

Data Recovery

What you Need to Know



a guide by



What **NOT** to do When you Lose Data from a Storage Device

- [!] Never run a program that writes to, or alters, a storage device in any way.
- [!] Do not power up a device with obvious physical damage (e.g. a hard drive that is making a clicking noise). Persistent read/write attempts on a drive with defective heads will just incur further damage and potentially make the data recovery process twice as complex.
- [!] Do not activate the write-protect switch on any memory cards or USB sticks.
- [!] Be aware that there is no software in the world that can fix a storage device with physical defects.
- [!] Do not run the *CheckDisk*, *Disk Utility* or any third-party “disk repair” utilities. They are designed to correct small errors in the file system, not more serious logical errors. If there are physical problems with your drive, these utilities can exacerbate them.

What to do When you Suspect you Have Lost Data from a Storage Device

- [!] Keep calm – some users get distressed and panicked about data loss. Instead of trying “quick fix” solutions, step back from the situation and maximise the probability of a successful data recovery, without further jeopardising your data. Evaluate your options carefully.
- [!] Diagnose correctly – you can waste hours trying to fix a hard drive problem that does not exist, so it is vital to diagnose the root cause of the data loss problem correctly.
- [!] Handle hard drives correctly after a data loss situation. Some users panic and do not properly observe proper hard drive handling procedures. This can be a mistake. For example, if a drive has mechanical issues, do not compound the problem further by not observing proper anti-ESD precautions as this will cause electronic issues on the drive as well.
- [!] Avoid solution overkill – do not be tempted to deploy drastic solutions. Trying to factory reset a RAID array on a NAS device in the hope that it will fix a broken RAID will reduce your chances of a successful data recovery.
- [!] Sometimes the best and safest solution is to take the storage device to a professional data recovery company. Experienced recovery technicians who deal day-in and day-out with data loss will have the expertise, equipment and insight to successfully recover all of your data.

Myths about Data Recovery

If I remove the PCB from a failed drive and replace it with an identical one, will that fix any electronic problems with the drive?

This probably would have worked 10-15 years ago. For example, PCB swaps used to work brilliantly with Quantum hard drives. However, times have moved on in the world of data recovery and 20 Gigabyte Quantum drives are not very common anymore. With modern high-capacity drives, PCB swaps generally do not work. Every hard drive is now “hyper-tuned” to optimise performance. This means each time a hard drive is powered up, an orchestra of heads, platters, electronics and firmware parameters all work together in unison. When an “alien” PCB is introduced into the equation – which uses a slightly different variant of PRML read channel to the one in the failed drive – the drive will not read or will not initialise properly.

To fix the heads in my hard drive, all I need to do to get the drive working again is to open up the drive quickly and reposition them on the platters, right?

Drives cannot be safely opened up without a clean-room. If you want to test this, get a clean mirror and place it in a standard room for a couple of hours. You will probably notice, even after an hour, tiny particles of dust have fallen on its surface. The same contamination happens to the platters of a hard drive. These tiny particles of dust can severely interrupt the heads reading from the platters. Remember that the average “flying height” of the drive heads against the platter is only 3 nanometres. (A particle of dust is the equivalent of putting a rock on a train line, except on a microscopic scale). Do not try to reposition the drive heads manually as, from our experience, it can cause irreversible platter damage. Recently, one Dublin user brought us a drive that he tried to recover himself. We opened the drive to find fingerprints, dust and scratches on the platters. It looked as if Edward Scissorhands had been poking around in there! To properly repair or replace a hard drive’s heads, a clean-room, a special device called a “head comb” and years of experience are needed.

Even if a hard drive has severely damaged heads, there must be a universal platter reader invented by someone, right?

Many computer users assume there must be a machine out there that can recover data from all failed hard drives. They imagine a magical machine where you drop platters from a failed drive into it, and a couple of hours later all the data starts flowing out. General users would not be alone in imagining such a device. In the early 2000s, the US Department of Defense even put out a tender for a device that could read platters drive-independently. Well, if there is a universal platter reader in existence, the general public and data recovery professionals have yet to be told about it! Many companies of proprietary tools have claimed they have developed a way of recovering data from platters drive-independently for one-off cases. However, none of them have proved to be commercially viable.

When Backup Files are Useless

We have come across several data recovery cases where the user “thought” they had an up-to-date and complete backup.

