It is not an if, but a when. All hard drives will eventually fail, and many as soon as 2-3 years old. The way to defend against this is to do regular backups. But what kind, how often, and what software or service is the best to use?

There are several types of backups, and each have strengths and weaknesses. There is usually no one perfect solution, but there are great solutions for most all types of users and environments. Further, a combination of backup systems can create a robust and very reliable system to prevent data loss.

Image backups are backups that take a snapshot or identical copy of your disk and copy it into a backup file. Once completed, you can use this backup file to create an identical disk on another drive. This method is used only on Windows based systems, so for Mac and Linux users, this is not an option. Image backups are now the most commonly used on servers and critical workstations. They work great for home users too. In most cases, image backups also function as a file backup allowing the restoration of a complete disk, or individual files when needed.

Acronis is the industry leader in image backups, and provide both simple personal based solutions as well as enterprise level drive imaging solutions. While Acronis is clearly one of the best on the market, they are also the most expensive solution. A close competitor is Aomei Backupper. Like Acronis, Aomei is feature rich and provides most of the same features but at a substantially lower expense. In fact, the basic version of Aomei Backupper is free for personal and business use. While not as feature rich, a solid and reliable imaging solutions is provided by r-tools called r-drive Image. R-drive Image is also quite inexpensive and runs on workstations or servers for the same price.

File based backups is the traditional way backups have always been created since hard disks have been used. This is a simple and very functional solution that works on all operating systems. Its biggest shortcoming is the unfortunate limitation on copying files that are currently open. In most cases, copying an open file will corrupt the resulting copy, and invalidate the backup. Newer backup systems use various approaches to resolve this issue, so good quality software is a must. For Mac, the built-in Time Machine backups or Carbon Copy Cloner are great solutions. Acronis is also available and creates a hybrid image for Macs as well.

Cloud backups are essentially the same as file based backups, but rather than storing the data on a local media or disk, it is stored remotely at another facility. Most backup providers store your data encrypted so that even the providers employees do not have access to your files. The biggest disadvantage to cloud backups is the time that it takes to backup a system. Because files are copied over the internet, it will take days if not weeks to backup a full system the first time. Due to improved methods in backup solutions, cloud backups employ changed data updates which minimizes on the time to update an existing backup to the latest information.

In most situations, a choice of one of the above solutions is appropriate and provides plenty of protection from data loss. However, for all servers and systems that have critical data, it is best to complete a dual solution of an image or file backup along with a cloud solution. This provides protection against hardware failure, loss from theft, natural disasters and more. Further, utilizing dual backup systems further minimizes the risk of data lost due to failed backups.

For most home systems and non-critical workstations, backups can be performed weekly or how ever often important files are modified. On almost all other systems where data is important, daily or live backups should be performed and verified daily. On critical systems, the best approach is a multiple backup, such as imaging and cloud backups simultaneously, and performed at least daily. For critical systems, it is important to have off-site in the event of theft, fire, or other natural disaster since the backups themselves may be damaged or destroyed in the process.

For more details on protecting your data on home systems, workstations or servers, contact us for a free consultation.