



Creative ITC

SOME OF OUR MOST VALUABLE DATA LIVES
IN OFFICE 365 APPS - AND IT'S AT RISK.

**DON'T SETTLE FOR
SOMETHING THAT
DOESN'T WORK.**

Protecting your business against data loss
requires a more Creative solution.

3 MAJOR RISKS TO YOUR O365 DATA – AND HOW TO AVOID THEM

It's a common misconception that Microsoft fully backs up your data. Microsoft's focus is on managing the O365 infrastructure and maintaining uptime. The responsibility for protecting O365 data is yours.

3 reasons to backup O365 data

- To prevent data loss and corruption
- To avoid downtime if disaster strikes
- To comply with laws and regulations

But avoiding these risks by implementing effective backups across your Exchange, SharePoint, OneDrive and Teams domains is not straightforward as there are so many moving parts to consider. Worryingly, 76% of data stored in Office documents and applications still isn't being backed up, meaning it could become permanently lost.

85%

businesses using O365
suffered data loss
in the past 12 months

3 MAIN CAUSES OF PERMANENT O365 DATA LOSS



2 IN 5

Organisations lost data through user error or accidental deletion.



1 IN 5

Organisations lost data through malicious attack.



1 IN 5

Organisations mistakenly thought data was backed up.

ACCIDENTAL DELETION

2 in 5 organisations lost data permanently through user error or accidental deletion.

Although you can retrieve recent accidentally deleted files and emails from Deleted and Recoverable folders, in many instances the native O365 recovery tools are limited.

If you delete an O365 user, whether you meant to or not, that deletion is replicated across the network, including their OneDrive account and mailbox, meaning their entire account data is erased forever. Deleting O365 accounts is a standard procedure for many organisations, for example to reduce license costs when an employee leaves. User accounts may also be removed inadvertently by human error, as a result of license services ending or when migrating data to another account.

Humans are also widely acknowledged to be the weakest link in an organisation's cyber defences. Employees can unknowingly create serious threats by downloading infected files or accidentally leaking usernames and passwords to sites they thought they could trust. 1 in 4 organisations experienced a security breach resulting from an employee email and 1 in 3 suffered permanent data loss. If an Outlook mailbox is corrupted, and the version history is turned off, any data not backed-up is lost forever as there is no way to restore to a "clean" version and restore it.



MALICIOUS INTENT

1 in 5 organisations suffered permanent data loss through malicious attacks.

Rising cybercrime poses a serious threat to organisations around the world, putting operational continuity, reputation and data security at risk.

External threats such as malware, ransomware and viruses are increasingly infiltrating organisations through emails and attachments. Exchange Online's limited recovery functions are inadequate to restore lost or uninfected data in the face of serious attacks.

Businesses are also facing growing risk from actions by their own employees, resulting in permanent data loss more often than you think. Employees may

deliberately delete critical data if terminated or in an attempt to hide evidence of wrongdoing from legal, compliance or HR departments.

A point-in-time restoration of O365 data is not in scope with Microsoft. In the case of a malicious action by an internal or external person, if you don't have a backup solution in place, you'll be unable to roll back to a previous point-in-time prior to the incident to recover your data.



RETENTION GAPS AND CONFUSION

1 in 5 organisations lost data after mistakenly thinking it was backed up.

Office 365 has limited backup and retention policies and is not intended to be an all-encompassing backup solution.

If you delete an O365 document or email, it usually goes into the Recoverable or Deleted items folder. But if someone has manually removed items from the folder, you won't necessarily be able to retrieve them. Moreover, standard retention time by Microsoft is limited - by default, items are kept and can be retrieved for up to 30 days. So, if you exceed the 30 day retention limit, you won't be able to recover your data.

Microsoft Teams brings together Office 365 services, such as SharePoint Online and OneDrive for Business, providing agile, real-time collaboration and file sharing and making it a popular choice for project teams. Once those projects are complete, you may need to retain the records and associated files. But these Teams records often get mistakenly deleted or retention misapplied, removing access to the messages, files and any associated interconnections between applications.

Sometimes you need to retrieve data for legal or compliance requirements. Microsoft's built-in litigation hold and retention safety nets are not a robust solution. Without an effective O365 backup, you won't be able to retrieve accidentally deleted emails or files to ensure you meet your legal obligations and could face fines or other penalties.



BENEFITS OF CREATIVE'S FULLY MANAGED O365 BACKUP-AS-A-SERVICE



SCALABILITY AS YOUR OFFICE 365 NEEDS EVOLVE

Other solutions don't cover as much of your Office 365 data, nor protect it as thoroughly, leaving you open to loss or corruption. Our complete solution easily scales as your Office 365 estate changes, whether your data sits on premise or in a public, private or hybrid cloud setup, with no impact on your data centre footprint or networking resources, nor need for expensive add-ons, like cloud connectors or point products.



IMPROVES YOUR SPEED OF RECOVERY

Instantly restore your O365 data and select RTO and RPO to better match your business needs, meet regulatory requirements and compliance audits. Short term backups or long-term archives, granular or point-in-time restores, everything is at your fingertips making data recovery fast, easy and reliable.



FULL CONTROL OF YOUR DATA

Our fully managed, optimised solution provides an organisation-wide, real-time view of your data protection status, putting you firmly in control of systems, users and devices and eliminating risk of user error, retention policy gaps and restore inflexibility.

READY TO MAKE YOUR BUSINESS MORE RESILIENT WITH CREATIVE ITC?

To learn more about how Creative ITC can help safeguard your organisation, contact us at hello@creative-itc.com.



Creative ITC

