ConversationalGeek

Microsoft Teams Backup
Practical Tips

By Brien M. Posey, Microsoft MVP

#1 Make Sure that You Are *Backing Up Microsoft Teams*

Although it might seem completely obvious, the number one best practice with regard to Microsoft Teams backups is to make sure that you are actually backing up Microsoft Teams (and the rest of the Microsoft 365 apps).

18% Increase in third-party backup use for Office 365 in 2020 to 2021 from 27% to 45%
http://vee.am/DPR21report

50% of lost data can be attributed to human error as the number one reason according to Netwrix Research
https://hostingtribunal.com/blog/data-loss-statistics/#gref

35% of data loss can be attributed to hardware failure according to Netwrix Research
https://hostingtribunal.com/blog/data-loss-statistics/#gref

#2 Adopt a *Backup Solution* that Truly Understands Teams

Unlike applications such as Exchange Online or SharePoint Online, Teams does not store all of its data in one place. Instead, Microsoft Teams data is scattered across a variety of different Microsoft 365 applications. While any Microsoft 365 backup application should be able to backup Teams data, the restoration process could be extremely difficult unless the application has been specifically designed to support Microsoft Teams.

According to Tech Radar, Microsoft revealed in July 2021 that it had 250 million active monthly users on Teams. This is an increase of over 100 million from the 145 million reported in April of the same year.
https://www.techradar.com/news/microsoft-teams-now-has-250-million-monthly-active-users

"Over 500,000 organizations use Microsoft Teams as their default messaging platform"
https://www.businessofapps.com/data/microsoft-teams-statistics

#3 Use the *Right Tool* for the Job

A third best practice for Microsoft Teams backups is to make sure that you are using the right tool for the job. There are features within the Microsoft 365 ecosystem, such as retention policies and litigation hold, that can act as a pseudo-backup. However, these tools exist for compliance purposes, not data protection. As such, they do not adequately protect Microsoft Teams data.

60% According to Avast, "60% of backups are incomplete". This is largely due to companies using outdated backup technologies
https://invenioit.com/continuity/disaster-recovery-statistics

37% 37% of SMBs have lost data in the cloud
https://invenioit.com/continuity/disaster-recoverystatistics

#4 Take a *Hybrid Approach* to Backups

Best practice number four is to take a hybrid approach to your backups. Rather than backing up Microsoft 365 separately from your on-premises Microsoft Office applications, it's better to use a single backup application that can simultaneously protect both environments.

Backup is shifting from on-prem to cloud-based solutions that are managed by a service provider, with a trajectory reported from 29% in 2020 to 46% anticipated by 2023.

Over the next two years, most businesses expect to gradually reduce their physical servers, maintain, and fortify their virtualized infrastructure, and embrace 'cloud-first' strategies. This means half of production workloads will be cloud-hosted by 2023.

https://solutionsreview.com/backup-disasterrecovery/veeam-data-protection-report-2021-shows-58-of-backups-are-failing

#5 Keep SLAs at the *Forefront of Your Backup Plan*

Best practice number five is to keep Service Level Agreements (SLAs) at the forefront of your backup planning. Specifically, you need to consider the appropriate Recovery Point Objective (RPO) and Recovery Time Objective (RTO) for your Microsoft Teams environment. The RPO will determine the frequency with which backups are created, thereby determining the maximum amount of data that could potentially be lost between backups. The RTO pertains to the length of time that it will take to restore a backup.

80% 80% of organizations recognize that they have an "Availability Gap" between how fast they can recover applications versus how fast they need applications to be recovered.

76% 76% of those same organizations have a gap between how frequently data is backed up versus how much data they can afford to lose.

#6 Don't Overlook *Recovery Granularity*

One of the often-overlooked best practices for Microsoft Teams Backup is to make sure that the backup solution that you are using allows for granular recovery capabilities. While it is important to be able to restore an entire team (or even multiple teams), it is equally important to be able to restore a file or a chat within a team.

44% of SaaS admins and 47% of Backup admins list better restoration, including granularity as their primary reason for protecting data from Office 365.
https://www.youtube.com/watch?v=RIHm8-OLUJs

70% of Fortune 500 firms purchased Office 365 in 2020
https://hostingtribunal.com/blog/microsoft-statistics/#gref

#7 Use Backup to Augment Your *eDiscovery Capabilities*

Microsoft 365 has long included eDiscovery capabilities that allow an organization to locate specific data from within the Microsoft 365 ecosystem in response to a subpoena. Although the native eDiscovery capabilities have their place, it is often more effective to use backup software in the discovery process.

A Disruption in eDiscovery poll found that "at least 58 percent of the audience had used eDiscovery technology for matters not involving claims or disputes at least 'on several occasions'." Illustrating that eDiscovery is no longer limited solely to litigation.*

$12.9 Billion The eDiscovery market is forecast to grow to $12.9 billion by 2025**

**https://ediscoverytoday.com/2020/08/31/here-are-some-disruptivestats-in-discovery-ediscovery-trends*
***https://www.prnewswire.com/newsreleases/global-12-9-billion-ediscovery-market-forecast-to-2025---focus-on-proactive-governance-withdata-analytics-and-the-emergence-of-new-content-sources-301231643.html*

#8 Defend Teams *Against Ransomware*

Another best practice is to make sure that you are protecting your Microsoft Teams data against ransomware. Contrary to popular belief, data that is stored in Microsoft 365 can be encrypted by ransomware. The fact that so many people are still working remotely from personal devices greatly increases the risk of a ransomware infection. A good backup is the best defense against ransomware related data loss.

According to the Ponemon Institute, only 45% of businesses believe that they have an adequate cyber security budget*

According to IDC, 69% of organizations have faced successful malware attacks within 12 months, 39% of which involved ransomware**

**https://www.keeper.io/hubfs/PDF/Cybersecurity%20in%20the%20Remote%20Work%20Era%20-%20A%20Global%20Risk%20Report.pdf)*
***https://www.veeam.com/why-backup-office-365.html*

#9 Ensure Your *Storage* Offers *Flexibility*

When selecting a backup application for Microsoft Teams, it's important to ensure that the solution that gives you the freedom to choose your own storage, regardless of where that storage is located. That way, organizations can choose a storage tier that offers the performance and resiliency that the business needs, and at the best possible cost. Having storage flexibility also gives organizations the option of writing backups to immutable storage if they so choose, thereby protecting backups against ransomware attacks.

CNA Financial set a world record in 2021 when the company paid a $40 million ransom.*

A 2021 survey by Sophos found that "7% of respondents' organizations were hit by ransomware in the last year"

**https://www.businessinsider.com/cna-financial-hackers-40-million-ransom-cyberattack-2021-5).*
***https://www.sophos.com/en-us/medialibrary/pdfs/whitepaper/sophos-state-ofransomware-2021-wp.pdf?cmp=120469*

#10 Focus on *Ease of Use*

Some backup applications have a reputation for being overly complex to configure and use. The problem with this is that complexity increases the odds of human error. If an organization selects a backup application that is intuitive and easy to use, it can decrease the odds that backup or recovery failure will occur as a result of human error.

According to FEMA, 40-60% of small businesses will never reopen after a data loss event
https://hostingtribunal.com/blog/data-loss-statistics/#gref

58% According to a 2021 study, 58% of backups fail when restoration is attempted*

**https://www.continuitycentral.com/index.php/news/technology/6092-survey-finds-that-58-percent-ofdata-backups-fail-when-restoration-is-attempted*

ConversationalGeek