7 Critical Reasons for Microsoft 365 Backup

The case for why organizations need to protect Microsoft 365 data

Introduction

Do you have control of your Microsoft 365 data? Do you have access to all the items you need? The knee-jerk reaction is typically, "Of course I do," or "Microsoft takes care of it all."

But if you really think about it — are you sure?

Microsoft takes care of quite a bit, and provides a great service for their customers. However, Microsoft's primary focus is on managing the Microsoft 365 infrastructure and maintaining uptime to your users. They are empowering YOU with the responsibility of your data. The misconception that Microsoft fully backs up your data on your behalf is quite common, and without a shift in mindset, could have damaging repercussions when this responsibility is left unattended.

Ultimately, you need to ensure you have access to, and control over, your Exchange Online, SharePoint Online, OneDrive for Business and Microsoft Teams data.

This report explores the hazards of not having a Microsoft 365 backup in your arsenal, and why backup solutions for Microsoft 365 fill the gap of long-term retention and data protection.

> "We worried about the backup and retention policies in Microsoft 365. That's why we decided to ensure we have a backup of our data residing in Microsoft 365."
>
> **— Karen St.Clair,**
> IT Manager,
> Columbia Power & Water Systems

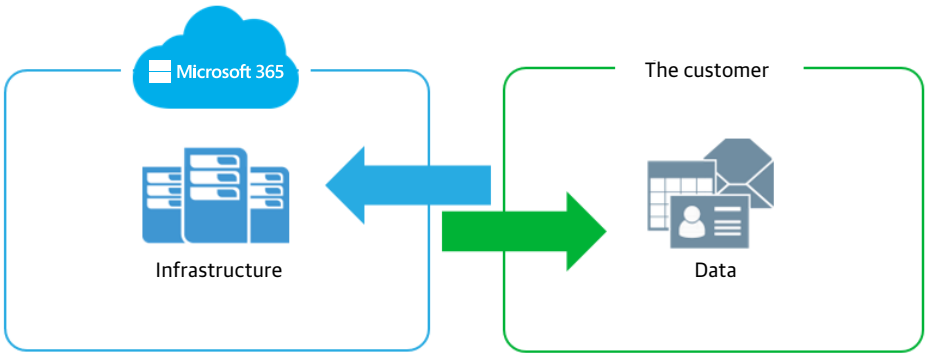
The big Microsoft 365 misconception

The misunderstanding falls between Microsoft's perceived responsibility and the user's actual responsibility of protection and long-term retention of their Microsoft 365 data. The backup and recoverability that Microsoft provides and what users assume they are getting are often different. Meaning, aside from the standard precautions Microsoft 365 has in place, you may need to re-assess the level of control you have of your data and how much access you truly have to it.

Microsoft 365 offers geo redundancy, which is often mistaken for backup. Backup takes place when a historical copy of data is made and then stored in another location. However, it is even more important that you have direct access to and control over that backup. So if data is lost, accidentally deleted or maliciously attacked, for example — you can quickly recover. Geo redundancy, on the other hand, protects against site or hardware failure, so if there is an infrastructure crash or outage, your users will remain productive and often oblivious to these underlying issues.

Source: https://docs.microsoft.com/en-us/azure/security/fundamentals/shared-responsibility

Microsoft takes care of infrastructure, but the data remains the customer's responsibility



Uptime of Microsoft 365

Protection and long-term retention of Microsoft 365 data

"For all cloud deployment types, you own your data and identities."

— Microsoft Documentation

7 reasons why backing up Microsoft 365 is critical

As a robust and highly capable Software as a Service (SaaS) platform, Microsoft 365 fits the needs of many organizations perfectly. Microsoft 365 provides application Availability and uptime to ensure your users never skip a beat, but a Microsoft 365 backup can protect you against many other security threats.

You or your boss might be thinking, "The recycle bin is probably good enough." This is where many people get it wrong. The average length of time from data compromise to discovery is over 140 days[1]. A shockingly large gap. The likelihood is high that you won't notice something is missing or gone until it's too late for the recycle bin.

By talking with hundreds of IT professionals across the globe who have migrated to Microsoft 365, seven vulnerabilities in data protection rise to the top:

Accidental deletion

Retention policy gaps and confusion

Internal security threats

External security threats

Legal and compliance requirements

Managing hybrid email deployments and migrations to Microsoft 365

Teams data structure

[1] — http://info.microsoft.com/rs/157-GQE-382/images/EN-GB-CNTNT-eBook-Security-HolisticVision.pdf

#1 Accidental deletion

If you delete a user, whether you meant to or not, that deletion is replicated across the network, along with the deletion of their OneDrive for Business account and mailbox.

