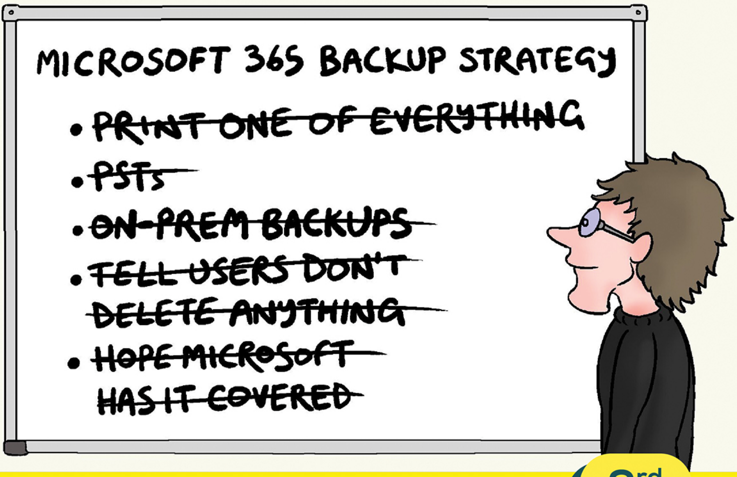
ConversationalGeek®

Conversational Microsoft 365 Backups

Nick Cavalancia (Microsoft MVP)


MICROSOFT 365 BACKUP STRATEGY
• ~~PRINT ONE OF EVERYTHING~~
• ~~PSTs~~
• ~~ON-PREM BACKUPS~~
• ~~TELL USERS DON'T DELETE ANYTHING~~
• ~~HOPE MICROSOFT HAS IT COVERED~~

3rd MINI Edition

Learn about:

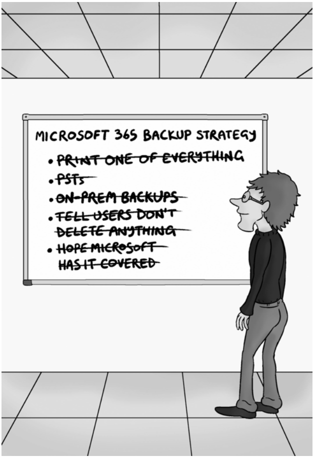
- Why Microsoft 365 needs to be backed up and how Microsoft isn't responsible
- What needs to be backed up and why BaaS is the best option for cloud-native workloads

Sponsored by

COHESITY

Conversational Microsoft 365 Backups (Mini Edition)

by Nick Cavalancia


MICROSOFT 365 BACKUP STRATEGY
~~PRINT ONE OF EVERYTHING~~
~~PSTs~~
~~ON-PREM BACKUPS~~
~~TELL USERS DON'T DELETE ANYTHING~~
~~HOPE MICROSOFT HAS IT COVERED~~

ConversationalGeek®

Conversational Microsoft 365 Backups (Mini Edition)

Published by Conversational Geek® Inc.

www.ConversationalGeek.com

Trademarks

Conversational Geek, the Conversational Geek logo and J. the Geek are trademarks of Conversational Geek®. All terms mentioned in this book that are known to be trademarks or service marks have been appropriately capitalized. We cannot attest to the accuracy of this information. Use of a term in this book should not be regarded as affecting the validity of any trademark or service mark.

Warning and Disclaimer

Every effort has been made to make this book as complete and as accurate as possible, but no warranty or fitness is implied. The information provided is on an “as is” basis. The author and the publisher shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising from the information contained in this book or programs accompanying it.

Additional Information

For general information on our other products and services, or how to create a custom Conversational Geek book for your business or organization, please visit our website at www.ConversationalGeek.com.

Publisher Acknowledgments

All of the folks responsible for the creation of this book:

Author:	Nick Cavalancia
Project and Copy Editor:	Pete Roythorne
Content Reviewer(s):	Raj Dutt Doug Ko

The “Conversational” Method

We have two objectives when we create a “Conversational” book. First, to make sure it’s written in a conversational tone so that it’s fun and easy to read. Second, to make sure you, the reader, can immediately take what you read and include it into your own conversations (personal or business-focused) with confidence.

“Geek in the Mirror” Boxes

We infuse humor and insight into our books through both cartoons and light banter from the author. When you see one of these boxes it’s the author stepping outside the dialog to speak directly to you. It might be an anecdote; it might be a personal experience.

Within these boxes I can share just about anything on the subject at hand Read ’em!

