

# Acronis<sup>®</sup> SMB Guide to Backup and Recovery



Alan Stevens, Freelance Journalist

Hard work brings its own rewards we're told, and there's no harder work than that of building and running a small business. Regardless of how much time and effort you put into it, however, that business can be all too easily compromised when something goes wrong with your IT. It really doesn't matter what causes your systems to fail, be it a virus attack, software bug or a hardware breakdown the results are pretty much the same: hours or even days of downtime and, the potential loss of untold amounts of work. If you've got a recent backup, however, and a well conceived recovery plan, the financial and productivity impact on your business can be minimised.

Devising an appropriate backup and recovery strategy will, of course, take time and effort, and you may not see it as a priority, especially if you're busy running and developing the company. That's something we recognise, so the idea behind this guide is to fast track you down the path, addressing the questions you need to consider and discussing what the implications of system downtime might be for your business.

## Protect what?

One of the first things to think about is what areas of your business need protection the most and, more importantly, how quickly you need to be able to get them up and running again should disaster strike. You may be able to get by for a couple of days if the payroll system goes down, for example, but lose the order entry and invoicing departments for just a few hours and cash flow is bound to be affected.

Likewise, you need to consider which systems to protect within each business function and prioritise deployment to get the maximum benefit. Should you, for example, opt to backup everything in the HR department or could you save time by only protecting documents and data files - on the basis that you can always re-install Windows and any applications required from scratch. Likewise, if users store their files on a shared server or storage appliance (and you take backups of those servers), is there any point backing up individual desktop PCs at all?

Only you can decide what's best for your company. As a general rule of thumb, however, it's better to backup more rather than less. You may think, for instance, that you've got everyone to save their work on the server, but users will still often keep local copies to enable them to work offline, especially if they have to travel as part of their job. Performance concerns and not "trusting" the server can, similarly, lead to users keeping local copies of their work which will, inevitably, be the most up to date and cause the biggest headache if lost. In fact, according to analyst estimations, up to 60% of corporate data is held on workstations, something worth bearing in mind.

Another consideration has to be the time it's going to take you to recover should the need arise, what analysts call the RTO or Recovery Time Objective. In some cases the ability to recover a system within minutes will be vital to your business, such as if your Web, email or key database server goes down. If you've got to reload the operating system first and the backup program before you even start recovery, the process will take a long time. Far better if you've the whole server backed up ready and waiting to be restored.

Recovering an individual workstation, on the other hand, may not be so important, but it's amazing how time consuming the process can be if you don't have adequate backup protection. Reloading Windows alone can take an hour or so, not to mention tracking down the disks to re-install Office and other applications, plus sorting out license codes, entering account passwords and changing other settings. If technical staff are tied up for hours or even days rebuilding crashed PCs that will have knock-on effects and can be just as costly as a server outage, not to mention the productivity implications it has for the employee who is without a PC for a couple of days.

## The true cost of downtime

*The cost of downtime isn't easy to calculate, but it's always expensive and not just in pure financial terms – consider these three examples:*

- **The web server goes down, perhaps for just an hour** – orders are lost, customers start to browse competitor sites and your company reputation is dented.
- **Exchange crashes and important email records are lost** – it takes days to find and re-enter old paper copies, re-build mailing lists and recover to where you were before the crash. Customers and partners get annoyed and staff frustrated because they can't do their jobs effectively.
- **A trojan affects all the tills in your shops and the software has to be re-installed** – support staff have to work overtime to cope and other projects are neglected. Employees are forced to revert to manual systems and customer loyalty is stretched to the limit.

