Read or listen to this article online

Scan the QR code to open this article on XO.PL

Article source:

https://xo.pl/it-made-fun-data-backup

DATA & STORAGE

Backups: why one copy may be no copy at all

The Central Document Warehouse, named after its Manager, has burned down. So have its two safes and its magnificent **RAID**. The manager is discovering that surviving a disk failure is not the same as surviving a fire, accidental deletion or ransomware. Fortunately, the accountant has an old drive in a drawer. Operation “Save Whatever We Can” begins — a story about backups that needn't be fancy, but must actually be restorable.

Chapter one: socks save the company

The manager stands among the ruins.

— GENTLEMEN! WE HAVE NO WAREHOUSE!
— We know, boss.
— NO SERVERS!
— We know.
— NO **RAID**!
— We know that too.
— THEN WHAT DO WE HAVE?!

The accountant speaks up.

— I have a hard drive.
— WHAT DRIVE?!
— With company documents. At home, in a drawer underneath my socks.
— YOU KEEP COMPANY DOCUMENTS UNDER YOUR SOCKS?!
— Yes. You kept both safes in the same burning building.
— ...
— ...
— BRING ME THOSE SOCKS IMMEDIATELY!

🤣🤣🤣

That's how we meet a **backup**: a spare copy from which we can recover lost data. The best one needn't be the most expensive. It needs to be **correct, appropriately protected and genuinely restorable**. A forgotten two-year-old drive could save precious photographs, although it isn't a replacement for a planned, current backup system.

Today's motto: **“There is no stupid backup. The stupid thing is having no backup!”** It's encouragement to start with something real, not a promise that any random copy provides enough protection.

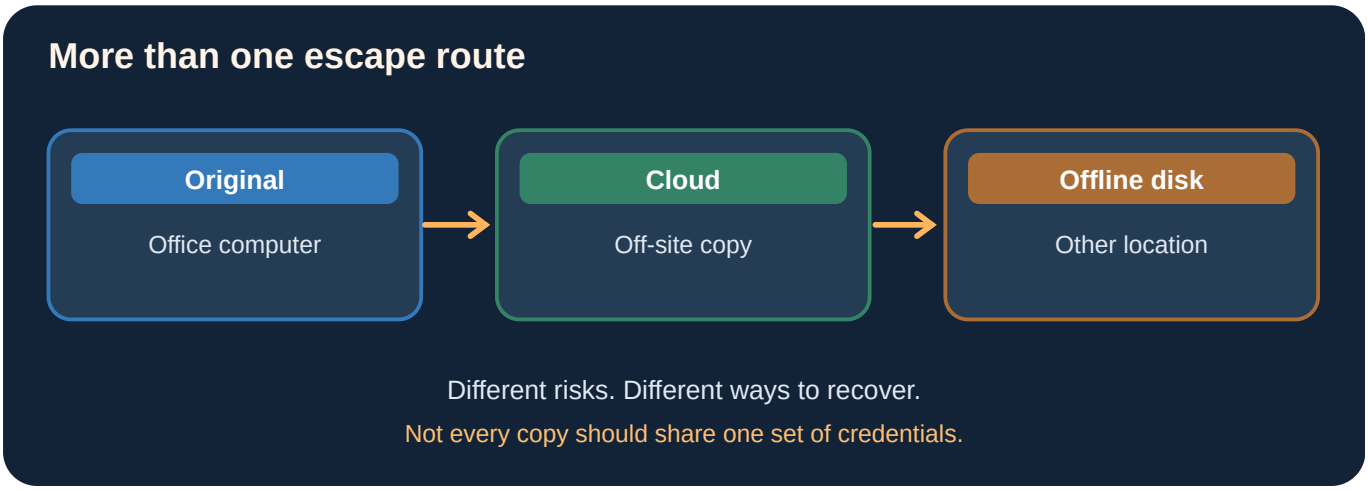
Chapter two: one warehouse, several escape routes

The manager calls a meeting.

— FROM TODAY WE KEEP BACKUPS EVERYWHERE!
— In the office, another building and the cloud?
— YES! AND AT THE ACCOUNTANT'S HOUSE!
— IN THE FRIDGE TOO? — asks Frank.
— IF IT FITS!
— Boss, a fridge isn't a suitable hard-drive storage cabinet.
— THEN BUY AN IT FRIDGE!

