Microsoft 365 Backup (Myths and Truths)

Why Cloud Backups Are Often Misunderstood

- A lot of companies think that just because their data is hosted in the cloud automatically, then that means it will be completely secure.
- Microsoft has a large amount of customers who use their Suite 365 for email, files and ways to collaborate.
- Customers think that because Microsoft stores their data in very secure global data centres that Microsoft takes care of backing their data up all the time.
- This is a widespread misunderstanding about how Cloud Services operate.
- When Microsoft creates a safe and sound platform for their users, they protect the platform's availability but they do not guarantee a full backup of any user's data.
- Companies and organisations are responsible for protecting and backing up their own data, even though they use Microsoft 365.
- Losing emails or shared documents could severely interrupt your business operations.
- Establishing a proper backup will provide your business/organisation with another level of protection against your most critical data and by doing so, you can avoid the risks associated with not backing up your critical data.

How Microsoft 365 Stores Business Data

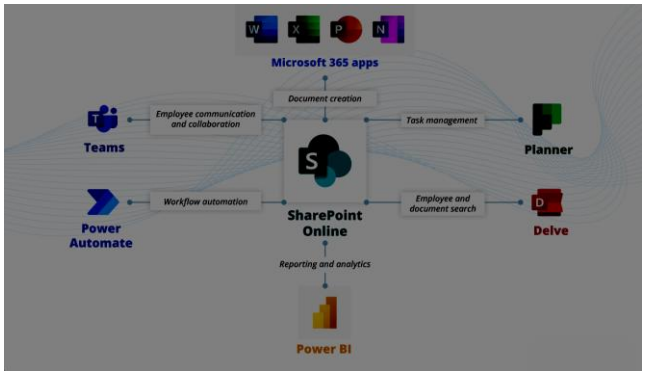
Microsoft 365 consists of multiple inter-related services:

- **Exchange Online:** houses your emails and calendar items
- **OneDrive:** houses users' files
- **SharePoint**: houses files accessible by all company personnel.
- **Teams:** houses conversation and associated files (in SharePoint)

All of your information is housed in the Microsoft cloud infrastructure & synchronised across your multiple devices. Therefore:

- **Edit a file on your laptop:** updates everywhere
- **Delete a file:** deletes everywhere
- **Encrypt a file (due to virus/worm):** replicates everywhere

The ability of your information to be synchronised is powerful, but conversely, creates high levels of risk associated with failure points.



What Microsoft Protects vs What Businesses Are Responsible For

The Cloud Services that Microsoft provides uses a Shared Responsibility Model to deliver the services you use. This means that while Microsoft holds many of the responsibilities for the services it operates, customers also retain some of those responsibilities.

Microsoft’s Responsibility (at Microsoft's Data Centres):

- Data Centre Infrastructure
- Reliability of Hardware
- Availability of the Platform
- Security of the Network
- Availability of the Service

If there is an issue at a Microsoft Data Centre that is caused by Hardware Issue, Microsoft Will Automatically Restore the Service for You.

Customer Responsibility:

- Accidental Deletion of Files or Emails
- Mistakes By Employees
- Cyber Attacks
- Ransomware
- Misuse By Internal Users of Data
- Data Retention
- Regulatory and Compliance
- Backup Data Independently

To put it simply, Microsoft will provide you with a platform that works, however, it is your responsibility as a business to protect your data within the Cloud Services.

Companies and organisations that rely on Microsoft 365 to perform their everyday operations need to understand the difference between Microsoft and their Company or Organisation’s responsibilities.

Common Microsoft 365 Backup Myths

Myth #1: "Microsoft automatically makes back ups of everything"

- **Reason We Believe This:** Since Microsoft is a cloud service, we think it is backing everything up.
- **Truth:** Microsoft does not provide full back up solutions, they provide data retention. This feature restricts the retention (length of time keeping the data) of your data and is not intended for long term recovery.
- **What To Do Instead:** Use a separate independent back up solution that can create and store separate copies of your data.

