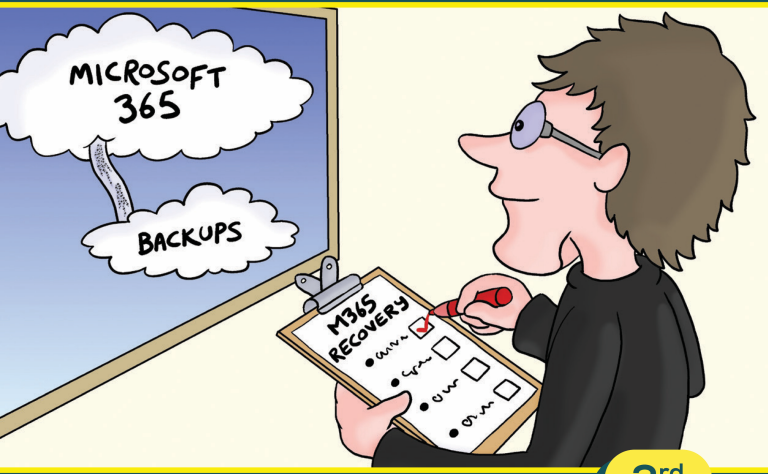
ConversationalGeek

Conversational Microsoft 365 Recovery Best Practices

Brien Posey (Microsoft MVP, Commercial Scientist Astronaut Candidate)



Learn about:

- What's available within Microsoft 365, and when it's not the right option.
- Key recovery considerations when choosing how and who will recover your Microsoft 365 data

3rd MINI Edition

Sponsored by

veeam

Sponsored by Veeam

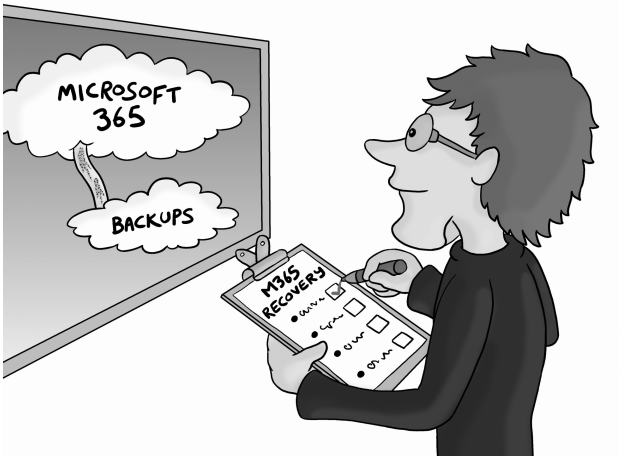
Veeam, the #1 global market leader in data protection and ransomware recovery, is on a mission to help every organization not just bounce back from a data outage or loss but bounce forward. With Veeam, organizations achieve radical resilience through data security, data recovery, and data freedom for their hybrid cloud. The Veeam Data Platform delivers a single solution for cloud, virtual, physical, SaaS, and Kubernetes environments that gives IT and security leaders peace of mind that their apps and data are protected and always available. Headquartered in Columbus, Ohio, with offices in more than 30 countries, Veeam protects over 450,000 customers worldwide, who trust Veeam to keep their businesses running.

To learn more visit
www.veeam.com
or follow Veeam on
LinkedIn @veeam-software and
Twitter @veeam

Conversational Microsoft 365 Recovery Best Practices (3rd Mini Edition)

by Brien Posey

© 2024 Conversational Geek



ConversationalGeek®

Conversational Microsoft 365 Recovery Best Practices (3rd Mini Edition)

Published by Conversational Geek® Inc.

www.ConversationalGeek.com

All rights reserved. No part of this book shall be reproduced, stored in a retrieval system, or transmitted by any means, electronic, mechanical, photocopying, recording, or otherwise, without written permission from the publisher. No patent liability is assumed with respect to the use of the information contained herein. Although every precaution has been taken in the preparation of this book, the publisher and author assume no responsibility for errors or omissions. Nor is any liability assumed for damages resulting from the use of the information contained herein.

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:	Brien Posey
Project and Copy Editor:	Nick Cavalancia
Content Reviewer(s):	Edward Watson
	Donna Suen

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!

Recoverability isn't always a given with Microsoft 365

"Are you sure this is going to work?"

The fact that organizations need to backup their Microsoft 365 deployments has been well established. Over the past several years myself and others have published countless books, articles, and blog posts explaining that Microsoft 365 is based on

a shared responsibility model in which Microsoft is responsible for protecting the underlying infrastructure, and subscribers are responsible for protecting their own data. This means that if you use Microsoft 365, you have to backup your own data. Microsoft isn't going to do it for you. In fact, Microsoft is even creating its own backup tool for Microsoft 365, presumably as a way of reminding customers that they need to be backing up their data.

