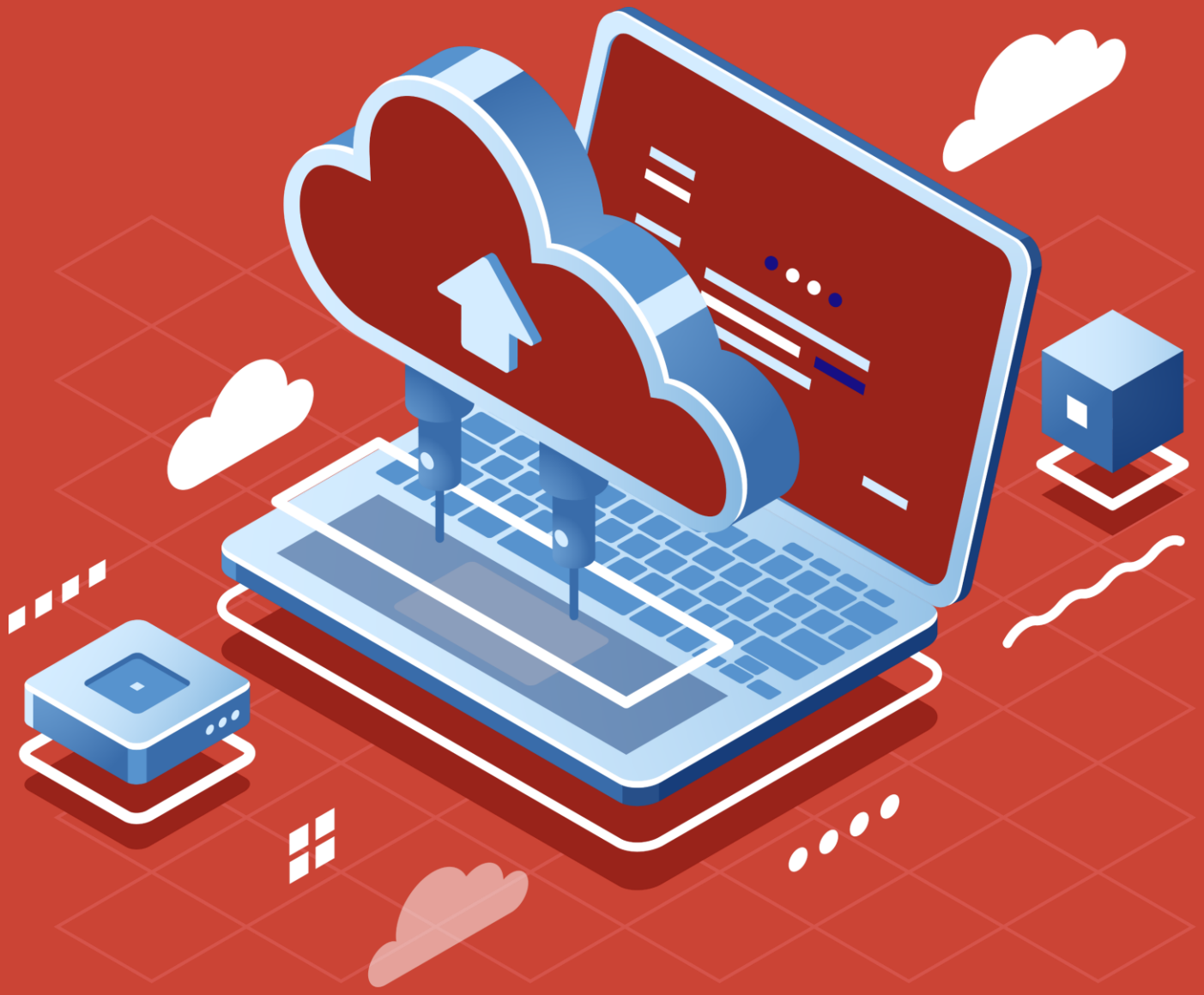
MAXtech



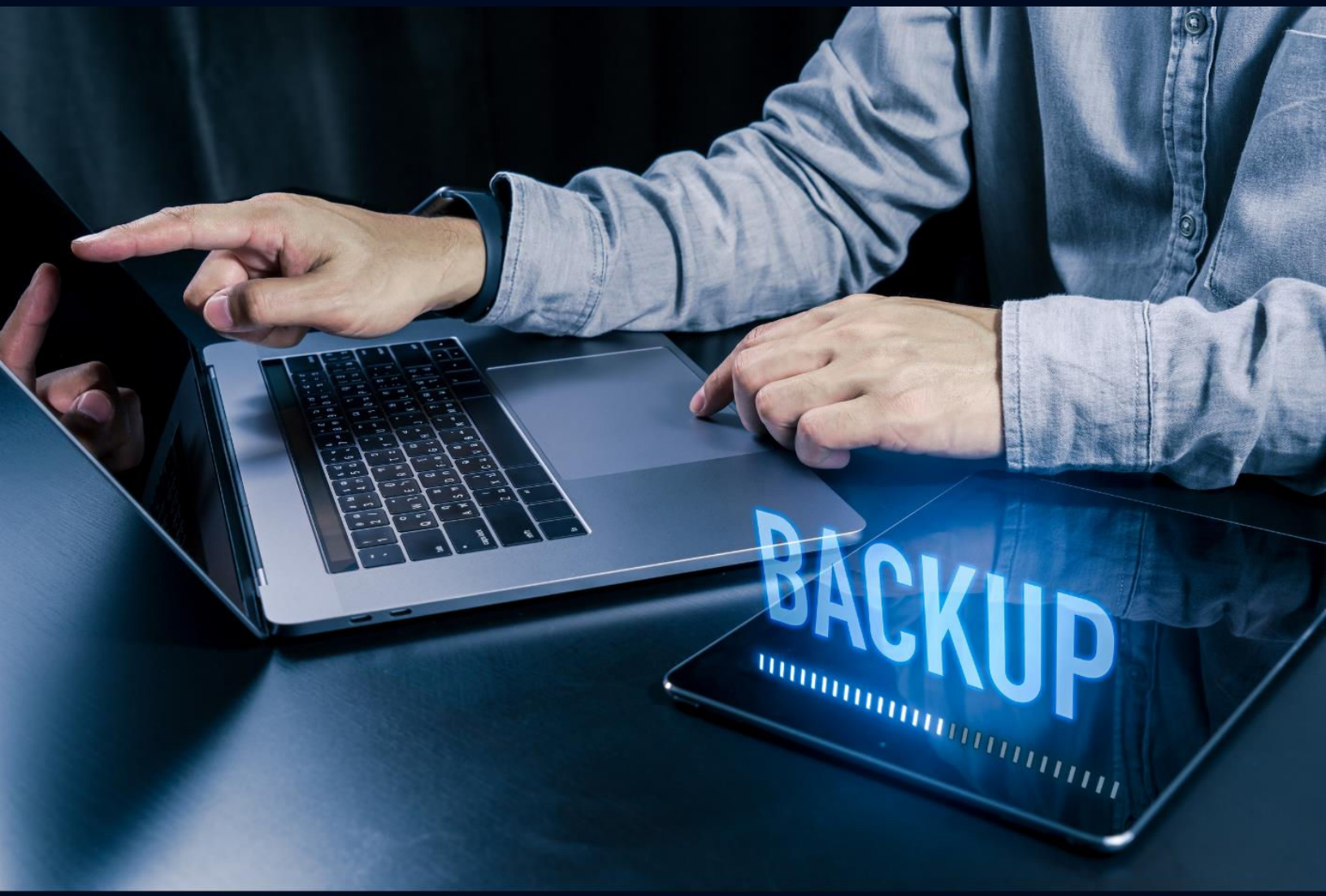
BACKUPS

www.maxtechagency.com

What would happen if you lost all your data? All the digital information related to your business. What would you do? If you can't recover your data, your business likely won't recover either. Everything you've worked for could be lost. So how do you keep your data safe? It's simple: you need to back up your data.

