Backing up your email

(Reprinted from our April 2023 newsletter, because we think it's that important)

Organizations continue to choose Microsoft 365 for ease of collaboration in the cloud. Today, Microsoft 365 is at 300 million commercial seats and growing. Pretty impressive. And we'd like to think Microsoft has guaranteed that all those email mailboxes are safe from loss. Well, not so fast, my friend; we should look at the fine print.

The fine print in this instance is in the form of Microsoft's Shared Responsibility Model (MSRM). In a nutshell, when you subscribe to Microsoft 365, you are agreeing to participate in the MSRM, which means you agree that Microsoft will be responsible for THEIR global infrastructure and their commitment to keeping their infrastructure up and running, consistently delivering uptime reliability of their cloud services. YOUR responsibility is to have complete access and control of your data — regardless of where it resides. This also means protecting the data from loss. To put a finer point on it, if Microsoft loses your data they can, potentially, tell you that backing up your data was YOUR responsibility.

Replication vs Backup

For their part, Microsoft delivers a solid infrastructure and reliable cloud services that include built-in data replication; this provides data center to data center georedundancy. This replication is a necessity. If something goes wrong at one of Microsoft's global data centers, they can failover to their replication target, and in most cases, the users are completely oblivious to any change.

But replication isn't a backup. And furthermore, this replica isn't even YOUR replica; it's Microsoft's. So, what's the difference between a replica and a backup anyhow? A backup is commonly defined as a separate copy of data that's stored in a separate location, from which data can quickly and easily be recovered. Data replication is the process of storing the same data in multiple locations.

While having a replica of your data may sound similar to having a backup of your data, it's important to note that with a replicated copy, all data is copied, whether it was deleted or corrupted, meaning you now have a copy of all good data and all bad data, and as we mentioned, this is Microsoft's data and it's use is not guaranteed to you. Thus, relying solely on Microsoft to maintain and host your data puts your organization at risk of losing control and access to your own company's data.

How to protect your data from loss

The counter to putting Microsoft in the position of sole protector of your data is to protect the data yourself. When we talk about data here, we include your email, OneDrive documents, Teams data and everything you have stored in SharePoint. In short, everything you have stored on Microsoft's 365 servers. There are various third-party solutions that will make the backup process easy, but before we get to that, let's look at some other great reasons to back up your email.

7 Reasons to back up your email

Veem Software, a data protection company, has identified 7 Reasons Why Microsoft 365 Backup is Critical

1. **Accidental deletion:** This is actually the most common cause of data loss in Microsoft 365. If you delete a user, whether you meant to or not, that deletion will then be replicated across the network. A backup (yours – not Microsoft's) could restore that user, either to on-premises Exchange or Microsoft 365.
2. **Retention policy gaps and confusion:** Retention policies in Microsoft 365 are designed to help organizations comply with regulations, laws and internal policies that require that they retain or delete content; they are not backups. But even if you do rely on your retention policy in place of a backup, these retention policies are hard to keep up with,

let alone manage. A backup provides longer and more accessible retention that's all protected and stored in one place for easy recovery.

3. **Internal security threats:** When we think of threats to our business, we usually think in terms of protecting against external forces. However, many businesses also experience threats from the inside, and these issues happen more often than you think. Having a high-grade recovery solution mitigates the risk of critical data being lost or destroyed.
4. **External security threats:** Ransomware is becoming more and more sophisticated, and criminals are finding more ways to reach our users and deceive them into clicking a link that encrypts the entire organization's data for ransom. A backup can easily restore data to an instance before the attack.
5. **Legal and compliance requirements:** There are eDiscovery capabilities built into Microsoft 365, but a third-party backup solution is purposely built to easily search within a backup and quickly bring back data to meet any regulatory compliance needs.
6. **Managing hybrid email deployments and migrations to Microsoft 365:** Whether you are migrating to Microsoft 365 or have a blend of on-premises Exchange and Microsoft 365 users, the exchange data should be managed and protected the same way, which makes the source location irrelevant.
7. **Teams' data structure:** The Microsoft Teams backend is much more complex than many realize. Teams is not a self-contained application, meaning the data generated in Teams resides in other applications like Exchange Online, SharePoint Online and OneDrive. With this added layer of complexity, ensuring that data is adequately protected is paramount.

How to back up your email and 365 data

Many of our TekResults clients use server backup software and external hard drives to back up their servers every night, however server backups only back up things that are stored on the server. Those things usually do not include email. An email backup at the office level wouldn't do you any good if Microsoft were to lose your data. Why? Because Outlook stores your email in an OST file. These files can be backed up, but when you restore them to another computer from the backup, they won't work. Outlook requires a connection to the 365 Exchange servers to keep your mailbox up to date and if Outlook finds an old version of the OST file, it won't use it.

Fortunately, there are cloud-based solutions dedicated to email backup. Microsoft has its own backup solution, but you guessed it, it's not free. At TekResults, we rely on a service called Cloud-to-Cloud Backup, a Zix-AppRiver solution. Zix-AppRiver is the service provider we use for all our email clients, so we already have a relationship with them should you decide to use their 365 backup solution.

Carbonite Cloud-to-Cloud Backup provides a comprehensive solution to protect your cloud applications and data and offers these features.

- Automate backups of Microsoft 365
- Protect against ransomware, malware, data loss and data breach
- Flexibly search and recover items, mailboxes or sites at any granular level
- Easily recover data with point-in-time recovery
- Browse daily snapshots and run searches
- Feel more secure with full redundancy
- Store more with unlimited storage and retention

To get started, or just to ask some questions, give us a call. We'd love to discuss this with you.