In their Services Agreement, Microsoft makes it very clear on the delineation around customer data (referred to below as "Your Content"):

"We don't claim ownership of Your Content. Your Content remains Your Content and **you are responsible for it.**"

As important as backups might be, however, there is one critical item that always seems to get left out of the conversation. That item is recoverability. After all, backups are meaningless unless you can restore them. I've lost count of the times over the years when I have seen an organization attempt to restore a backup, only to discover that the backup was corrupt or that it didn't contain everything that they thought it did. In those situations, the organizations in question might as well have not even had a backup at all. To put it bluntly, having a backup might give you a warm fuzzy feeling, but ultimately the only thing that really matters is whether or not you can restore that backup when the time comes.

I wanted to write this book because the ability to restore a backup is often treated as a foregone conclusion. In reality, recoverability isn't always quite as straightforward as we might like it to be. This can be especially true when you bring Microsoft 365 into the picture. As such, I'm going to talk about some of the things that you need to think about with regard to Microsoft 365 recovery.

Treat the Native Recovery Tools as a Convenience Feature

As you probably know, Microsoft provides several different built-in recovery tools for Office 365. For example, Microsoft provides a recycle bin for OneDrive for Business, SharePoint Online, and Entra ID (formerly Azure AD). These and other recovery tools can sometimes be used to get data back after it has been accidentally deleted.

As a best practice, I would strongly recommend using the various protective mechanisms that are built into Microsoft 365 as a convenience feature rather than a backup substitute. There are any number of reasons for this, but the important thing to know is that there are numerous situations in which the native protective features do not provide the necessary level of protection. Additionally, the levels of protection that these tools provide (and the length of time for which data is recoverable) tend to be inconsistent across the Microsoft 365 ecosystem.

The point is that while the native recovery tools that are baked into Microsoft 365 definitely have their place, you can't depend on them to work in every situation. Therefore, I strongly recommend treating them solely as a convenience feature as opposed to a go-to mechanism for data recovery.

When I took my first Windows certification class, the instructor said that Windows Backup (the backup tool that is built into Windows) will work in a pinch, you shouldn't bet your job on being able to use it to recover data. That's exactly how I think of the native data recovery tools that are built into Microsoft 365. They might work, but if they don't you really don't want to have to explain to your boss that you never put a proper backup solution into place.

Backup Immutability

A backup must do more than just to give organizations a way of recovering data that has been accidentally deleted or overwritten. Backups must also be able to protect against ransomware attacks. This is no small task but a big problem, as 76% of organizations indicated that they had experienced at least one ransomware attack in 2023[1].

Unfortunately, ransomware authors know that nobody is going to pay a ransom if they can just restore a backup instead. As such, an increasing number of ransomware variants are being designed to attack an organization's backups with the goal of rendering those backups useless.

This is where backup or backup copy immutability comes into play. Immutability makes it so that a backup cannot be overwritten, deleted, or encrypted by ransomware. Having immutable

---

[1] Veeam, *Data Protection Trends Report* (2024)

backup storage greatly increases the chances of being able to successfully recover from a ransomware attack.

The Difficulty of Recovery

When it comes to using a third-party product to restore Microsoft 365 data, one of the first things that you need to consider is what the recovery process will be like. Can you simply point and click your way through the recovery operation, or will you have to delve into PowerShell?

Even though I live and breathe PowerShell, I personally would not want to use a backup product that required me to use PowerShell in order to restore Microsoft 365 data (although having PowerShell support is always good). The reason for this is that simplicity decreases the amount of time required to initiate a recovery operation, and also decreases the chances of human error.

Backup products can differ widely in terms of their complexity. Some of this complexity (or lack thereof) can obviously be attributed to user interface design. However, there is a little bit more to it than that.

Microsoft has created a collection of APIs that backup vendors can use for Microsoft 365 backup and recovery. These APIs allow developers to backup and restore Microsoft 365 data based on Microsoft's own best practices. At this point in time, most backup vendors do use the Microsoft 365 APIs. However, there are vendors who only use a subset of the APIs, and there may still be a few whose products are not based on the APIs.

While it's tempting to think of API use as being one of those things that only matters to developers, whether or not a backup vendor chose to use an API plays directly into what will be involved in a Microsoft 365 recovery operation.

Imagine for a moment that a backup vendor uses all of the Microsoft 365 APIs, except the API for Teams. Such a product would probably allow you to restore Teams data, but because Teams data is scattered

across several other Microsoft 365 applications, it would likely be up to the person who is restoring the Teams data to figure out where the data actually resides, how to restore that data, and how to make Teams recognize the data that has been restored.

Microsoft Teams recovery is one area in which the native recovery mechanisms really fall short. You can restore a deleted team by going into PowerShell and recovering the group associated with that team, but the native tools do not allow you to recover individual items from within a team. Teams recovery using native tools is an all or nothing operation. You can't pick and choose what gets recovered.