You Need To Back Up Microsoft 365

"Do you have a copy of that email I deleted?"

It's pretty safe to guess your organization is already using Microsoft 365. With over 300 million active users[1], it means that a majority of businesses are using Microsoft 365 in one form or another. The shift from traditional on-prem enterprise applications such as Exchange, SharePoint, and even

[1] Microsoft, *Q3 FY21 Earnings Call*

file services has taken the burdens of implementing, managing, maintaining, securing, and upgrading off the shoulders of IT and placed them very firmly on Microsoft through the use of Exchange Online, SharePoint Online, OneDrive for Business, and Teams. In addition, supporting services like Microsoft 365 Groups enables cross-application access for those wishing to collaborate.

But, as with each data set critical to business operations, there's always the pressing issue of whether the data is protected or not. And, even in the case of Microsoft 365, there is a question you should have a very good answer to…

Why Back Up Microsoft 365?

It's amazing how so many IT folks I meet look at me funny when posed with the question "*Do you back up your Microsoft 365 environment?*" I think part of the reason is the assumed deferral of backup responsibility to a cloud provider most experience when using any service in the cloud. And the other part likely revolves around "*gee… I never thought about it.*"

There are a number of reasons you need to backup the data within Microsoft 365 that your organization relies upon:

1) **It's *Your* Data** – The emails, documents, conversations, lists, etc. you put into Microsoft 365 are still owned by your organization. If we were talking about, say, an on-prem Exchange server, you'd certainly be accepting responsibility for backups. All that's changed is: *someone else manages the hardware and applications*. Therefore, you're still responsible. Microsoft's own SLA even states: *"We don't claim ownership of Your Content. Your Content remains Your Content and **you are responsible for it."**[2]*

2) **Data Gets Deleted** – Sure, applications like Exchange Online, SharePoint Online, and OneDrive have deleted-item retention, but that only works if the user realizes the need for the deleted item(s) within the allowed time period.

[2] https://www.microsoft.com/en-us/servicesagreement

3) **Microsoft 365 Credential Attacks** – New malware, such as *FTCode*, includes PowerShell scripts that go after mainstream browsers and even Windows Outlook to decrypt stored passwords. This puts any and all data in Microsoft 365 (as well as any other cloud service) at risk of deletion, manipulation, encryption, etc.

4) **Microsoft 365 Access Attacks** – I first saw this done by infamous hacker Kevin Mitnick two years ago demonstrating what he called "Ransomcloud;" a phishing scam resulting in each message within an Exchange Online Inbox being encrypted and held for ransom (you can see this in action at **bit.ly/RansomDemo**). I've seen recent attacks in the wild use OAuth (the open standard for access delegation to cloud resources) as part of the attack to establish a level of access and persistence to Microsoft 365 applications and data resources that extends well beyond just Exchange Online and well past a password change.

OAuth attacks provide access to Exchange, SharePoint, and OneDrive separate from the access granted to the user. So even if the user resets their password, the malicious access remains in place until it’s specifically revoked.

5) Incident Response – As part of a post-attack effort to return the environment to a known good state (just like you would if this was all on-prem), you may need to recover a few things; anything from a single file to a SharePoint list, to an entire mailbox, and beyond.

A ransomware attack on the government offices in a borough in Alaska wiped out their Exchange data entirely, causing them to set up a greenfield installation due to a lack of backups. It also impacted 500 endpoints and 120 servers. To stay operational, they literally resorted to using typewriters!

6) Microsoft Believes in Shared Responsibility – There are a number of docs on the web that

spell out where Microsoft believes the division of responsibility should be. In short, they handle infrastructure, data replication, infrastructure-level security, and compliance (in a data processor role). Your organization is responsible for *your* data, backups, data retention, data-level security, and compliance (as the data owner).

7) **You Should Plan for the Future** – It's always possible that your organization's strategy may shift, the company may be acquired, etc., causing the need to egress from Microsoft 365 to either on-prem solutions or another cloud-based office solution. In most cases, there are migration tools but, to be safe, you should have a copy of your data just the same.

It's apparent that backing up Microsoft 365 is necessary, so, let's dig a bit deeper and look at what you should be backing up.

What Needs to Be Backed Up?

I think the focus of backup needs to be primarily on four parts of Microsoft 365 around which most businesses revolve their operations:

Teams

With the shift to working remotely, the use of Teams has reached new heights with over 145 million daily active users[1]. Everything from channels, chats, channel messages, files, voice mails, integrations, owners, permissions, and more all need to be protected.