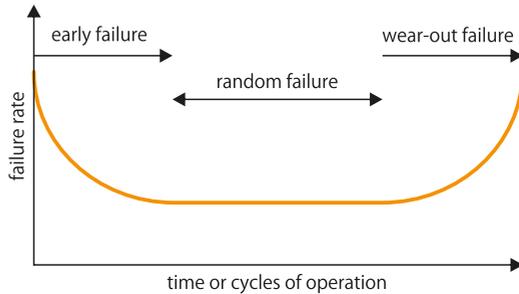
But, when data loss does occur, they experience the painful discovery that the backup is either not fully up-to-date, not complete or corrupt. A backup that is, for example, three months out-of-date can be useless, as is a backup file that is not complete or corrupt.

The IT industry could learn a lot from the airline industry, which rigorously rehearses and simulates emergency situations every couple of months. Emergency equipment is rigorously tested so that when a real emergency does occur, crews are usually well-versed in executing the proper procedures in a calm and efficient manner.

Every so often, you or your users should test preparedness for data loss. For example, when was the last time you downloaded files from your Cloud backup? Was all your data intact after downloading it? Are the backup folders on your external drive all up-to-date and complete? If you work in IT support, encourage your users to test their backup files on a regular basis. A good backup is only good if it is complete, has full integrity (i.e. no corruption) and is up-to-date.

Why New Drives have a High Risk of Failure

Even though most hard drives undergo quality control testing before they leave the factory, there are some latent failures that do not manifest themselves during manufacturer testing. These latent failures can happen due to small defects that occur during the manufacturing process.



As you will see from the graph above, hard drives failure rates follow the “bath-tub curve”. This means that hard drives have higher-than-average failure rates during the first 12 months of their lifecycle. After this period, the failure rates plateau. Then, after about 6-7 years of use, the probability of failure rises steeply again.

So, no matter how “new” a drive is, complacency should never set in. Statistically, a new hard drive (i.e. a drive that is less than 12-months-old) is more likely to fail than a 3-year-old one. Just because a hard drive or computer is new does not mean that you can sit on your data backup laurels.

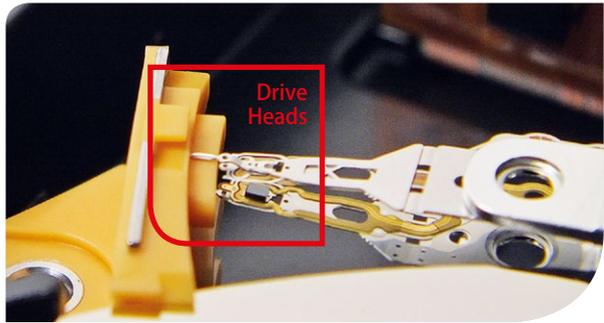
To illustrate the faux sense of data security which new hardware can instil in users, here’s a common scenario that we see a lot:

- 1) A user gets a new computer.
- 2) They do not configure any backup to the new computer. (*How could such a powerful and shiny computer lose any data?*)
- 3) The user begins using new system for a couple of months.
- 4) The drive fails due to a latent failure (or data is lost due to data corruption)
- 5) The user has no backup.
- 6) They, or their IT support, provider tries to recover the data.
- 7) If unsuccessful and the data is sufficiently important, they bring the failed drive to a data recovery company.

They might have had a disciplined backup regime with their old computer, but with the acquisition of a new computer, complacency sets in. As a result, scheduled backups go by the wayside. No matter how “new” a computer system or storage device is, it is still prone to data loss.

Critical Success Factors for a Head Disk Assembly Swap

Replacing the head disk assembly is sometimes necessary when there is damage to the drive heads. This is an intricate task and time-consuming task which Drive Rescue has performed successfully hundreds of times.



From our experience, a successful Head Disk Assembly swap has the following characteristics:

When choosing a donor drive, it must be an **exact match for the failed drive**. It must have the same model number, same serial number and same revision number. A “close match” will not work, it must be an exact match.

The head’s **flying height** must be the exact same distance as used by the old Head Disk Assembly. An incorrect flying height will result in a weak or saturated signal.

The **head stack must be aligned perfectly** in the same position as the original heads. If alignment is off-kilter, there will be excessive head-to-platter “eccentricity” that cannot be tracked out by the drive’s servo.

The **spacing of the heads** must be the same as that used on the original HDA. If the spacing is not correct, the disk pack will not successfully reload.

The **centres of the platters should line up perfectly** with each other. If they are not in perfect alignment, the servo will not be able to track out the irregularity.

When replacing the platters and spacers, it is important that the data recovery technician **torques the retraining screws correctly**. If not enough pressure is applied, the platters can warp. The drive heads can tolerate small degrees of warp as they fly, but too much and accurate syncing between the heads and platters is very difficult.