Restoration Granularity

Another key consideration is the granularity with which a third-party backup application allows you to restore Microsoft 365 data. Consider Exchange Online for example. You obviously need to be able to perform a comprehensive restoration in the event that your entire Exchange Online environment was to be wiped out. However, these types of comprehensive restorations are relatively rare.

Most of the time when a restoration becomes necessary in an Exchange Online environment, admins are asked to restore an individual mailbox, or perhaps even a single message or calendar item.

This same basic concept applies to all of the various Microsoft 365 applications. In a Teams environment for example, you may need to recover message data, individual files, voicemail messages, recordings, or other types of data. It's important that whatever backup application you are using is able to perform both large-scale recovery operations and extremely granular recovery operations, down to individual items.

Versioning and Attributes

Another important consideration when it comes to recovering data within a Microsoft 365 deployment is the ability to preserve and use any existing attributes associated with the items that are being recovered.

Consider, for example, the fact that OneDrive for Business allows you to retain multiple versions of files. If you were to restore a file to OneDrive from backup, that restoration should not occur in a way that causes the file versions to be deleted. Ideally, you should be able to choose which version of the file you want to restore, but you shouldn't lose access to other versions of the file.

While I am on the subject of OneDrive for Business, it's also important to be able to restore files that have been changed or that are missing. If a ransomware infection were to encrypt a bunch of files stored on OneDrive, for example, it's important to be able to restore the encrypted files, but without overwriting untouched files in the process.

Of course, file versions are not the only type of attributes that exist. Each of the Microsoft 365 applications uses data attributes in its own way, and it's important for any backup application to be able to recognize and retain these attributes.

Imagine for a moment that you needed to restore a Microsoft Teams team. One of the most important attributes for any team would be the team members. You shouldn't have to manually

repopulate the team once it has been restored. Your backup application should recognize attributes associated with membership so that the team's membership is retained. The same thing goes for a team's settings and for any other attributes associated with a team, or with any other type of Microsoft 365 data.

Recovery Flexibility

Another important thing to consider with regard to Microsoft 365 data recovery is that a good backup tool should give you a significant amount of flexibility with regard to the data recovery process. Imagine for a moment that an administrator in your organization accidentally deletes a user's mailbox. Obviously, it's important for the backup application to be able to restore that mailbox, but there's a little bit more to it than that.

It's easy to assume that when you restore the mailbox you will be restoring it to its original location. However, there are no guarantees that this will always be the case. If for example, the mailbox existed on an on-premises Exchange Server and the on-premises environment is having

problems, then you may need to restore the user's mailbox to the Microsoft 365 cloud (even if only temporarily) just so that the user can get back to work while the on-premises infrastructure is being fixed.

Similarly, you might need to restore a particular piece of Microsoft 365 data to a location that is completely different. Imagine for a moment that a particular user sends a rather questionable email message and then deletes the message from their sent items folder. Depending on what the message was all about and your organization's policies, it might become necessary to restore the message to someone else's mailbox for review. Similarly, it might be better to simply export the message as a .MSG file so that it can be handled outside of anyone's mailbox.

Of course, there are any number of situations in which you might need to restore Microsoft 365 data to a different location or to export that data. For instance, if litigation were to be filed against your organization, then there is a good chance that there would be a discovery process in which specific emails were subject to subpoena. Rather than

setting up a mailbox for the opposing legal counsel, it would usually be more practical to simply export the requested data, and then save it to removable media or to cloud storage where it can be used by the opposing counsel.

This brings up another important point. In a situation like the one that I just described; it is obviously important to be able to export Microsoft 365 data in a way that allows that data to be used outside of your organization. However, it is equally important that your backup product includes a really good search engine that will be able to locate all of the data that needs to be restored or exported.

Think back to the situation that I just described in which certain data is subpoenaed and must be provided to opposing counsel. In a situation like that, you wouldn't want to just export everything. Even though that might be the easiest option, you never want to provide opposing legal counsel with data that they did not ask for because that extra, unrequested data could potentially be used against your organization. Similarly, if your backup application includes a subpar search engine, then it

may not be able to find all of the data that needs to be handed over, thus landing you in trouble for an entirely different reason. In other words, it is absolutely essential for a good backup product to feature a first-rate search engine.

Complete Visibility

One of the most critical, and yet most often overlooked backup capabilities is complete visibility into your backups. At a high level, this means that your backup application needs to have good monitoring and reporting capabilities. However, there is a bit more to it than that.

Because your backups are so crucial to your organization's wellbeing, you need to be absolutely sure that they are functioning as intended. This means more than just having the ability to check your backup logs to make sure that backup jobs are running. You need to be able to verify that the backup application is healthy and that it is running as intended. Similarly, it's important to be able to verify that specific files have indeed been backed up.