*Backup isn't just about being able to "undelete" files that have been accidentally dropped in the recycle bin. It's about being able to recover your systems from any kind of disaster, be it a virus attack, software bug or hardware crash, and quickly to minimise the business impact.*

## Jargon buster – Image backup

*The traditional approach to backup involves copying every document and file individually from the server or PC on which they reside to the backup medium. This though is reliant on the host file system, requires special software to handle files in use by other applications and can be very time consuming.*

*Disk imaging technology, originally designed to “clone” PCs, helps get round these issues by taking a hard disk snapshot or “image”. Because the image is taken at the block level it’s not dependent on the file level and can be much quicker than the conventional file by file approach. It also helps circumvent open file issues and can help simplify disaster recovery.*

*Image based backups are a popular solution and provide protection without any loss of flexibility should you just want to restore the odd deleted document or two.*

## How often?

While thinking about what you need to backup, think also about how often you’ll need to do it. Common practice over the years has been to take backups on a daily basis, usually overnight when systems are otherwise little used, thus avoiding open file conflicts and minimising the impact on other processing. This approach, however, is rapidly becoming untenable as IT systems are made to work harder for longer. Added to which overnight backups can be up to 24 hours out of date, which could mean losing a whole day’s worth of data just because of a simple “blip”.

Overnight backups shouldn’t be dismissed out of hand as they provide baseline protection worth having. Modern backup applications, however, incorporate technologies to enable backups to be taken more often with minimal impact in terms of both performance and the amount of space needed to store the copies. One such is the use of disk imaging technology. Using this, and other technologies, means hourly backups are now a reality.

## Start where?

There are no hard and fast rules but, in general, here’s what to think about when putting together a small business backup strategy.

**Shared resources** – Start with the servers and other shared resources such as storage appliances. Even if they are not critical to the business, downtime here will have an impact on a lot of users so it’s important that you be able to get them up and running as soon as possible following any kind of problem. And don’t cut corners, backup the whole server or appliance if at all possible as this will save valuable time when it comes to recovery.

**Network desktops** – Encourage users to save their files to shared storage as it’s much easier to manage the backup process if they do. In addition, however, look at how desktop PCs can be incorporated into the backup regime, preferably using tools that can be managed centrally and automated rather than leaving it to users to handle it themselves, as most won’t.

There’s no absolute need to back up everything but doing so will reduce recovery time considerably. If opting for a selective approach, pay special attention to email protection, particularly where users download their email to a local message store on their PC hard disk.

**Mobile desktops** – Where users spend lot of time out of the office it isn’t always practical to save everything to shared storage. In which case it’s important to look at ways of taking backups and recovering from disasters offline. The two big concerns here are making easy for the notebook user to manage the process (ideally they shouldn’t be involved at all or even aware its happening) and what media to use, something we’ll cover in detail shortly.

**Virtual resources** – Don’t overlook the need to backup virtual servers and desktops. Taking a backup of a physical host server is a good start but to provide full protection and be able to recover individual virtual machines you’ll need tools especially designed to work with virtualisation technologies. Other than that the considerations are much the same as for “real” resources and you should back up everything to reduce the time and effort required to recover when things go wrong.

**Hosted resources** – One of the advantages of a hosted service, such as Google Apps or a hosted Exchange service is that everything should be backed up for you. Don’t, however, take this for granted. Look closely at the terms of the agreement to see what you can expect, especially when it comes to recovery as the “best efforts” of the service provider may not meet with your recovery time objectives.

## What media?

So, you've decided what systems need backup protection the most and at least have an idea as to how far you want to go down protecting everything. The next task has to be to compare the various solutions on offer and decide what best fits your needs. There are lots of different technologies and products to choose from, each with its own unique advantages, which we'll discuss below. However, when reading this, bear in mind that one size doesn't necessarily fit all and the best approach may involve a mix of what's on offer.

Nowhere is this more true than when it comes to backup media. Long gone are the days when tape was the only affordable option. Tape is still popular but has been largely superseded by disk which is not only quicker, with random rather than linear access to data stored on it, but increasingly cheaper too with no need for complex robotics to deliver the kind of capacities needed to protect modern servers and workstations.

