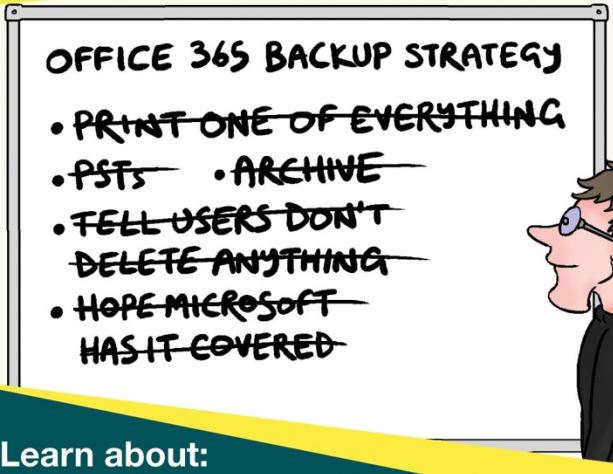
Conversational
Office 365 Backups

A ConversationalGeek® Book

Sponsored by COHESITY



Learn about:

- Why Office 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

MINI Edition

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

Sponsored by Cohesity

Cohesity empowers organizations to protect, store, and easily manage their data in a single logical environment that spans seamlessly between data centers and clouds - eliminating legacy infrastructure silos and mass data fragmentation while providing a single point of global control. Cohesity also enables enterprises to draw new business insights from their most important digital asset that can fuel competitive differentiation and better customer experiences.

COHESITY

For more information, visit

www.cohesity.com

Conversational Office 365 Backups (Mini Edition)

by Nick Cavalancia

ConversationalGeek®

Conversational Office 365 Backups (Mini Edition)

Published by Conversational Geek® Inc.

www.ConversationalGeek.com

Trademarks

Warning and Disclaimer

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 Editor:	Michele Touchet
Copy Editor:	Steven Zimmerman
Content Reviewer(s):	J. Peter Bruzzese

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 Backup Office 365

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

It's pretty safe to guess your organization is already using Office 365. Microsoft's 56% market share in 2018 – the result of a 64% increase in Office 365 adoption between 2016 and 2018[1] – means that over half of all businesses are using Office 365 in one form or another. That shift from traditional on-

[1] Bitglass, *Cloud Adoption Report* (2018)

premises enterprise applications (e.g., Exchange, SharePoint) has taken the burdens of implementing, managing, maintaining, securing, and upgrading off the shoulders of IT and placed them very firmly on Microsoft.

But, as with every 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 Office 365, there is a question you should have a very good answer to…

Why Back Up Office 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 Office 365 environment?*" I think part of the reason is the deferral of responsibility 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 the data your organization relies on within Office 365 needs to be backed up:

1) It's *Your* Data – The emails, documents, conversations, lists, etc., you put into Office 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 and SharePoint within Office 365 have deleted-item retention, but that only works if the user realizes the need for the deleted item(s) within the allowed time period. Note: *for email, it's 14 days by default and up to 30 days if you make a remote PowerShell connection and up it*.

3) Office 365 for Ransom – Infamous hacker Kevin Mitnick demonstrated what he called "Ransomcloud"; a phishing scam resulting in each message within an Inbox being encrypted and held for ransom (you can see this in action at bit.ly/RansomDemo). Given Microsoft's desire to make many parts of

Office 365 accessible to mobile apps, I'd expect to see this threat tactic expand beyond Exchange Online and employed for practical (ahem… *malicious*) purposes.

When Kevin did this demo in front of a live audience of 300 people, he started by asking "how many of you back up Office 365's Exchange Online?" Only 3 people raised their hands in the audience. He said "perfect" and proceeded to show them why it was a mistake due to modern cloud-based ransomware encryption threats.

4) 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 message to entire mailboxes.

A ransomware attack on the Mat-Su 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!

5) 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).

6) 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 Office 365 to either Exchange on-prem or another email solution (whether in the cloud or on-prem). 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 Office 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 Office 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. Having backups that provide a granular recovery of your Exchange mailboxes will allow the organization to easily continue business at the point of recovery.

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. I can also see extending this up to web applications, and even to farms, to ensure availability. But, for most organizations, having granular recovery of data stored within site collections will suffice.

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.

Azure Active Directory (AAD)

I'm guessing you weren't thinking about AAD. When most people think of backing up Office 365, they focus on "the data within." But, given the basis for every Office 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 Office 365

I'm going to group all the other services provided in Office 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 (although Teams is getting there). Additionally, development for these services' backup 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 Office 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 Office 365 is focused on availability of the infrastructure and services; *it has nothing to do with your data*. While the architecture of Office 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.