Things to remember when buying and using an NAS drive

RAID 0 offers no level of data redundancy.

It increases data throughput rates, but no redundancy. If one disk fails, the RAID array gets broken. That disk will have to be repaired in order to facilitate data recovery.

If you are using a NAS as a file server, then **it is not a backup device**. NAS devices also fail. For this reason, you will often see a USB port or and E-SATA port on an NAS device. This enables the user to backup their files onto another drive.



Choose a NAS device that uses **active cooling** (i.e. it uses a fan) instead of **passive cooling**. Thermal stress kills hard drives. It causes damage to the electronics onboard, causes failure of mechanical components and can induce a phenomenon known as the super-paramagnetic effect to corrupt your data. From our NAS data recovery experience, NAS drives that only use active cooling are much likely to be damaged by thermal stress.

Try to choose a **NAS device that allows backup directly to the Cloud**. For example, many NAS devices now allow direct backup to a Dropbox account. This mitigates against the risks of fire, flood, theft and employee sabotage.

Try to avoid plugging your NAS device into your mains power supply. If there is a power surge, you risk turning your NAS into an expensive doorstop. **Instead, plug it into an Uninterruptible Power Supply.**

These days many users have a desktop PC in their office that is not being used. By installing high capacity drives into such a PC, you can turn it into a **cost-effective NAS solution**.

Failed RAID or NAS - Data Recovery Process and Best Practice Tips

The RAID data recovery process normally involves the following steps:

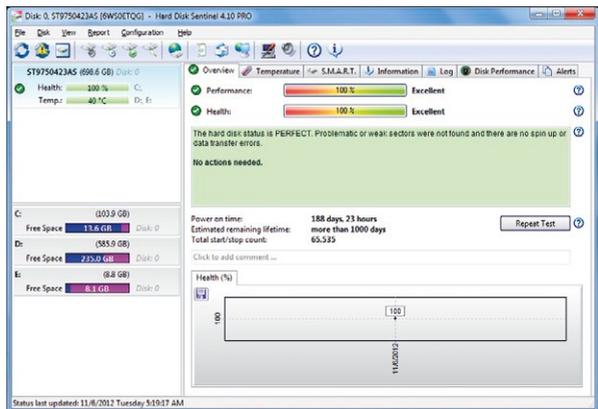
- 1) Diagnosis or confirmation of RAID failure
- 2) Careful numbering of all drives
- 3) Imaging of all drives in the array
- 4) Determination of RAID type
- 5) Determination of member disks
- 6) Finding out the correct disk order
- 7) Finding out the Block Size
- 8) Finding out the start offset points on each of the disks
- 9) Start of RAID rebuild process
- 10) Verification of data integrity
- 11) Extraction of the data

Raid Data Recovery - Good To Know

- > If you suspect one of the disks in your RAID array has failed, do not continue to use that system. Normally, you will get a warning error from your SCSI BIOS / BIOS or a message from your NAS device.
- > Do not run CHKDSK or FSCK repair commands unless you have imaged your drives first.
- > RAID data recovery programs need “to speak” to the drives directly without any RAID controllers. Therefore, each drive must be removed and mounted directly to the recovery system.
- > Most RAID data recovery programs cannot work with proprietary formats. The partition must be NTFS or EXT2/3. For example, they cannot work with RAID configurations, such as *BeyondRAID* as used on Drobo devices. For the purposes of RAID data recovery, these configurations have to be manually configured.
- > Before you start removing disks from a failed RAID array, make sure that you examine the RAID controller log to see what order the drive(s) failed in. The more information you are armed with the better.
- > When you are removing disks from a server or NAS device, remember to number all the drives carefully, bearing in mind that the first drive will always be labelled “0” not “1”. Never attempt to change the order of the disks.
- > Do not use USB enclosures for RAID rebuilds, which can take hours. When you use drives attached via USB it can take days (even when you use USB 3.0 enclosures).
- > Before you attempt the RAID rebuild process make sure that you image all your drives. It is advisable that you run diagnostics on all drives before imaging as failing drives might not survive the imaging process.
- > If you need to find out the parameters of your broken RAID array you can use the free ReclaiMe tool available at www.freeraidcovery.com

Useful Tools to Prevent Data Loss

Your ultimate tool against data loss is by having a scheduled backup to several different backup mediums. In turn, this backup is verified frequently to make sure that the backup application(s) are performing the backup tasks comprehensively and maintaining data integrity.



