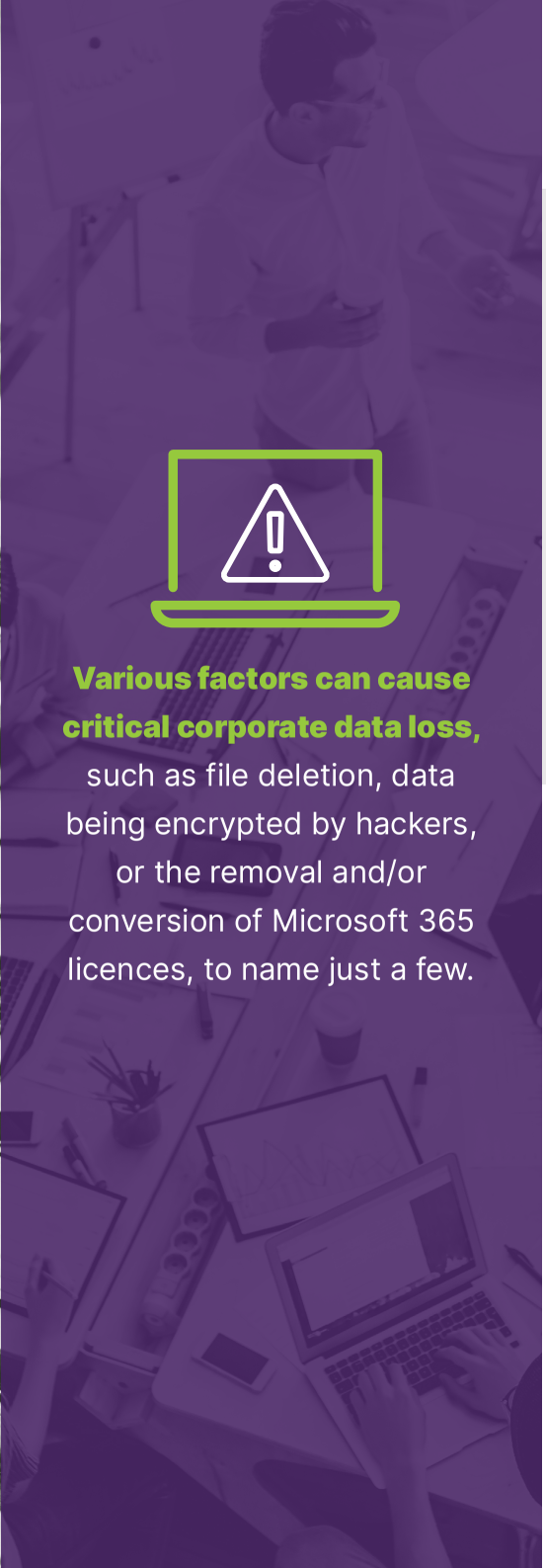
CARBONITE
an opentext company

Why Carbonite® Backup for Microsoft 365 is essential for your business data protection plan

Data is a valuable company asset and if it gets lost, this can have serious consequences for a company.

Gabriëlle Offringa, Sr Marketing Manager of EMEA Carbonite, an OpenText company



Various factors can cause critical corporate data loss, such as file deletion, data being encrypted by hackers, or the removal and/or conversion of Microsoft 365 licences, to name just a few.

WHAT IT'S ALL ABOUT

Microsoft 365 applications such as Exchange, SharePoint, OneDrive and Teams are essential cooperation tools for companies. Microsoft is seeing a rapid increase in cloud licences with the rise of cloud computing. But as a company, have you ever asked what this means for your backup and storage plans? Do you already have a solution for your company to save and store company data in the Microsoft 365 suite securely? These questions are often left unanswered because for most people Microsoft 365's backup and retention principles are unclear.

According to a survey conducted by the Enterprise Strategy Group, one in four companies believes backing up is not necessary for Microsoft 365 (source: ESG Master Survey Results, Data Protection Cloud Strategies, June 2019).

In this white paper, we will provide you with an overview so that you can decide for yourself what's necessary and what isn't in terms of backup and recovery for Microsoft 365 and the data stored in applications such as Teams, OneDrive, SharePoint, etc.