🤣🤣

Here's the point: **don't put every way of recovering your data within reach of the same disaster**. Disk failure, human error, theft, fire, flooding, provider trouble and account compromise are different risks. An off-site copy helps with some of them, but distance alone doesn't always protect against remote deletion.



A backup drive permanently plugged into the same PC is better than nothing, but won't solve everything. Another device, cloud storage, an off-site location or a disconnected drive can reduce different risks. This isn't about buying the most expensive product. It's about independent failure scenarios and proving that restoration works.

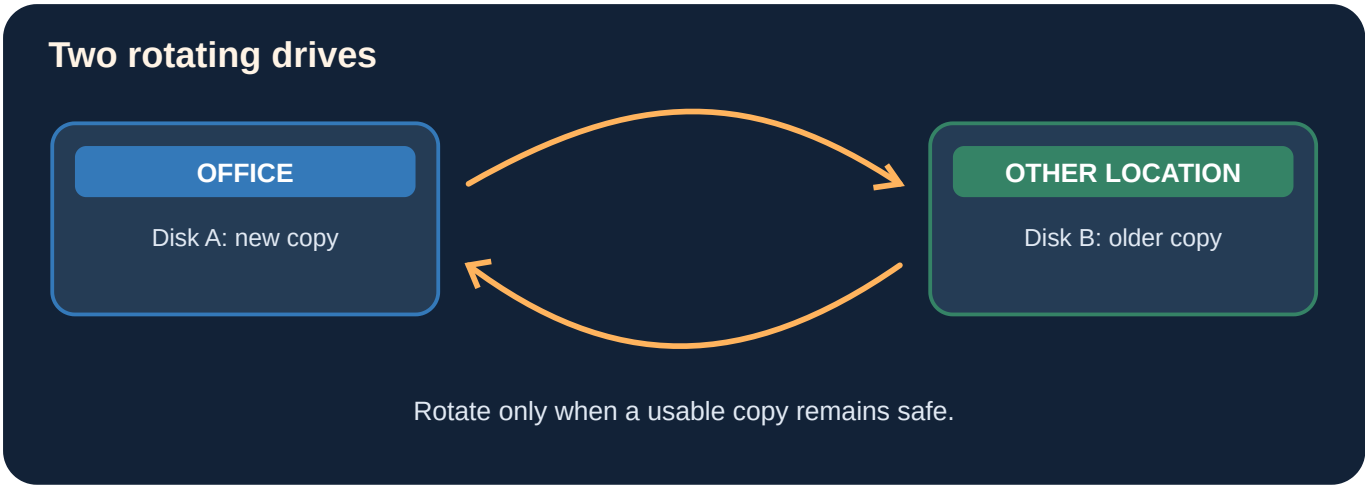
Chapter three: two drives take turns travelling

Frank arrives with two external drives.

— We'll back up onto one in the office. The other stays at another location. Then we swap them.
— SO THE DRIVES GO ON HOLIDAY?!
— Yes, but not both at once.
— WHAT IF ONE GETS LOST?!
— That's why we have another, and we verify the copy.
— THEN BOOK THEM RETURN TICKETS!

🤣

Rotating external drives can be a perfectly reasonable solution. Make a backup, safely disconnect the drive, keep it at another location, and use the second one in the next rotation. Arrange swaps so you don't remove the last verified copy from a safe place before the next one has been successfully completed.



A drive in a home, office or a secure cupboard elsewhere can be useful. You don't need Fort Knox. You need common sense: **dry storage, reasonable temperatures, protection from moisture and shock, and no casual access by strangers**. A protective case helps during transport; keeping the disk out of sight helps when travelling.

— BOSS! THE BACKUP IS OUTSIDE THE OFFICE NOW!
— WHERE?!
— ON THE REAR PARCEL SHELF OF THE CAR!
— WHAT'S THAT SIGN ON THE WINDOW?!
— “COMPANY BACKUP DRIVE. PLEASE DON'T STEAL”.
— FRANK! YOU'VE JUST ADVERTISED IT TO THIEVES!

🤣🤣

Don't leave backup drives in a hot car or visible to passers-by. A portable backup must be physically protected, and drives containing sensitive information should generally be **encrypted**.

