ConversationalGeek®

Conversational Microsoft 365 Backups

Nick Cavalancia (Microsoft MVP & Co-founder of Conversational Geek)

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

2nd MINI Edition

Learn about:

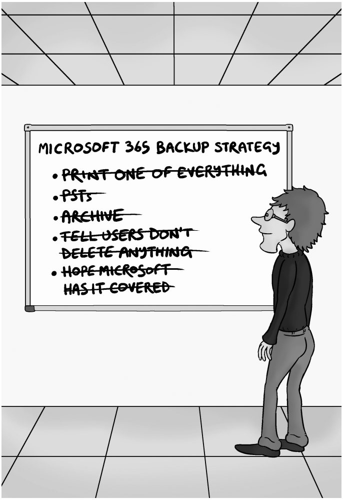
- Why Microsoft 365 needs to be backed up and why Microsoft isn't responsible
- What needs to be backed up and how to identify the right solution

Sponsored by

COHESITY

Conversational Microsoft 365 Backups (Mini Edition)

by Nick Cavalancia


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

ConversationalGeek®

Conversational Microsoft 365 Backups
(Second 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):	Theresa Miller
	Douglas 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 200 million active commercial users[1], it means that a majority of businesses are using Microsoft 365 in one form or another. The shift from traditional on-premises enterprise applications such as Exchange,

[1] Microsoft, *Q1 FY20 Earnings Call*

SharePoint and even 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 and OneDrive for Business.

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.

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.

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-premises 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:

Exchange Online

This is the one service most people think of, as it’s the most widely used; messaging 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.

Other Parts of Microsoft 365

I’m going to group all the other services provided in Microsoft 365 here as a sort of secondary focus. Services like Yammer and Teams have not yet reached a critical mass, like the previous four have (for example, as of the beginning of 2020, Teams has 10K users[1]). Additionally, development for the backup of these services has not reached uniform granularity, so there is neither the same opportunity nor need to back them up in the same manner as, say, Exchange Online.

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, 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 is clearly more in line with business continuity / disaster recovery (BC/DR) initiatives. So, the decision of how to properly back up Microsoft 365 should revolve around a few considerations:

- Business Requirements – Like any backup strategy, you first need to determine the recovery constraints for Exchange Online, SharePoint Online, OneDrive and Azure AD. Identifying the recovery time and point objectives for each will help you determine whether a particular backup method is viable.

- **Meeting the 3-2-1 Backup Rule** – Even data that originates in the cloud needs to follow this fundamental principle of backups: *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” can be another cloud storage provider, or on-prem storage.

- **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** – Archives exist for long-term eDiscovery of specific data within various parts of Microsoft 365. While 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 within the Microsoft 365 compliance center, more organizations look for archiving to encompass both legacy email solutions and email from cloud-based vendors. Thinking about archiving well beyond the foreseeable future will put you in the proper mindset; 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.

- **Cloud vs. On-Prem** – One way or another, you're going to need to utilize a solution or service that assists with backups. So, the question of whether it matters that it exists in the cloud or on-prem should be addressed. While some would point out that there's a reason you went to the cloud (so using a cloud-based solution makes sense), your backup solution should *include* Microsoft 365 as one of *many* data sources to protect, which may mean you will use an on-prem solution to back up both local and cloud-based data sets.

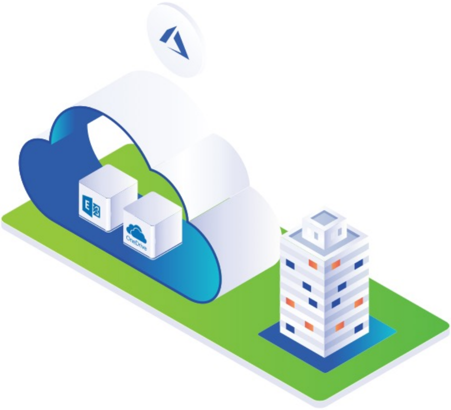
For each of these considerations, look at them through the lens of “business requirements;” *what does the business need*? Always start there and work back to the technology, the capabilities, and cool features of a potential solution.

The Big Takeaways

Your organization’s investment in Microsoft 365’s leading solutions – Exchange Online, SharePoint Online and OneDrive for Business – is only going 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-premises 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*.



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.