Microsoft has a default retention time that ranges from 1-7 days for messages, with other data types (e.g., meeting invites and files) falling subject to the service-specific retention times delivering them (e.g., Exchange and OneDrive for Business, respectively).

Exchange Online

Messaging still represents the bulk of most organizations' communications. Exchange Online supports a default deleted item retention time of 14 days that can be upped to 30. And, let's be real –

archiving and legal holds are for security compliance and are *not* backups.

Having proper backups that provide a granular recovery of your Exchange mailboxes will allow the organization to easily continue business at the point of recovery.

OneDrive for Business

The ease of use of cloud storage, and its ability to simplify content sharing, has made OneDrive a no-brainer for disparate workforces using a variety of client devices; the documents stored here represent the entirety of work for some roles within the organization. This data should be included in your backup strategy.

Because OneDrive uses SharePoint as its underlying technology, some capabilities around recovery are available to OneDrive. This includes recovery from the user's recycle bin within the default of 30 days as well as the recovery of the entire OneDrive from the Site Collection Recycle Bin within 93 days.

Microsoft does backup a given user's OneDrive instance for 30 days and supports you using their

Files Restore functionality to recover the entire instance from, say, a ransomware attack. And OneDrive uses the same two-tier recycle bin as SharePoint Online.

Even so, all this is done on a per-user basis, so it offers no value in a situation where you wish to recover multiple users at once.

SharePoint Online

I’ve seen entire organizations leverage SharePoint as the way to, in essence, run their business; calendars, task lists, documents, discussions, and more all make up a productive operation. So, at a minimum, backing up site collections and their contents are a necessity. As with OneDrive, SharePoint Online allows for recovery from the user’s recycle bin within 30 days and the Site Collection Recycle Bin within 93 days. Microsoft also keeps a backup of deleted items for an additional 14 days. Deleted site collections (and their contents) also can be recovered within 90 days by admins.

But, like Exchange Online, recovery of deleted items isn’t a backup. What’s needed is an ability to granularly recover anything from a single entry in a list up to an entire Site Collection – you expected this when SharePoint was on-prem and nothing has changed except the server's location.

Azure Active Directory (AAD)

I'm guessing you weren't thinking about AAD. When most people think of backing up Microsoft 365, they focus on "the data within." But, given the basis for every Microsoft 365 service is AAD, it makes sense to have an ability to recover it in circumstances where mailboxes and accounts need to be in-sync.

For those of you thinking "I sync my AAD with my on-prem AD, which is backed up already," you still need to have backups of AAD. There are plenty of unique bits of data stored in AAD that are *not* synchronized back to on-prem; Azure-specific attributes and license data, for example.

Microsoft Groups

Groups were created to empower teams of users to provide access to data across Teams, SharePoint, OneDrive, Exchange, and more. These need to be included in your backup strategy, as any permissions granted to facilitate access to a team of users would be lost.

What about Microsoft?

Now that you realize the importance of backing up quite a bit of Microsoft 365, it’s likely that many of you are thinking about Microsoft’s role in all this. You should be mindful of all that they have put in place in order to identify the gap that exists between what kind of backup and recovery capability you have today, and what you need as an organization. So, let’s look at what Microsoft offers, both at a platform level, and within their applications.

Microsoft’s Service Level Agreement

The Service Level Agreement (SLA) Microsoft provides for all of Microsoft 365 is focused on availability of the infrastructure and services; *it has nothing to do with your data*. While the architecture of Microsoft 365 does address data redundancy and some resiliency, there is no protection against data loss, accidental or malicious deletion, deletion beyond retention timeframes, corruption, encryption (ransomware), etc.

Plenty of Deleted Item Recovery Features

While I’ve covered some of the abilities to, in essence, *un-delete* items within these most critical parts of Microsoft 365, you need to recognize that it’s most definitely *not* the same level of data protection as maintaining a regular backup from which you can granularly recover.

It should be clear by now that a) Microsoft isn’t in the business of protecting your Microsoft 365 data, and b) your organization needs to be the one to do something about it.

So, what kind of backup solution should you be looking for?