Capabilities inside Office 365

SharePoint and OneDrive offer some form of deleted-item retention in the form of the Recycle Bin. Services like Exchange additionally host a second-stage recovery method in the form of the Recoverable Items folder. In all cases, the weakest link is the policy-based retention period, which defaults to 30 days in most cases. And, even when configured for a longer period, it still may not be enough to truly *recover*.

There is also Legal Holds (a.k.a. In-Place Holds, now part of Retention Policies in the Security and Compliance Center [SCC]) to retain specific Exchange and SharePoint data for longer periods of time, as well as to archive email, which uses very simple and broadly applied policies to control it. Both features cause data to be retained for longer periods of time, but neither should be considered a backup for the purpose of recovery.

While there are some abilities to, in essence, *un-delete* items within Office 365, recognize that it's not the same level of data protection as maintaining a backup.

Microsoft offers exporting to .PST as a backup solution for Exchange Online customers. While viable for, perhaps, SOHO (Small Office / Home Office) and small business customers, this isn't practical, scalable, secure, or compliant.

It should be clear by now that a) Microsoft isn't in the business of protecting your Office 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 Office 365

Backing up Office 365 is clearly much more on the business continuity / disaster recovery (BCDR) end of the spectrum than on the "*let's export to a .PST*" side of things. The decision of how to properly back up Office 365 revolves around a few considerations:

- Business Requirements – Like any backup strategy, you first need to determine the recovery constraints for each data set within Office 365. 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 Office 365), on two media, with one offsite instance (meaning, in this case, not*

within Office 365 itself). The "offsite" can be another cloud storage provider, or on-prem storage.

- Long-Term Retention – Backups of Office 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 months, or years, as is needed.

- Archiving – Archives exist for long-term eDiscovery. While Microsoft does provide a means to search through many parts of Office 365, 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 Office 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 Office environment changes.

- Disaster Recovery – Most Office 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 Office 365 backup as a part of your DR strategy. Having the ability to include Office 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 the solution 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* Office 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

Microsoft has taken great strides to architect a cloud-based service from the ground up that gives you anytime, anywhere, any-device access to your business in the cloud.

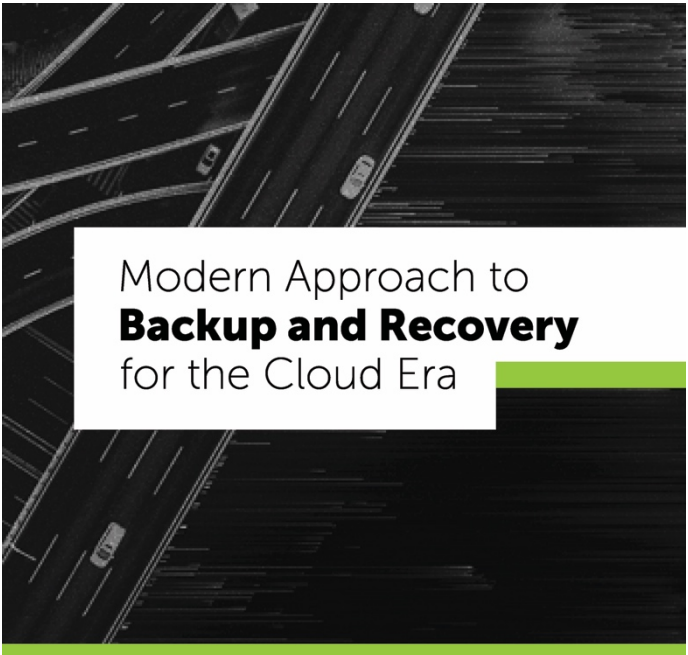
Your organization's investment in Office 365 is only going to grow over the coming years; improved functionality, new services, and simple pricing is likely going to keep you a customer for a while.

It's important to consider the data you keep in Office 365 as *your* data that *you* must back up. Every part of Office 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 Office 365. The stuff you keep in there is important; *treat it as such*.

NOTES

NOTES



Modern Approach to **Backup and Recovery** for the Cloud Era

COHESITY

WWW.COHESITY.COM

Your Office 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 Office 365 to protect the organization and its ability to remain operational, productive, and risk-free.

About Nick Cavalancia

Nick Cavalancia is 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®

Visit conversationalgeek.com for more books on topics geeks love.