Myth #2: "I can always recover deleted files"

- **Reason We Believe This:** Because there is a recycle bin and the option for recovering files.
- **Truth:** Deleted files can only be recovered for a specific period of time (generally 30 to 93 days depending upon which service).Once that amount of time expires, the deleted files are permanently lost.
- **What To Do Instead:** Create a back up system that retains your files for an extended amount of time (for instance, retain 1 year or 7 years depending upon business needs).

Myth #3: "Ransomware can¹t infect Cloud Storage"

- **Reason We Believe This:** We think cloud storage is a secure and stand-alone storage solution.
- **Truth:** If ransomware infects a computer or device and encrypts files, those files will become synchronised with the Cloud when the Cloud is set up to sync with that device.
- **What To Do Instead:** Create back up sets that are immutable (not able to be altered by ransomware or other methods) and isolated from your computer or device.

Myth 4: “Version history acts as a complete backup”

Why people believe this: A person can revert back to earlier versions of a file.

The truth about version history is:

- It has limitations.
- It can be overwritten.
- It doesn't provide long-term protection for files that have been deleted.

What to do instead: Use a backup method that backs up multiple copies of the same file; that's what a backup should do.

Myth 5: “Recycle bins are permanent filing cabinets for company data”

Why people believe this: After the customer has deleted a file, it is stored in the recycle bin.

The truth about recycle bins is:

- They are only temporary storage spaces with limited amounts of time before they are emptied.

What to do instead: Consider recycle bins as temporary storage spaces and not as backup storage.

Myth 6: “Small businesses do not need to back up their data”

Why people believe this: "We are small, no one is going to go after us."

The truth about small and medium-sized businesses is:

- There is a greater chance of a small or medium-sized business being attacked because of limited resources available to them.

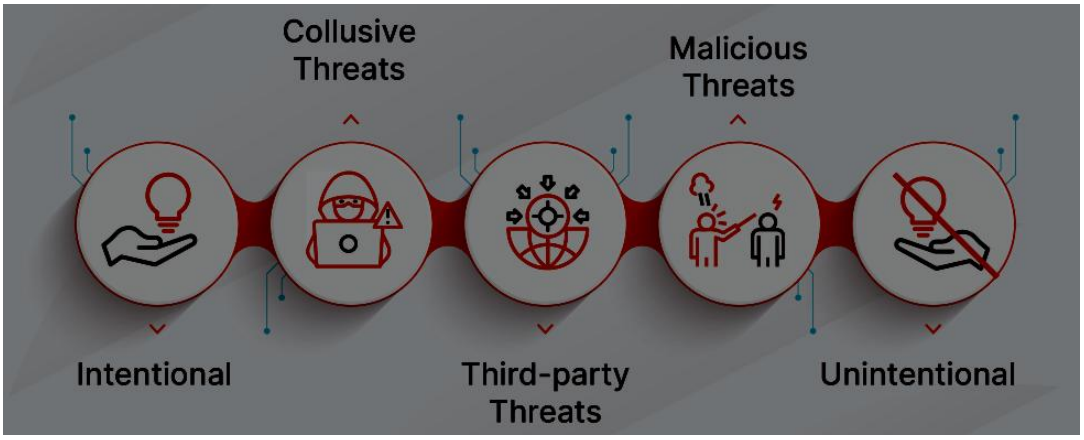
What to do instead: Use easy, cheap backup options this will save your business money compared to losing your data.

The Real Risks to Business Data

The actual triggers of data loss in the SME market in the UK are:

- Accidental deletion: staff unintentionally deleting files;
- Malicious insiders: disgruntled former employees deleting data;
- Ransomware: files being encrypted and synced to all systems;
- Sync issues: corrupted or missing files;
- Retention limits: files being deleted after a predetermined period of time;
- Overwriting: saving changes over important data;
- Compliance: needing to keep historically accurate data.

For most businesses, data loss isn’t dramatic – it occurs every day through human error.



