Why home working with Teams demands a backup check-up.

Demand for Teams soared by 35 percent in just one week during the early stages of the coronavirus pandemic before jumping a further 70 percent in April alone.

Microsoft's unified communications platform now has 75 million daily active users worldwide, 200 million daily meeting participants, and 4.1 billion daily meeting minutes. It stands to reason then that there is an ever-increasing amount of vital data in Teams that needs protecting.

Organisations can ill afford to assume that, just because Teams is accessed and stored in the cloud, their data is protected from all eventualities. Retention and versioning features provide some protection for Microsoft 365 data, but not enough to preserve business-critical files if something goes wrong and data is lost or deleted.

Why back up Teams?

Microsoft is heavily invested in mitigating against disasters that might affect the availability of Teams, OneDrive, SharePoint and Exchange, but there are certain risks that SaaS providers have no control over. Ransomware, user mistakes, malicious behaviour, sync or configuration errors all threaten an organisation's cloud-based live data.

Section 6B of Microsoft's own Services Agreement recommends using a third-party to back up data. Here are some of the reasons why:

Accidental deletion

What happens when users accidentally or intentionally delete or overwrite files? Recycle bins and version histories in Microsoft 365 provide only limited protection. Once an item is purged from the mailbox database, it is unrecoverable.

Backup plans guarantee that your data can be restored quickly and efficiently regardless of human error.

When employees leave the company

When someone deletes a user or users from Active Directory - intentionally or otherwise - once they are outside of retention, their Sharepoint sites and OneDrive data are also deleted. Most of the time, a former employee's Teams data is lost because many companies lack an efficient way to export it within the application. A third-party backup strategy will ensure that all information gets transferred safely.

Corruption caused by third-party apps

Teams integrates with hundreds of third-party applications, but what happens if one malfunctions, deletes records, or corrupts data? The proliferation of add-on software makes it prudent to take precautions and ensure your data is always retrievable.

Separation of roles as a security standard

Lastly, who will recover sensitive information stored in Microsoft 365 and how much will they be able to see? Are you happy for admins to assign themselves full access to search and export Teams conversations, Exchange mailboxes, SharePoint folders, and OneDrive locations?

Better to have a backup provider that enables the delivery of centralised management without circumventing Microsoft 365 security and auditing.

Malicious insiders

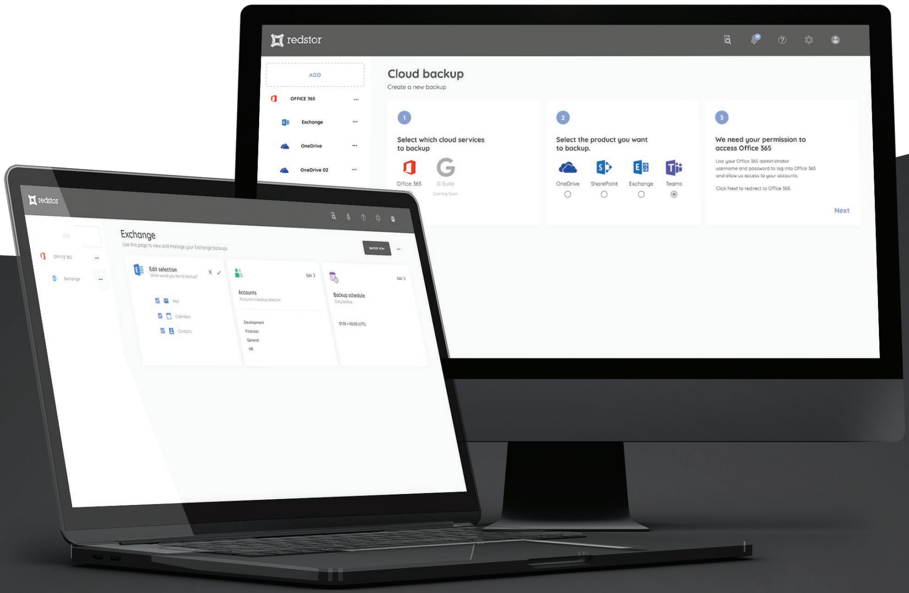
What happens if a rogue employee or resentful contractor with the right user credentials decided to delete incriminating emails or files? It typically takes more than 200 days for someone to realise data has been compromised - yet default settings only provide you with 30 to 90 days in which to act. Microsoft's backup and retention policies can't take the place of third-party data management solutions.

Ransomware attacks

Regular backups will help ensure a separate, uninfected copy of your data is always available, which ensures that you can recover mailboxes quickly to an instance before the ransomware attack. The best data management providers offer streamed, on-demand access to all data instantly.

Next step: True cloud-to-cloud protection

You are responsible for your Microsoft 365 data - and with a third-party backup strategy, you mitigate the risk of storing it solely with the cloud service provider. You stay in full control for business continuity. Modern businesses need a unified view of all their data whether it is in Teams, elsewhere in the cloud, stored on-prem or in a hybrid environment.



Cloud backup

Create a new backup

1 Select which cloud services to backup

2 Select the product you want to backup.

3 We need your permission to access Office 365

Use your Office 365 administrator username and password to log into Office 365 and allow us access to your accounts.

Click Next to redirect to Office 365.

Exchange

Use this page to view and manage your Exchange backups

Edit selection

What would you like to backup?

Accounts

Accounts in backup selection

Backup schedule

Daily backup

If you would like to:

- Manage your data environment through one central, easy-to-use system
- Establish consistent protection policies across your entire date estate
- Comply easily with Subject Access Requests, finding and deleting references if required, including in Microsoft 365 backups
- Set up in minutes, auto-scale protection of Teams, Exchange, OneDrive and SharePoint
- Avoid any requirement for local hardware and ensure there's no impact on local bandwidth and no need for local storage

Contact Risc IT Solutions on 01492 862 780 or visit www.riscitsolutions.com