Properly Backing Up Microsoft 365

The idea of truly backing up Microsoft 365 clearly aligns with your business continuity / disaster recovery (BC/DR) initiatives. So, the decision of how to properly back up Microsoft 365 should revolve around a few considerations:

- **Meeting the 3-2-1 Backup Rule** – Even data that originates in the cloud needs to follow this fundamental principle: *three copies (one of which is the production copy in Microsoft 365), on two media, with one offsite instance (meaning, in this case, not within Microsoft 365 itself)*. The "offsite" ideally should be another cloud storage provider.

- **Using Backup as a Service** – The choice to move to Microsoft 365 indicates a corporate desire to shift from capex to opex spending with SaaS solutions. I think it's warranted to ask the question "*Why would you even backup on-prem?"* Using Backup as a Service fits with your choice to leverage Microsoft 365, providing speed, flexibility, and scalability while enjoying that same opex spending model.

  Similarly, you also chose Microsoft 365 to offload the responsibility for any and all components involved in delivering the service. It may make sense to look to a BaaS provider (often offered by the backup solution provider themselves) to offload the ongoing work of creating, managing, and maintaining backups of Microsoft 365.

I’d recommend sticking with BaaS offerings that are cloud-based, but have an ability to address the needs of those of you with a hybrid environment that require a degree of flexibility when it comes to on-prem backup and recovery needs.

- Keeping an On-Prem Option – Should you have a hybrid environment with some on-prem instances of one or more services working in conjunction with Microsoft 365, the answer may still be BaaS in combination with on-premises protection for other data sources. This can also potentially help with exit planning, should you want to return to on-prem or switch digital workspace providers.

- **Long-Term Retention** – Backups of Microsoft 365 may need to be preserved for an extended period to ensure recoverability back to specific points in time. Your backup solution should include an ability to keep backups for months, or years, as is needed.
- **Archiving** – Microsoft does provide a means to maintain archives (as in the case of Exchange Online), as well as an ability to search through many parts of Microsoft 365 via Content Search, more organizations look for archiving to encompass both legacy email solutions and email from cloud-based vendors. I recommend you should think of backups as *contributing to an archive* and not *being the archive* itself.
- **Adjusting with the Organization** – This is a bit tactical, but I think it’s important. Whichever way you back up Microsoft 365, remember that there will be new mailboxes, new OneDrive folders, and new SharePoint

sites. To ensure you capture every bit of data that should be protected, look for a solution or service that automatically updates as your Microsoft 365 environment changes.

- Disaster Recovery – Most Microsoft 365 backup discussions (even those in this book) revolve around the recovery of just a few messages or, perhaps, just one mailbox. But, in situations where you need to put the entire environment back into that known-good state, you should be thinking about your Microsoft 365 backup as a part of your DR strategy. Having the ability to include Microsoft 365 as part of your DR efforts ensures post-recovery operational consistency.

For each of these considerations, look at them through the lens of “business requirements;” *what does the business need*? Always start there and work back to the technology, the capabilities, and cool features of a potential solution.

The Big Takeaways

Your organization’s investment in Microsoft 365’s leading solutions – Teams, Exchange Online, SharePoint Online, OneDrive, and Microsoft Groups for Business – is only going to continue to grow over the coming years. Improved functionality, new services, and simple pricing is likely going to keep you a customer for a while.

It’s important to consider the data you keep in Microsoft 365 as *your* data that *you* must back up. Just as with on-prem services, this data is still subject to the same user error, cyberattacks, data breaches, and shifts in organizational strategy – all requiring IT to protect it. So, every part of Microsoft 365 that you leverage should be included in your backups to ensure you can recover not just the data, but your operations as well.

Look for a solution that specifically addresses business needs around backup and recovery and not just a service that simply backs up Microsoft 365. The stuff you keep in there is important; *treat it as such*.

COHESITY

Microsoft 365 Data is Your Responsibility

cohesity.com/microsoft365

This material (a) is intended to provide you information about Cohesity and our business and products; (b) was believed to be true and accurate at the time it was written, but is subject to change without notice; and (c) is provided on an "AS IS" basis. Cohesity disclaims all express or implied conditions, representations, warranties of any kind.

Your Microsoft 365 instance is the lifeblood of your organization. And yet, you have no backup strategy or execution in place. Why? In this book, I'll cover the why, what, and how around backing up Microsoft 365 to protect the organization and its ability to remain operational, productive, and risk-free.

About Nick Cavalancia

Nick Cavalancia is a Microsoft MVP, a Technical Evangelist by trade, and is a 25+ year IT veteran who regularly speaks and writes for some of today's most recognizable companies.

ConversationalGeek®