Why Independent Backups Are Important

An independent backup is defined by

- The fact that it will be held somewhere other than Microsoft 365;
- The fact that it will not be impacted by the original user's activity;
- The fact that it will be safe from ransomware;
- You will be able to recover your data at any time.

A good independent backup is essentially the safety net for your whole business.

Without one, you will have limited, time-sensitive options for recovering your lost data.

Microsoft 365 Backup Checklist

- Back up all Microsoft 365 Services of Various Types
- Perform Automated Backups Daily
- Store Long-Term
- Use Secure, Isolated Locations to Store Your Backups
- Test Your Backups Periodically

Cloud Data Protection Checklist

- Have Strong Passwords + Multi Factor Authentication (MFA)
- Provide Access Controls
- Train Staff on Cloud Data Protection
- Monitor Activity and Provide Alerts
- Verify Your Backups

Questions to Ask Your IT Provider

- Do we have separate independent backups for Microsoft 365?
- How long do we keep our data?
- How fast do we have the ability to restore data?
- Are backups safe from Ransomware?
- When was the last time we have done a restore test?

FAQs

1. Is there a backup for Microsoft 365?

Microsoft offers data redundancy and short-term recovery services through its platforms, however, backup services/instruments are not included in Microsoft 365.

It is required for all businesses to protect their own data.

2. **For how long does Microsoft keep deleted items?**

Deleted items in Microsoft 365 have differing retention policies between services. However, over several weeks and months files can be permanently removed from the service.

For this reason independent backups are highly encouraged.

3. **Is it possible for a ransomware attack to affect my data stored in the Microsoft 365 environment?**

Yes, if ransomware was to encrypt your files on a device with direct (synchronization) access to the cloud, those encrypted copies of the files would also become available in the cloud.

Having backup copies of your data allows businesses to restore clean file copies.

4. **What type of data would I want to back up from Microsoft 365?**

Popular workloads typically include:

- Mailboxes (Exchange Online)
- OneDrive files
- SharePoint Online
- Microsoft Teams data
- Contacts and calendars

5. **What are the best backup intervals for Microsoft 365?**

Most businesses have a successful backup schedule of running daily backups, however; the best time frame is based on how much the business changes its data.

About This Guide

The **Computer Support Centre** has produced this comprehensive guide to assist small and medium sized businesses in the UK to help them through the confusion that is the misunderstanding of data protection with Microsoft 365. A lot of organisations mistakenly believe that because their email, files and collaboration tools are stored on a cloud platform, they automatically have a backup of their data on this cloud platform and that their data is fully protected through the Microsoft 365 service.

This informative guide explains the difference between Microsoft's responsibility to maintain a cloud platform and the business' responsibility to protect their data. It also highlights the common myths surrounding Microsoft 365 backup services, the real world risks of losing your data, and why independent backup solutions are important for protecting your business information.

Using straightforward explanations, real life examples, and a series of practical checklists, this guide provides and assists owners and/ or managers of small to medium-sized businesses to better understand their responsibilities as they relate to ensuring that they have protected their critical business data against the potential of losing their information due to a system failure or corruption.

If you learn more about **Computer Support Centre**, our services, and our approach, please visit our official website:

 https://computersupportcentre.com

Conclusion

Although cloud services such as Microsoft 365 offer a reliable platform and powerful collaboration tools, they should not be considered a substitute for making sure that you have proper backups of your data. Many organisations believe that simply storing their information on the cloud ensures complete protection from accidental deletions, cyber attacks, ransomware.

To understand how this works, you need to know about the "shared responsibility" model. Microsoft is responsible for the availability of its platform and securing it from outside threats, but businesses are responsible for protecting their own data and backing it up. Without independent backups, organisations are limited in what options they have to recover lost emails, documents, or other collaboration items.

Business owners can reduce the risk of data loss by using regular independent backup solutions and implementing strong data protection practices. Proper backup planning not only protects important records, but also provides assurance of business continuity, complies with regulatory requirements, and provides long-term operational stability.