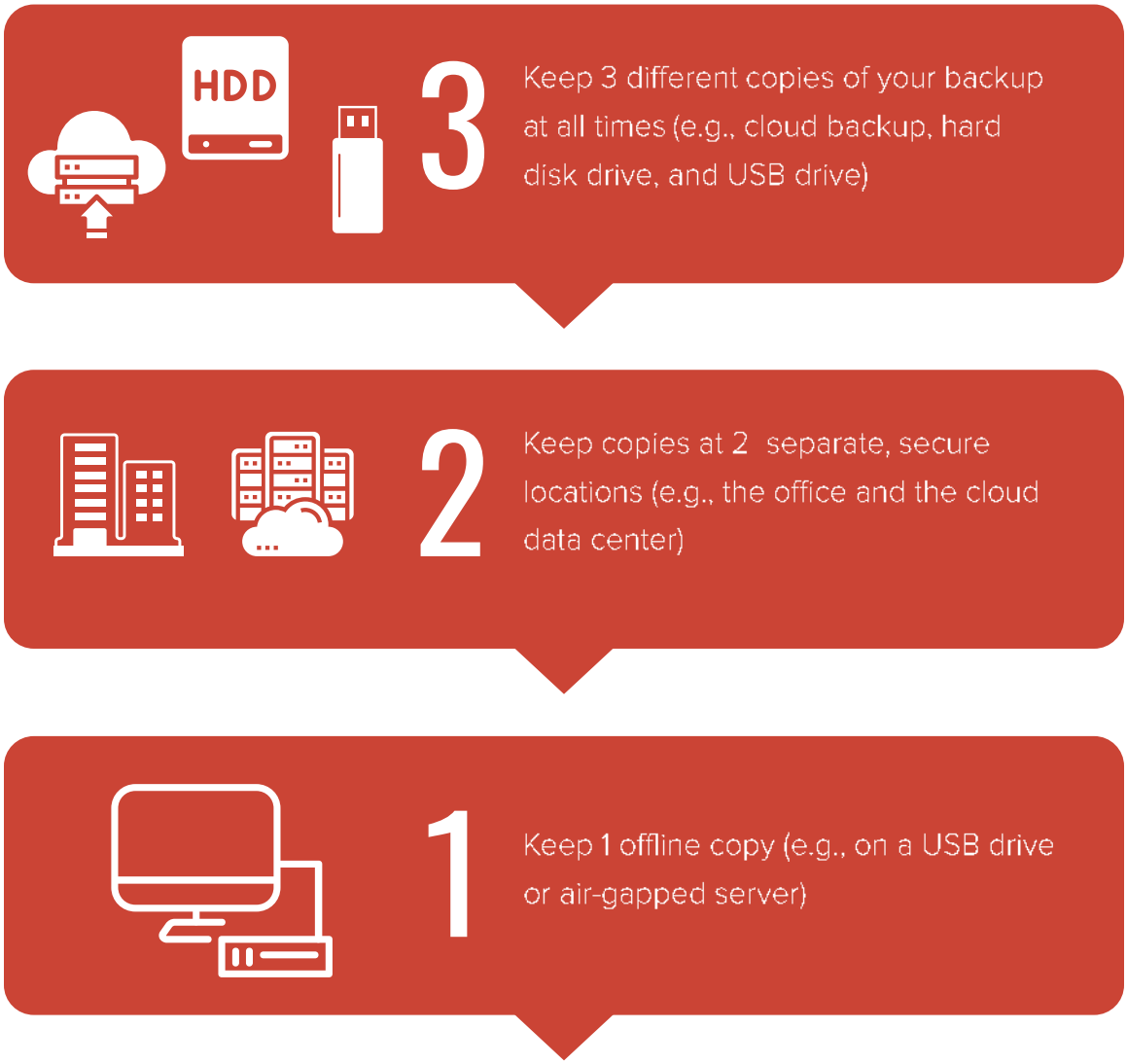
There's no question that your business needs data backups, but it's important that you back your data up properly. If you don't, you'll end up in the same position with no data and a crumbling company.

