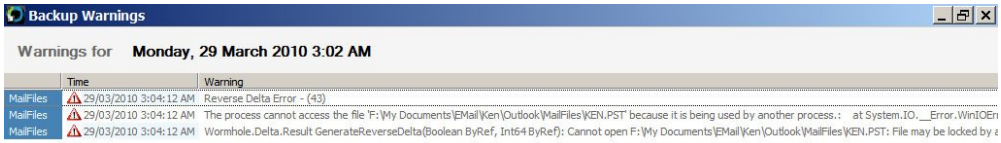
Right mouse click on the entry for the Backup Report with the warnings and select 'View List of Warnings' from the context menu.

The list of warnings as shown in the following screenshot shows that a file was not able to be backed up as required. However, keep in mind that these warnings can occur for other reasons.

If this is a file that you will usually have opened for long periods during which you make changes to it, then decide if it is important that backups are taken during the period you have it open. If so, then you need to turn on Windows Shadow Copy.

© Ken Wakefield

If not already covered by a special folder, create another special folder for the windows folder containing this file and check the 'Enable MS Volume Shadow Service' option for it, but only if you really want backups taken while the file is being edited.



Copywrite - Ken Wakefield