Native recycle bins and version histories included in Microsoft 365 can only protect you from data loss in a limited way, which can turn a simple recovery from a proper backup into a big problem after Microsoft 365 has geo-redundantly deleted the data forever, or if the retention period has passed.

There are two types of deletions in the Microsoft 365 platform, soft delete and hard delete. An example of soft delete is emptying the Deleted Items folder. It is also referred to as "Permanently Deleted." In this case, permanent is not completely permanent, as the item can still be found in the Recoverable Items folder.

A hard delete is when an item is tagged to be purged from the mailbox database completely. Once this happens, it is unrecoverable, period.

#2 Retention policy gaps and confusion

The fast pace of business in the digital age lends itself to continuously evolving policies, including retention policies that are difficult to keep up with, let alone manage. Just like hard and soft delete, Microsoft 365 has limited backup and retention policies that can only fend off situational data loss, and is not intended to be an all-encompassing backup solution.

Another type of recovery, a point-in-time restoration of mailbox items, is not in scope with Microsoft. In the case of a catastrophic issue, a backup solution can provide the ability to roll back to a previous point-in-time prior to this issue and saving the day.

With a Microsoft 365 backup solution, there are no retention policy gaps or restore inflexibility. Short term backups or long-term archives, granular or point-in-time restores, everything is at your fingertips making data recovery fast, easy and reliable.

#3 Internal security threats

The idea of a security threat brings to mind hackers and viruses. However, businesses experience threats from the inside, and they are happening more often than you think. Organizations fall victim to threats posed by their very own employees, both intentionally and unintentionally.

Access to files and contacts changes so quickly, it can be hard to keep an eye on those in which you've installed the most trust. Microsoft has no way of knowing the difference between a regular user and a terminated employee attempting to delete critical company data before they depart. In addition, some users unknowingly create serious threats by downloading infected files or accidentally leaking usernames and passwords to sites they thought they could trust.

Another example is evidence tampering. Imagine an employee strategically deleting incriminating emails or files — keeping these objects out of the reach of the legal, compliance or HR departments.

#4 External security threats

Malware and viruses, like ransomware, have done serious damage to organizations across the globe. Not only is company reputation at risk, but the privacy and security of internal and customer data as well.

External threats can sneak in through emails and attachments, and it isn't always enough to educate users on what to look out for — especially when the infected messages seem so compelling. Exchange Online's limited backup/recovery functions are inadequate to handle serious attacks. Regular backups will help ensure a separate copy of your data is uninfected and that you can recover quickly.

#5
Legal and compliance requirements

Sometimes you need to unexpectedly retrieve emails, files or other types of data amid legal action. Something you never think it is going to happen to you until it does. Microsoft has built-in a couple of safety nets (litigation hold and retention). But, these are not a robust backup solution that will keep your company out of legal trouble. For example, with a backup solution, if you accidentally delete emails or documents before implementing a legal hold, you'll still be able to get them back to ensure you meet your legal obligations.

Legal requirements, compliance requirements and access regulations vary between industries and countries, but fines, penalties and legal disputes are three things you don't have room for on your to-do list.

#6
Managing hybrid email deployments and migrations to Microsoft 365

Organizations that adopt Microsoft 365 typically need a window of time to serve as a transition window between on-premises Exchange and Microsoft 365 Exchange Online. Some even leave a small portion of their legacy system in place to have added flexibility and additional control. These hybrid email deployments are common, yet pose additional management challenges.

The right Microsoft 365 backup solution should be able to handle hybrid email deployments, and treat exchange data the same, making the source location irrelevant.

Furthermore, you should be able to store the data anywhere you choose, whether on premises, in cloud object storage such as AWS S3 or Azure Blob, or with a managed service provider.

#7 Teams data structure

Microsoft Teams is gaining rapid adoption and growth with the increase in remote working. It's now the center of our productivity universe. Microsoft structures Teams as a user interface that brings together Microsoft 365 services, such as SharePoint Online and OneDrive for Business. This approach provides agile, real-time communication and collaboration for teams.

