

Don't fall victim to common backup mistakes

Backup mistakes happen every day in businesses around the globe. The end result is serious damage to business reputation and potential eradication of complete company data. Businesses cannot afford for this to happen in today's competitive environment. With the advent of online backup data loss and backup disasters are **completely avoidable** as proven by keepITsafe, Ireland's largest online backup provider.

Many individuals and businesses alike are too familiar with that sinking feeling when they realize that the data is *actually* gone and cannot be restored to their computer. This pain is felt from the IT Manager conducting the backup in larger companies to the administrative staff in smaller organizations, whose responsibility it is to backup.

Human error exposes individuals to the several common mistakes when conducting a backup. See details below

Using a manual solution

When using a manual solution such as tapes, companies are exposing themselves to additional risk. Choosing the correct backup method and sticking to it is crucial to the success of any company's backup strategy. There is a significant failure rate with tape backup's that can leave companies with irreplaceable data loss. The primary disadvantage of tape backup is the inherent inefficiency in the administration and the time it takes an individual to conduct a restore. Manual solutions pose huge problems when you are looking to restore data. This can take a considerable amount of time.

Tape backup costs are often times misunderstood and in turn lead to greater costs for companies in the long term. Fundamentally tape drives have a significantly high failure rate due to improper use and maintenance. Tape users are living with a false sense of security when processing their backup with tape. In our experience the failure rate for tape backups is anywhere between 25-35%.

Who is managing your backup?

Who wants the responsibility of conducting tape backups or any manual backup available today? This is often an area of ambiguity in companies. Consider the following situation: The receptionist is left with the task of backing up the company data and is away for two weeks in July. What happens next? In an ideal world another member of staff is informed and takes over

the task. Unfortunately this is not always the case and the result is two weeks of no backups for the company. The potential catastrophe the company is exposing itself too is beyond belief.

Businesses should always make sure that they have a designated person who conducts the backup and realizes the significance of it. On numerous occasions non technical staff members are left with the task of backing up and also restoring files with little or no understanding of the task and how important it is to get it right. If manual backup is your solution of choice you can reduce your risk of data loss through planning and delegation of the backup process. Statistics have shown that the best way to eliminate any risk of data loss is to automate the backup process. By outsourcing your backup to an online backup provider, such as keepITsafe, your data is monitored and managed 24/7, to make sure that data is available for restore at any time.

Not taking backups off-site

Another common area of failure with a backup process is the lack of continuity with taking backups offsite. If a tape has backed up information it is completely null and void if it stays onsite. The purpose of backups is to take the backed up information and store it away from the original in the event of a fire or theft. Tapes need to be taken offsite for the act of backup to be a viable one.

Not encrypting backups

Every company holds very sensitive and extremely valuable information on its servers. Most of this data is confidential and company sensitive from budgets to customer details to strategies etc. As tapes need to be transported manually from one location to another the data is being exposed to external threat or even theft. Many different threats are out there so it is extremely important for companies to encrypt their backups. By not encrypting tapes any third party who comes in contact with a tape will have access to all the information on them – breaching your legal obligations in relation to data protection. If you have encrypted your media and it gets lost or stolen it is impossible for the information to be recovered by the third party.

Not testing backups regularly

Is there anyone monitoring your backups for success? If your backup fails and no one notices, what happens next? A simple thing such as checking that the backup is actually working could be the savior of many backup disasters. Backups should be checked regularly and verified that the requested data is backed up and no errors are showing. Complacency is the root of many

problems in tape backup disasters. Just because they have worked for the last 4 months does not mean they can fail at some stage in the future.

Lack of proper cleaning and maintenance of tape backup drives will lead to file corruption over time. Tape backup drives should be cleaned at least once per month. Lack of proper cleaning is responsible for the majority of tape restore failures.

Regular reviews should also be undertaken to document exactly what is being backed up across all servers. As new programs are installed or updated backup requirements may change. It is important to review these regularly as successful backups each night render useless if the wrong information is being backed up.

Understanding the total cost of ownership

Tape drives have a 3 to 5 year lifecycle. Also, tape drives have moving parts and eventually will just stop working. Most backup software solutions have annual maintenance costs associated with them. There is also the cost of your tapes which again should be replaced annually. Finally, an area that is often neglected is the amount of time spent conducting tape backups. How many employee hours does your organization dedicate to changing tapes, cleaning the tape drive, and performing test restores? Adding all the above costs together will give you an approximate cost of ownership.

Restore time is also an area to consider when looking at the overall cost of ownership. You need to consider the length of time you will be down due to the time spent on restores. Not only does this take time but could also mean loss in revenue! This is hard to calculate but should be considered when looking at the cost of your chosen solution.

Over the last 5 years keepITsafe has gathered a wealth of knowledge from their customers as to the causes of backup failures while using manual tapes and also the main reason for restores – see below

“In our experience, 30% of restores are for data that has been deleted a week or more ago, 15% a month or more ago. One tape is needed for each night’s backup, which means the costs of tape backup can quickly spiral. Also a common mistake observed is staff only having a 5 tape rotation and realizing that they have overwritten information they wanted to restore, leaving the

staff member and company in a huge predicament!” stated Jonathan Crowe, Technical Director, keepITsafe.

Eliminating the common backup mistakes with keepITsafe’s online backup solution

keepITsafe’s online backup is a unique online service that allows you to back up and instantly restore all data and files held on your system. It continuously backs up your data via the internet and stores it securely off-site in multiple data centres. This gives your data the VIP treatment it deserves and is also available for recovery 24/7. All installations are performed by experienced engineers and backups are monitored 7 days a week, with proactive issue resolution.

Once the online backup solution is set up data is automatically compressed, encrypted and securely transferred to keepITsafe’s primary data centre in Dublin. keepITsafe only transmits the data that has changed since the prior backup. This means backups are lightning fast.

On a daily basis company data automatically synchronizes with the keepITsafe data centre and is also continuously mirrored to a secondary data centre. This process gives companies the assurance that all their data is stored safely. All deleted and old file versions are stored by keepITsafe. This period can be customized but each package includes a month’s worth of backups plus the 1st day of the month for the last 3 months. Included in each package are regular health checks to insure that the information being backed up is up to date. Test restores are also performed during this health check.