CLOUD BACKUP

The simple guide to avoid losing digital assets in the cloud age

LIFE IS FOR SHARING.

EASY COME, EASY GO

Many companies and organizations only fully understand the value of their data once it is lost. Information is not just becoming more and more prized, it is also increasingly irreplaceable.

Yet it's incredibly easy to lose company data. In addition to the traditional hazards of hardware failure, theft, flooding, hackers, or viruses, new threats are emerging, such as the recent wave of "ransomware", a type of malware that encrypts hard drives and demands a ransom in exchange for decrypting them. If a proper backup hasn't been carried out recently and no reliable recovery procedure has been put in place, paying the ransom may be the only hope – and a potentially vain one at that.

MORE THAN A COPY-PASTE

Most organizations at least attempt to back up their accounting data or other essential documents, but the way these backups are protected is typically weak. Backing up is not simply copying data to one side and then copying it back if necessary. The process may have been that simple 30 or so years ago, but it has largely evolved since.

Nonetheless, it is not uncommon for many companies to keep only one simple copy of their data on a device such as a USB disk. This may contain a recently made error, which would then get backed up as well. Backups at smaller organizations are usually done manually and sporadically, and are often stored too close to their primary source, so certain disasters, such as a fire, would destroy them along with the primary storage.

> "Backing up is not simply copying data to one side and then copying it back if necessary."

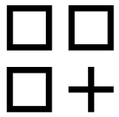
WHAT TO BACK UP

For most of us, backing up data concerns only a few critical document files or pictures. However, large systems and servers house many other types of files that do change frequently and are critical to recovery operations in case of a failure, including OS binary files, configuration files, drivers, application files, or metadata.

Media

OS

Metadata



Applications

Documents

Database

Configuration filtes

Drivers

3 TYPES OF BACKUP

Full

The first and full copy of a system, capturing everything in it. The upside is that it is self-contained and has all the source information needed for a recovery. It takes a long time to make, however, and is often almost identical to a previous full backup.

Differential

This type of backup records only the differences between the current state and the last full backup. Recovery procedures using this method require both the full backup and this differential backup. It allows for the fastest recovery, but takes up more space and time to back up than the third type, the incremental backup.

Incremental

With this type of backup, the successive copies contain only the portion that has changed since the preceding backup was carried out. Recovery requires the last full backup plus all incremental backups until the point configuration files of restoration.

The typical backup strategy is to perform a full backup weekly during weekends, and differential or incremental backups on a daily basis at night. The average size of an incremental backup is 3-5% of a full backup, but this varies greatly depending on the business.