You need to protect data in these locations, but that's not all you need to protect. Teams has settings, configurations, and membership which all need to be protected and recoverable. A purpose-built backup solution can protect not only the data but also these settings and ther associated interconnections between applications.

More than ever before, people are spinning up Teams for projects and special initiatives at a rapid rate. But once you complete a project you probably need to keep a copy of the ended project for long-term needs such as legal and compliance requests. What often happens is that these Teams get mistakenly deleted or retention misapplied, which makes other files or essential documents unavailable.

Backups can also help in short-term scenarios. For example, if an employee says something inappropriate in a Teams conversation, but then deletes the message, having a backup would make those chats recoverable and available to HR for review. Third-party backup vendors not only provide protection from the unknown but can also offer a variety of ways to restore missing or accidentally deleted teams or channels.

How often do these reasons happen?

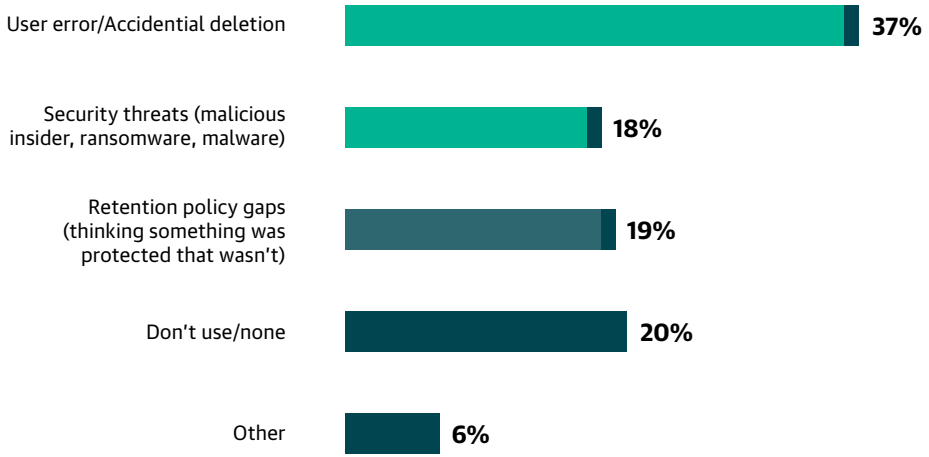
By now you understand why it's critically important to back up your Microsoft 365 data. But you're probably wondering to what extent these seven data protection vulnerabilities actually happen. Unfortunately, the answer is far too often...

Over 1,000 IT professionals were asked what forms of data loss they had experienced in the cloud. User error/accidental deletion, security threats and retention gaps all made the list from 18% to as high as 37%[2].

The scary reality is that even though sensitive cloud data is stored in Office documents, an estimated 76% is not being backed up[2]. In fact, IDC states that 6 out of every 10 organizations don't have a data protection plan for their Microsoft 365 estates[3]. Do you work in one of these unprotected organizations? If so, hopefully you now have the insights available through this report to encourage your organization to protect its Microsoft 365 data.

[2] — Veeam customer survey, September 2019
[3] — IDC: Why a Backup Strategy for Microsoft Microsoft 365 is Essential, 2019

Q14. What forms of data loss have you experienced within the cloud? (Check all that apply)



Respondents = 1,579

Conclusion

Go ahead and take a closer look. There are security gaps you may not have been aware of before.

You already made a smart business decision by deploying Microsoft 365, now find a backup solution that offers you both complete access and complete control of your Microsoft 365 data and avoid the unnecessary risks of data loss.

If you found this report helpful, we encourage you to email it to a colleague: Forward this report

Veeam Backup
for Microsoft 365

Download free trial
https://go.veeam.com/backup-office-365

Gold
Microsoft Partner

#1 Microsoft 365 Backup

More control. Effortless recovery.

NEW Veeam® Backup *for Microsoft 365* v6 has added the **Self-Service Restore Portal** for Microsoft 365 environments, empowering IT administrators to securely delegate restores to their users. V6 also includes **backup copy to Amazon S3 Glacier, Glacier Deep Archive and Azure Archive**.

Version 6 of Veeam Backup *for Microsoft 365* provides:

- **Automation and scalability** for enterprise organizations
- **Time savings** through handling restores for Microsoft 365 users
- **Enhanced security** with multi-factor authentication (MFA)
- **Recovery confidence** with a backup copy in low-cost object storage

Get started with a 30-day FREE trial!