So how do you go about backing up your data and keeping your information safe? We put together this handy guide that covers everything you need to know about data backups.



Use the 3-2-1 backup strategy

It's not enough to just back your data up once and be done with it. You need to back your data up regularly, and you need to use the "3-2-1" backup strategy:



Following the 3-2-1 backup strategy will help keep your data safe and up to date should you ever need to fall back on it.

Set your retention policy

You need to hold on to your records, but storage space is limited. To get around this dilemma, you can create a sensible retention policy that dictates when backups occur and how long they're retained.

We recommend these guidelines for a good retention policy:

- Back your data up **daily, weekly, monthly, and quarterly**
- Retain daily backups for **1 week**
- Retain weekly backups for **2 months**
- Retain monthly backups for **2 quarters**
- Aggregate quarterly backups into **1 yearly** archive and retain as long as necessary

Test your data restoration procedures

Data backups don't do much good if you can't restore the data. You need a good disaster recovery plan to get your data back. A good disaster recovery plan includes testing your restoration process each quarter and running specific disaster recovery scenarios each year.

Monitor your backups closely

Have a designated staff member in your office monitor the backups and keep an eye on the incoming email alerts. Your IT department (or your MSP) should also be monitoring these alerts, but it's important to have another mailbox receiving the same backup alerts.

Make your data backups immutable

If a hacker infiltrates your network, they can destroy or encrypt your backups and render them unrecoverable unless you pay a ransom. However, modern backup solutions can make immutable backups—that means the backup cannot be deleted nor changed in any way.

Know your RPOs & RTOs

There are 2 key measurables when it comes to data backup and recovery: the Recovery Point Objective (RPO) and the Recovery Time Objective (RTO).

The RPO describes the amount of time that can pass during a disruption before the data that has been lost exceeds the disaster recovery plan's tolerance threshold. For example, your disaster recovery plan might allow for 20 hours of RPO. If you experience a service disruption 15 hours since your last backup, you're within your defined RPO. If it's been 22 hours since your last backup, you're now outside of your RPO, and the lost data could negatively affect your business.

RTO time is the estimated time needed from the start of the resolution process to the moment the system is fully operational again. Different disaster scenarios have different recovery procedures and different RTO times. For example, a hardware failure on a server will have a longer RTO than a software failure on the same server, since it will take more time to receive and replace the hardware.

Don’t rely only on cloud storage

Cloud storage and backups are great for keeping copies in separate locations, but you should not solely rely on cloud backups. Think of it this way: having 3 cloud backups in 3 locations doesn’t fulfill the 3-2-1 rule because you’re only relying on 1 form of storage.

What’s more, cloud storage isn’t necessarily more secure than other forms of storage. The storage “cloud” itself is just a super-secure server in someone else’s data center, so you’re entrusting your data into someone else’s care. If their data center is compromised, your cloud backups could be compromised too.

Encrypt your backups

If hackers do get their hands on your backups, you want to make sure those backups are encrypted with “client-side encryption” (CSE). That means hackers can’t access or do anything with your backups without decrypting them, which is likely far more trouble than it’s worth.

MAXtech has your backup needs covered

No matter the size of your business, there’s no question you need good backup procedures and disaster recovery plans. We’re here to make that easy for you.

Our experts can set you up on a scheduled cloud backup—complete with monitoring and alert software—help you with your other storage media and locations, and ensure you have a comprehensive disaster recovery plan in place.

Talk to one of our experts today to see what MAXtech can do for you. Call us at 614-401-8800.