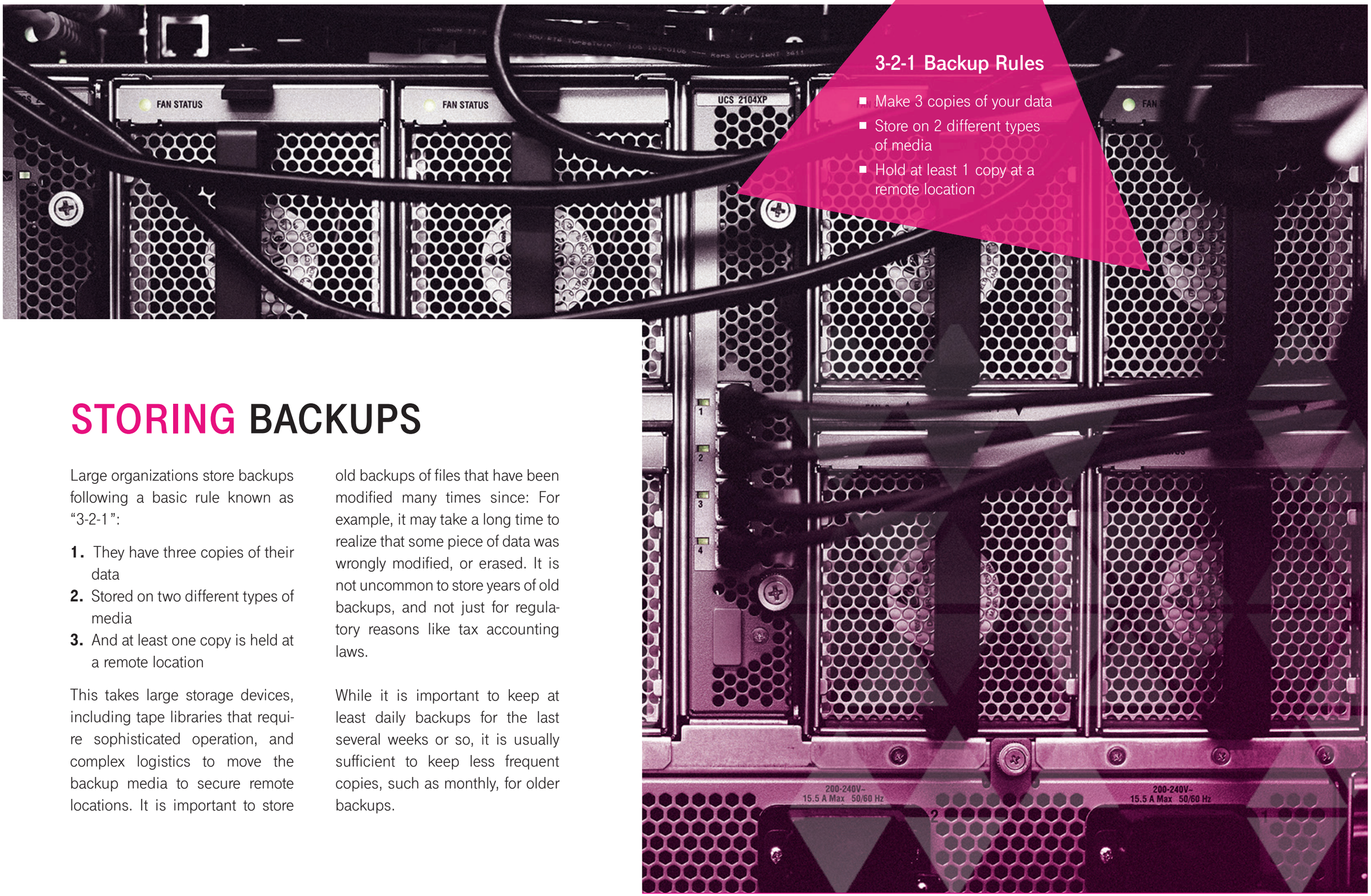
STORING BACKUPS

Large organizations store backups following a basic rule known as “3-2-1”:

1. They have three copies of their data
2. Stored on two different types of media
3. And at least one copy is held at a remote location

This takes large storage devices, including tape libraries that require sophisticated operation, and complex logistics to move the backup media to secure remote locations. It is important to store old backups of files that have been modified many times since: For example, it may take a long time to realize that some piece of data was wrongly modified, or erased. It is not uncommon to store years of old backups, and not just for regulatory reasons like tax accounting laws.

While it is important to keep at least daily backups for the last several weeks or so, it is usually sufficient to keep less frequent copies, such as monthly, for older backups.



3-2-1 Backup Rules

- Make 3 copies of your data
- Store on 2 different types of media
- Hold at least 1 copy at a remote location

THE CLOUD WAY

What does the cloud bring to backups? Nothing, except low costs and simplicity – but that is enough for a complete revolution. Anyone can now back up like the big organizations. The cloud counts as a different type of media, and is hosted at remote locations which are more secure than most organizations could afford or would have the knowledge to build. Therefore, the cloud satisfies all three points of the decades-old backup principle while also bringing more reliability and security to the table. It is common practice not only to compress backup data, but also to encrypt it. This has the added benefit of removing any possible doubts about the cloud provider's trustworthiness, as the data cannot be read without the appropriate private keys, which can be stored separately. There is no need to invest in any backup hardware, because the cloud backup comes as a flexible service that can be scaled as needed for a monthly charge. All the effort required to operate backup hardware and to manage, change, and transport backup media is taken off the company's hands, too.

Automation

The greatest advantage of cloud storage may be convenience. There is no concern with transporting media to a safe location, or with making duplicate copies in case some of the media fails along the way. Often, the issue with traditional backups is more fundamental: People don't remember or don't have the time to create backups manually. That's why they should be fully automated, and cloud-based services provide the software that ensures just that.

Connectivity

Transferring data to the cloud does require proper bandwidth. It's a huge advantage if the cloud provider also offers a connectivity solution, not only via the public Internet, but also over private data lines, especially for larger backups. To determine the required connectivity, it is important to define how fast the recovery needs to be to restore operations in the event of a failure or disaster. The bandwidth must be sufficient to transfer the last full backup and all subsequent incremental backups well within this time period to allow the recovery procedures to take place within the desired timeframe.

WHY DEUTSCHE TELEKOM

Wide range to fit all.

Deutsche Telekom and its subsidiaries offer several types of cloud backup solutions that are suitable for digital devices and infrastructure ranging from mobiles, tablets, and PCs, to servers, storage arrays, or mainframes, and scale from small businesses to the largest of data centers.

Our own experts.

We have more up our sleeve than just software tools and storage space, too: We have the required experts stationed in many countries in Europe and around the world, ready to consult and implement successful backup strategies right at customers' doors.

Unique network coverage.

It is absolutely essential to have a strong, secure and reliable connectivity for any cloud solution, and unlike the global cloud players, Deutsche Telekom has an extensive private data network spanning across western, central, and eastern Europe and large parts of the world. This is crucial to carrying out the vast transfers that successful cloud backup and recovery strategies demand.

Colocation Data Centers.

DT and its subsidiaries have decades of experience running over hundred data centers at carefully chosen locations, built to meet the highest security criteria to deliver their own telecommunications and media services. Many of DT's data centers offer colocation services, which makes DT suitable for hybrid cloud scenarios. In several countries, our DCs have a special status of strategic government importance and have guaranteed priority protection during extraordinary disaster events.

100% EU and German.

DT offers its cloud services in compliance with relevant EU and German laws and adheres to the strictest industry certifications on security, data protection, and business continuity.

THE CLOUD ERA IS HERE

It's undeniable: We live in the age of the cloud. More and more businesses and organizations are using it to store important data and to run mission-critical applications. The cloud's flexibility, affordable price, and agility are becoming irresistible. There could really be no difference in companies' data before and after it is lost – if it is backed up in the cloud, that is.