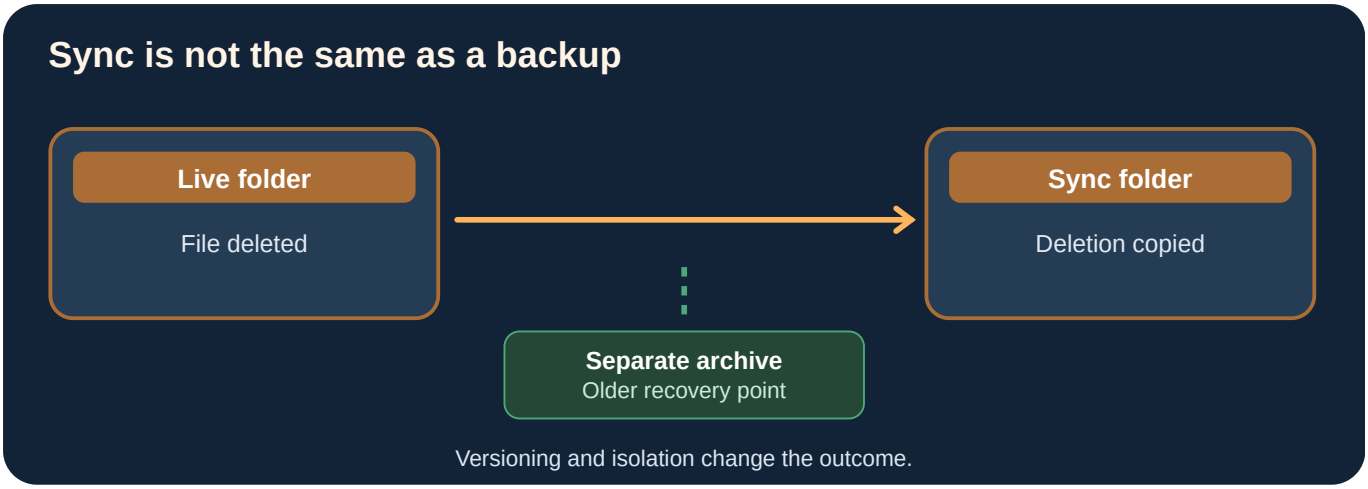
Chapter four: the cloud doesn't bite. But it can synchronise disasters

— BOSS! ALL THE DOCUMENTS ARE IN DROPBOX!
— BRILLIANT! WE HAVE BACKUPS!
— It depends.
— DEPENDS ON WHAT?!
— If it's only a synchronised folder, deleting a file can delete it on the other devices too.
— THEN WHAT KIND OF BACKUP IS THAT?!
— Primarily synchronisation.
— THEN SYNCHRONISE IT SO NOTHING DISAPPEARS!

🤣🤣

Dropbox, OneDrive, Google Drive and similar services can absolutely be part of a good backup strategy. You need to understand their version history, deleted-file **recovery**, retention, permissions and independent archive options. A folder synchronised one-to-one doesn't by itself guarantee safety against

accidental deletion or ransomware.



For example, keep dated archive files, retain multiple recovery points and protect older archives against automatic overwrites. Check the actual limits of the service you use and test restoring files. There's no rule requiring a dedicated enterprise backup product if a simpler service has been deliberately and safely configured for the job.

Chapter five: an archive the backup agent cannot erase

The IT administrator enters.

— Boss, automatic backups are useful, but older archives need protection too.
— FROM WHAT?!
— Someone taking over the backup agent's account, for instance.
— THEN TELL THE AGENT TO BEHAVE!
— Better not to give it permission to delete historical archives.
— WHAT?! MY OWN AUTOMATION CAN'T DO EVERYTHING?!
— Exactly.

🤣🤣

One useful approach is **separating regular backups from long-term archives**. Verified recovery points can periodically be copied or transferred into an area managed by a separate mechanism, without granting the production backup agent permission to change or delete older archives.



Real permissions and access separation matter more than naming a folder “SECRET — DO NOT TOUCH”. **Offline** copies (physically disconnected), **off-site** copies (stored elsewhere), and **immutable/WORM** archives (protected from changes for a defined period) are different properties. An off-site backup may still be online, and an immutable copy needn't be outside the building.