Disks, of course come in various guises and there are other backup media besides, the pros and cons of which are summarised in the following table:

**Table- Backup and recovery media compared**

Medium	Positive	Negative	Good for	Bad for
<b>Tape</b>	Tape cartridges are relatively cheap Not easily overwritten	Slow, linear, access Automated tape libraries can be very expensive	Automated backup of large data servers Long term archiving	Backup of individual workstations and PCs Fast recovery
<b>CD/DVD</b>	Random access Cheap to buy Almost every PC has a CD/DVD writer	Limited capacity which means swapping disks to backup large amounts of data	Offline backup of individual PCs and notebooks Bootable recovery disks Long term archiving	Server backup
<b>Memory card/stick</b>	Easy to handle and store No special hardware required other than USB ports or memory card slots	Easily overwritten, easily corrupted and lost Limited capacity	Ad-hoc backup of important documents and data files	Regular backup of servers or desktop/notebook PCs
<b>External hard disk</b>	Fast, random access Capacity Low cost	Easily overwritten Not easily transportable	Automated server and network workstation backup	Backup of large data servers Long term archiving
<b>Network storage</b>	Fast, random access High capacity Low cost	Easily overwritten	Automated server and network workstation backup	Long term archiving
<b>Online storage</b>	Externally managed resource	Backup/recovery performance limited by Internet bandwidth	Backup of mobile user notebooks	Server backup/recovery

Note that a good tip here is to spread the risk and use more than one medium for backups. A popular solution is to take immediate backups to locally attached or network hard disk then use tape or optical media (CD/DVD) for long term archiving. Another is to take backups to dual media, such as network and online storage, simultaneously, to provide additional security and flexibility.

You should also bear in mind the need be able to put your hands on your backups when they're needed. Don't just throw your backup tapes or disks in a drawer or leave them in the server running the backup program. Set down procedures to make sure they're properly labelled and stored in a secure location and make sure they can be retrieved quickly. If possible arrange for copies to be kept off-site and, if you're taking backups to a storage appliance consider taking a second level backup of that too and storing it somewhere else.

## Jargon buster – Data deduplication

*When it comes to backup compromises are inevitable. Backup everything and you soon run out of storage space. Be selective and you could miss something vital.*

*Compression helps, but the technology everyone's now talking about is deduplication, where you only ever store one copy of your data no matter how many occurrences there are. The majority of files needed for Windows for example, will be the same on every PC, so there's little point taking a backup of each individual copy. Far better if the backup software can save just one copy of each file and set a pointer to that location in subsequent backups.*

*A growing number of backup products now support file and, in some cases, block-level deduplication, saving on storage costs and the amount of time backups take, without impacting on the ability to recover individual files or complete systems should the need arise.*

## Where next?

The last step is to decide which backup products you're going to use. There are lots to choose from and it's worth arranging demonstrations or, better still, trials on your own site. That way you can check out exactly how easy they are to use – by non-technical as well as tech-savvy staff – plus whether they provide the level of protection you're looking for, and whether they meet your recovery time objectives.

After that it's just (just?) a matter of installing and deploying the products you've chosen. We do, however, have a couple of final tips, the first of which is to test your backups to make sure they work. Taking a backup does not equal being able to recover from a disaster and it's not at all unusual for companies to religiously create backups, day after day, only to discover that they're either unusable or, worse still, completely empty when the time comes to restore from them.

The other is to document your backup and recovery strategy and all the procedures involved. Don't simply rely on individuals "knowing" what to do. If something is going to go wrong, it will always happen when the person in charge of the backups is off sick or on holiday. Write procedures that detail how backups are to be taken, the media to be used, naming conventions, storage arrangements and so on. Do the same for recovery too, and make sure the people that matter read them. Spread the information as widely as possible and make the procedures readily accessible, in paper as well as electronic format - don't just put them in a folder on the server. Partly because no one will think of looking there, but equally because, if the server crashes - well, that's why you need a backup and recovery plan in the first place...

## About Acronis®

Acronis is a leading provider of onsite and offsite backup, disaster recovery and security solutions. Its patented disk imaging and management technology enables corporations and individuals to protect digital assets in physical and virtual environments. With Acronis' backup, recovery, server consolidation and virtualization migration software, users protect their digital information, maintain business continuity and reduce downtime. Acronis software is sold in more than 180 countries and available in 13 languages. For additional information, please visit [www.acronis.eu](http://www.acronis.eu). Follow Acronis on Twitter: <http://twitter.com/acronis>.



For additional information please visit <http://www.acronis.eu>

To purchase Acronis products, visit [www.acronis.eu](http://www.acronis.eu) or search online for an authorized reseller.

Acronis office details can be found at <http://www.acronis.eu/company/worldwide.html>