However, having a utility that pre-warns you about hard drive problems would be nice. It saves IT support technicians and end-users the time and hassle involved in doing a complete restoration from backups. It is the function of SMART to help give users a warning of imminent failure. SMART usually works by counting read-errors, write faults, reallocated sectors and temperature over time.

The Problem with SMART

Every time a warning is triggered, the drive can be returned for an RMA (return merchandise authorisation), providing it is still under warranty. As a result, manufacturers have set extremely high thresholds in their SMART fault-detecting algorithms. Independent statistical analysis of failed drives has estimated that SMART has a paltry failure detection rate of only 3-10%. Thankfully, third-party applications can help increase these detection rates by up to 50% without an unacceptable level of false alarms. There is a plethora of these tools on the market. Not all of them are worthy of mention. However, *Hard Disk Sentinel* stands out for its reliability and accuracy. When installed on a Windows PC, it can give sufficient warning that a hard drive is about to fail.

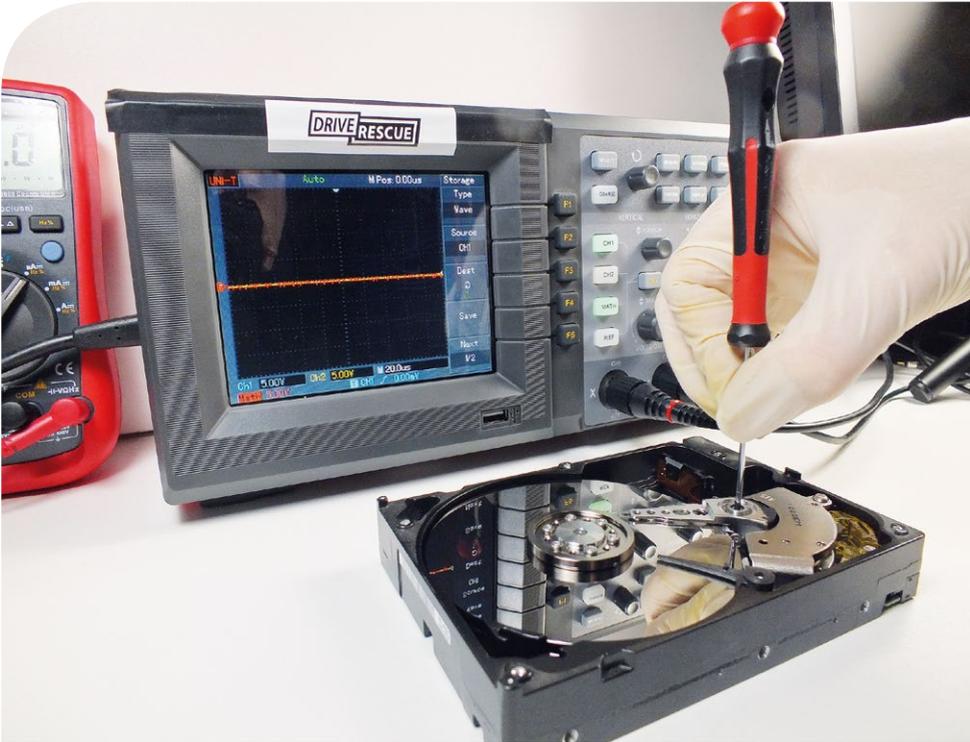
Get your users or customers to remember the LOCKSS Principle

Stanford University in the United States has one of the leading research and development laboratories in the world for Information Technology.



One of their studies investigated the best and most reliable way to archive information and keep it safe. The basic tenet of their research findings is this: make lots of copies of your data and distribute them in different places. To make this principle easy to remember, they came up with a simple mnemonic: “Lots of Copies Keep Stuff Safe” or LOCKSS. Users can now achieve remote backup more easily with some excellent online storage facilities, such as the *Amazon S3 Cloud*. Alternatively, you could simply store your data on two separate hard drives that are placed in different locations and verified on a regular basis.

The Gallery Rescue Lab



Removal of Drive Spindle

A disk platter
and Head Disk
Assembly
in perfect
alignment



The Gallery Rescue Lab



Drive Rescue
imaging station



Examination
of 2,5 inch PCB

Keep Informed and Stay in Touch with Drive Rescue

Have any data recovery questions or issues?

Please feel free to contact us

Email: info@datarecoverydublin.ie

Phone: 1890 571 571

For information on our complete range of data recovery services visit:

www.datarecoverydublin.ie

Keep updated and informed about data recovery - visit our blog at:

www.datarecoveryireland.ie



Drive Rescue Data Recovery

9 Trinity Street, Dublin 2, Ireland

www.datarecoverydublin.ie