— FRANK, WHY CAN'T THE BACKUP AGENT SEE OUR OLD ARCHIVES?!
— Because if someone compromises it, they shouldn't be able to delete them.
— SO I'M PAYING FOR SOFTWARE THAT DOESN'T KNOW WHERE OUR DATA IS?!
— That's part of why the data can survive.

With multiple backup layers, watch out for damaged or unwanted changes spreading through every subsequent copy. Preserve historical recovery points, manage retention and periodically verify integrity and restoration.

Chapter six: full, incremental, differential and snapshot

The manager demands definitions.

— I WANT A FULL BACKUP!
— We copy the entire selected dataset.
— WHAT IF ONLY ONE INVOICE CHANGES?!
— An incremental backup can record changes since the preceding backup in its chain.
— AND DIFFERENTIAL?!
— Usually changes since the last full backup.
— SNAPSHOT?!
— A view of the data at a point in time, depending on the system.
— GENTLEMEN, I ASKED FOR AN INVOICE COPY AND GOT FOUR NEW WORDS!

🤣

A **full backup** covers the planned set of data. An **incremental** typically captures changes since the previous backup in the chain: it saves space but restoration can depend on several pieces. A **differential** typically includes changes since the last full backup, growing as time passes. A **snapshot** freezes a point-in-time view, often using filesystem or block-storage features. A snapshot on the same machine isn't automatically an independent copy elsewhere.

Retention defines how long we keep recovery points. It may depend on age, data importance and storage space. “Keep archives for as long as capacity allows” can be reasonable, provided space is managed so the last good recovery point isn't accidentally removed.

Chapter seven: ransomware visits the warehouse

The doors fly open.

— HELLO! I'M HERE TO ENCRYPT ALL YOUR DOCUMENTS!
— SECURITYYYY! — shouts the manager.
— Your server's already **encrypted**.
— WE HAVE A NAS!
— Same compromised account had access.
— ANOTHER SERVER!

— Same administrator password.
— ...
— **Encrypted** that too.
— What about the disconnected drive at another location? — asks the accountant.
— WHAT DRIVE?! — asks the intruder.
— The one under my socks.
— DEAR ACCOUNTANT... MAY I HUG YOU?!

🤣🤣🤣

Once a server or account is compromised, every reachable copy may be at risk. Independent accounts, least-privilege access, isolation, versioning and offline or immutable backups all help. **An obscure folder name is not a security boundary.** An unusual design can be beneficial, but only if it's backed by real controls.

Chapter eight: an encrypted drive and a password on a sticky note

— BOSS! I'VE **ENCRYPTED** THE BACKUP!
— WONDERFUL! AND THE PASSWORD?!
— On a sticky note.
— WHERE?!
— Stuck to the drive.
— THEN WHY THE HELL DID WE ENCRYPT IT?!

🤣🤣

Encryption protects confidentiality, especially if a drive is lost or stolen. It's generally important for business documents, personal data and other sensitive material. For low-value, non-sensitive files, even an unencrypted backup may be better than nothing — provided it doesn't violate confidentiality requirements or applicable rules.

We don't have to put every backup in a military bunker. Use established **encryption** tools, strong keys or passwords, and protections proportional to the risk. **Encryption alone doesn't stop deletion**, and it won't restore your data if the only decryption key is permanently lost.



— FROM NOW ON, NO STICKY NOTES! — declares the manager.
— Where do we store the passwords?
— IN OUR HEADS!

— Whose head?
— MINE!

Three years later.

— Boss, we need the archive password.
— ...
— Boss?
— CAN'T WE RESTORE MY MEMORY FROM A BACKUP?!

🤣🤣🤣

A paper backup of a password or recovery key **isn't automatically a bad idea**. It can work when kept safely and separately from the drive. A properly protected password manager and an independent recovery procedure can also be good options. The worst plan is **encrypting** the only good copy and then losing all access to it.

Chapter nine: can encryption last forever?