Microsoft offers:

- Protection against data loss through service issues, hardware errors or natural catastrophes.
- Short-term protection of data against errors by users and/or administrators (recycle bin, soft delete).

But where are the data in the following cases?

- If files or chat logs are intentionally or accidentally deleted: if, for example, someone completely deletes something on a shared OneDrive or SharePoint or data is intentionally erased from emails or chat logs from Teams. If this isn't noticed quickly enough, the data may be lost forever.
- Hackers gain access or plant ransomware or other types of malware: if they attack files in OneDrive, for instance, there is a high risk of never again being able to access the data in an undamaged state.
- When transferring a Microsoft 365 licence from one employee to another if, for instance, an employee leaves, the former employee's data (including their contacts and all data in Exchange) may go missing.

Misunderstandings about backups for Microsoft 365

Switching to Microsoft 365 in the cloud does not mean that data is fully and automatically saved and stored in the cloud. Some people incorrectly assume that Microsoft is responsible for the security and long-term storage of data in the Microsoft 365 suite. Carbonite recommends implementing a regular backup schedule to ensure that Microsoft 365 data is backed up and stored in full. For further information, please contact our data backup specialists.

Reasons for data loss

Microsoft 365 data is often exposed to the same risks as locally hosted data.

Accidental deletion

The first and most obvious concern is the accidental deletion of data, files and directories. Employees at your company can easily delete data and chat logs in SharePoint, OneDrive or Teams, or overwrite versions of stored data. It is often possible to restore the deleted files from the recycle bin, but this data is only saved temporarily.

Intentional deletion

In some cases, however, data is deleted intentionally. A disgruntled employee can delete files in shared applications intentionally.

Theft

If an external party gets hold of a lost or stolen laptop with access to Microsoft 365 applications, they can remove or modify everything from shared folders.

Backup issues

Ransomware (and other malware) is able to encrypt files in Microsoft 365, which can have knock-on effects for many users. A user who downloads the wrong file by mistake can copy infected files to the cloud using the OneDrive sync feature and thus spread a virus and cause a host of problems.

Closure of an account

If you remove a Microsoft 365 licence for one employee and then assign it to a new employee, the data may potentially be lost.

What about OneDrive?

If companies use OneDrive to save files, a backup and recovery solution is definitely required if one is not already in place. All OneDrive files are in the cloud but this does not automatically mean comprehensive backup and recovery functions are in place.

+ If a file is deleted from a local device or becomes infected, this change is synchronised automatically in OneDrive If there is an Internet connection. To be more precise: the file is automatically deleted or infected on all synchronised devices.

+ Carbonite Backup for Microsoft 365 offers native backup features and flexible recovery options for user data on OneDrive, in addition to the Microsoft 365 recycle bin and file version history. This combination provides companies with flexible recovery mechanisms.

+ Microsoft OneDrive's recovery function is a form of 'destructive recovery'. It restores the data to an earlier point in time. In other words, the data content is restored to a previous state but the newer versions are lost in the process. With Carbonite, you can undo changes without losing newer content, which is a convenient form of damage control.

+ OneDrive can quickly spread malware such as ransomware through its real-time synchronisation function. With Carbonite Backup for Microsoft 365, you can restore the files to the point in time before they became infected.

The recycle bin

OneDrive offers some recovery options via the recycle bin, but the recycle bin lacks many of the properties of a true backup system:

+ File versions are not immutable, isolated recovery points. If an active file is deleted, all older versions of the file are also deleted. If files are permanently deleted from the recycle bin, they can no longer be recovered.

This makes centralised user data management impossible. In other words, the IT department has no control over backing up and recovering data.

With Carbonite Backup for Microsoft 365, recovery points for files, directories and users are managed in such a way that they can be restored more easily as required.

Why Carbonite Backup for Microsoft 365?

Carbonite Backup for Microsoft 365 protects the entire Microsoft 365 suite. Backups are performed automatically up to four times a day or every six hours. You are able to select longer intervals and the exact time that these backups are performed. Backups are stored in the secure Carbonite cloud hosted by Microsoft Azure.