In other words, your backup application should never leave you wondering if your data was backed up. It should provide you with an easy way to verify that your data has indeed been backed up as intended.

More importantly, your backup application should be able to notify you if it detects a problem. After all, you never want to be in a situation in which you need to perform a restoration but discover that there was a problem with your backup that left your data completely unprotected.

Some admins like to set up notifications so that they receive an email message when a backup job has been successfully completed. That way, if the expected email does not arrive then they know that they need to check their backups to see if a problem has occurred.

Backup Options

In the previous section, I explained that it is extremely important to have a way of verifying that your backup infrastructure is working in the expected manner and that your data has indeed been backed up. Rather than dealing with potential backup problems however, some organizations prefer to leverage Backup as a Service, or BaaS.

Somewhat recently, at least some backup vendors have begun delivering backup capabilities as a service (i.e., BaaS) in addition to their traditional backup software. Because both platforms are provided by the same vendor, the two offerings usually deliver a similar feature parity and similar backup and restore processes, allowing for an easier, seamless user experience.

BaaS providers run their backup service on their own servers and are responsible for keeping the backup infrastructure healthy. That means that the backup provider will handle tasks such as patch management and capacity planning, whereas the customer needs only to verify that their data is being properly backed up.

The main advantage to using BaaS is that BaaS tends to be easy to use and super convenient. Even so, BaaS might not be a good fit for organizations that need super granular control over their backup infrastructure.

In some cases, an organization can have the best of both worlds by protecting some workloads with a traditional backup and using BaaS for others. An organization might for example, use BaaS to back up its Microsoft 365 data, but use an on-premises backup solution to protect its accounting data.

In the past, it was a bad idea to mix match backup solutions in this way. At best, mixing backup solutions created management silos and data silos. At worst, using two different types of backups could result in coverage gaps that left some data unprotected.

But when using the same backup vendor for both its' traditional backup software and its' backup service, you don't have to worry about data or management silos. You are free to use BaaS to simplify your backups, and you can still use your existing backup infrastructure to protect any

resources that don't align well with the BaaS environment.

Self-Service Recovery

One last thing to think about is whether or not your organization could benefit from a backup application with self-service recovery capabilities. Not every backup application offers self-service capabilities. The whole concept of self-service recovery is still somewhat new. Likewise, self-service recovery isn't a good fit for every organization. Having said that though, there can be substantial benefits to allowing self-service recovery.

Consider what normally happens when a user needs to have a file restored. The user calls the helpdesk, the helpdesk calls a backup operator, and the backup operator restores the file. The user has little choice but to wait for the file to be recovered. Likewise, the backup operator has to take time out from whatever it was that they were working on so that they can assist the user. Self-service recovery allows the user to get their data back immediately, while also freeing up backup operators so that they can focus on more important matters.

The Big Takeaways

Any backup application should be able to allow you to recover the data that you have backed up. That's a given. However, Microsoft 365 data recovery capabilities vary widely from one backup application to another. Some backup applications for example, require you to use PowerShell as a part of the recovery process. Similarly, a backup application might not give you the granularity required for small recovery jobs or might fail to preserve certain attributes.

Your organization's backup is its lifeline. As such, the backup needs to be as flexible as humanly possible with regard to the types of backups that you can perform and the ways in which it allows you to recover your data. The more flexible a backup solution is, the better the chance that you will be able to get your data back after a disaster.

Gold
Microsoft Partner

Radical Resilience for Microsoft 365

Keep your business running with the #1 Microsoft 365 Backup and Recovery Leader

Veeam's Microsoft 365 backup solutions eliminate the risk of losing access and control over your Microsoft 365 data, including Exchange Online, SharePoint Online, OneDrive for Business and Microsoft Teams, so your data is always protected and accessible.

Veeam provides 3 different deployment, management and delivery options, allowing the freedom to use your preferred Microsoft 365 backup strategy.

- **Backup Service:** Veeam Data Cloud *for Microsoft 365*, the infrastructure is managed by Veeam, unlimited storage is included
- **Backup Software:** Veeam Backup *for Microsoft 365*, self-managed backup software and infrastructure, with any storage
- **Managed Services:** Offloaded expertise and services to a Veeam Cloud and Service Provider partner

Get started here

Microsoft's shared responsibility model means that if you're using their infrastructure, then you are responsible for backing up your own data. But your backups are useless if you can't restore them – and recoverability isn't always straightforward. This book looks at the key considerations with regard to Microsoft 365 recovery.

About Brien Posey

Brien Posey is a 22-time Microsoft MVP, a published author and conference speaker with 20+ years of IT experience, and a Commercial Scientist Astronaut candidate.

ConversationalGeek®

For more content on topics geeks love visit

conversationalgeek.com