— GENTLEMEN! OUR BACKUPS ARE **ENCRYPTED**! SO NOBODY CAN EVER READ THEM?!
— We can't promise that.
— WHAT?!
— Bugs, weak passwords and new kinds of attacks exist. Quantum computing is developing too.
— SO A QUANTUM COMPUTER WILL READ MY INVOICES?!
— Different algorithms face different risks.
— SHOULD I JUST HIDE THE DRIVE UNDER THE SOCKS?!
— Ideally **encrypted**, with the recovery key somewhere safe and separate.

🤣

No practical encryption deployment can be guaranteed 100% secure forever. Sufficiently powerful quantum computers would particularly threaten widely used public-key cryptography such as RSA and elliptic-curve systems. **AES-256**, used for data **encryption**, isn't broken in the same way by known quantum algorithms and remains a strong choice with a correct implementation and strong key management.

This isn't a reason to skip **encryption**. Use it thoughtfully, keep software up to date and remember that a password taped to the drive may be a far weaker point than the cipher itself.

Chapter ten: the 3-2-1 rule and a manager who wants more

— BOSS, PEOPLE RECOMMEND THE 3-2-1 RULE.
— WHAT'S THAT?!
— Three copies of data in total, two types of storage media and one copy off-site, in a common version of the rule.
— CAN I HAVE SEVEN?!
— Certainly.
— IN FOUR LOCATIONS?!
— Absolutely.
— THEN STOP LIMITING MY CREATIVITY!

🤣🤣

3-2-1 is a helpful rule of thumb, not a magical guarantee. You may also encounter **3-2-1-1-0**: an additional offline or immutable copy and zero errors confirmed by verification. What matters most isn't the numbers themselves, but independent failure risks, protection against common deletion and the ability to recover.

Five archives reachable through one compromised administrator account can be less resilient than a few genuinely isolated backups. And a procedure shouldn't become so cumbersome that people stop running it altogether.

Chapter eleven: backup successful! Have we ever restored it?

— BOSS! BACKUP COMPLETED SUCCESSFULLY!
— MARVELLOUS!
— Every day for two years!
— WONDERFUL!
— Have we tried restoring files?
— ...
— Checked the archives for completeness?
— ...
— Tested restoring the whole system?
— WE DON'T MAKE BACKUPS JUST SO WE CAN READ THEM AGAIN!

🤣🤣🤣

A “backup completed successfully” message doesn't prove you can recover what matters. Regularly **test restores**, verify completeness, and remember **encryption** keys, application settings, **databases** and system dependencies. Recovering one file isn't the same as restarting an entire company.

RPO describes how much recent data you can afford to lose (say, one day of work). **RTO** describes how long you can afford to wait for systems to be operational again. Two straightforward questions help you choose backup intervals and methods.

— HOW MUCH CAN WE LOSE?!
— Depends on the data.
— HOW LONG CAN WE WAIT?!
— Depends on the business.
— SO THERE'S NO SINGLE PERFECT ANSWER?!
— Exactly.

Chapter twelve: backups matter at home, too

It's not just business servers that need backups. Family photos, documents, phone files, personal projects and messages may be far harder to replace than a computer.

An old hard drive, a USB stick, a second computer or a cloud copy can be a valuable starting point, provided restoration works. Later you can add automation, another location, version history and protection against deletion. **A backup you never make because the process is too complicated is worse than a simple backup you actually perform.**

Finale: can anything in IT ever be finished?

Three months after the fire, the company has a new building, new servers, several independent ways to recover data and a restore-testing procedure.

— GENTLEMEN! WE HAVE BACKUPS IN SEVERAL PLACES!
— Yes.
— SOME ARE OFFLINE!
— Yes.
— SOME HAVE VERSION HISTORY!
— Correct.
— AND WE'VE TESTED RESTORING THEM?!
— Yesterday. It worked.
— WONDERFUL! THEN WE CAN STOP MAKING BACKUPS!
— No, boss.
— ...
— We need to keep doing them.
— CAN'T WE DO ANYTHING JUST ONCE IN THIS DAMN INDUSTRY AND BE DONE WITH IT?!

The accountant speaks from the doorway.

— You can lose all your data just once.

🤣🤣🤣🤣

Remember three things: there is no stupid backup — having no backup is the stupid part; a simple backup performed consistently may beat a perfect plan nobody follows; and the most important backup is **the one you can actually restore**.

Management reports that the accountant's drive has received an award for services to the company. The socks remain anonymous for security reasons.