Flexible recovery options

There are many ways in which company data can be lost. This is why it's important to have various recovery options to ensure that you only restore what you need. This speeds up recovery times and reduces the workload for IT. Carbonite Backup for Microsoft 365 offers several recovery options.

Central administration and security

Carbonite Backup for Microsoft 365 enables administrators to track, manage and report backup and recovery commands via a central console. The console enables you to see how backup and recovery services are used. The solution can also send email notifications featuring a detailed overview of backup and recovery information.

This is not just extremely important to protect files shared in OneDrive or SharePoint, but also data in collaborative tools, e.g. in Teams.

WHAT OTHER TYPES OF PROTECTION ARE NEEDED?

Carbonite® Endpoint

Carbonite also protects data on employee endpoint devices. Carbonite® Endpoint is a comprehensive, automatic backup solution for endpoints and the data stored in them. Carbonite® Endpoint simplifies the administrative tasks associated with deploying protection across an entire organisation.

- Centralised control: Centrally manage and restore user data and minimise data loss with audit trails, monitoring and alerts.
- Remote management: Recover data from a device remotely and restore to the same device in the same location or restore the data to an entirely new device.
- Incremental restore: Migrate an entire system to a new device while the user continues to work on the old device or a temporary device.

Carbonite® Endpoint and Carbonite® Backup for Microsoft 365

With protection for both physical devices and cloud applications, businesses can reduce the possibility of data loss for a far wider range of scenarios, and ensure recoverability for a larger share of use cases.

- Ensure protection of collaborative tools and not just files.
- Minimise the risk of data loss caused by ransomware and user error.
- The solution is easily scalable using a licence model per user.

> *Carbonite Endpoint and Carbonite Backup for Microsoft 365 enable businesses to protect all data generated by their users on Endpoint devices and within Microsoft 365.*

THE DISTINCTIVE NATURE OF CARBONITE BACKUP FOR MICROSOFT 365

Change permissions

Restoring just permissions is not an issue. The content remains unchanged only the permissions are changed without requiring user intervention.

Save data from former employees

Restructure the administration of directories to enable the new user to also access the former user's files.

Recovery for Microsoft Teams

Backup and recovery for Microsoft Teams, including conversations and the SharePoint site behind Teams.

Granular recovery

It is not necessary to recover the entire SharePoint site for example. Small portions of it can be restored instead, which makes the process quicker and more secure.

BYOK

An IT administrator can implement encryption using a key (Bring Your Own Key) for additional security, which ensures that the data can only be decoded by the same IT administrator.

GDPR

The GDPR stipulates that it must be possible to delete personal information upon request by the data subject. The search function at the file level makes it easy to locate data linked to a person and remove this data as appropriate when required.

Fault affecting Microsoft 365

If Microsoft 365 encounters a fault and you are temporarily unable to access your files, you can access the backup files created by Carbonite Backup for Microsoft 365.

Carbonite backup and recovery for business

Secure. Recover. Protect.

Qualifying questions:

- Do your employees use Microsoft 365?
- Do you have a backup and retention policy for Microsoft 365?
- What is your data worth to you?
- Have you already fallen victim to a cyberattack?

Try Carbonite Backup for Microsoft 365 free for 30 days.
https://go.carbonite.com/free-trial-O365-UK

CARBONITE®
an opentext™ company

Contact
Telephone no.: +44 (0)333 1234 200
Email: UK-smbc@opentext.com

About Carbonite and Webroot

OpenText companies Carbonite and Webroot harness the cloud and artificial intelligence to provide comprehensive cyber resilience solutions for businesses, individuals and managed service providers. Cyber resilience means being able to stay up and running, even in the face of cyberattacks and data loss. That's why we've combined forces to provide endpoint protection, network protection, security awareness training, and data backup and disaster recovery solutions, as well as threat intelligence services used by market-leading technology providers worldwide. By leveraging the power of machine learning to protect millions of businesses and individuals, we secure the connected world. Carbonite and Webroot operate globally across North America, Europe, Australia and Asia. Discover cyber resilience at carbonite.com and webroot.com.