

6 Critical Reasons for Office 365 Backup

The case for why organizations
need to protect Office 365 data

veeam

Virtual
Systems 

Introduction

Do you have control of your Office 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 Office 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 and OneDrive for Business data.

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



"We worried about the backup and retention policies in Office 365. Microsoft takes care of our data, and protecting historical email data is important. That's why we decided to ensure we have a backup of our data residing in Office 365."

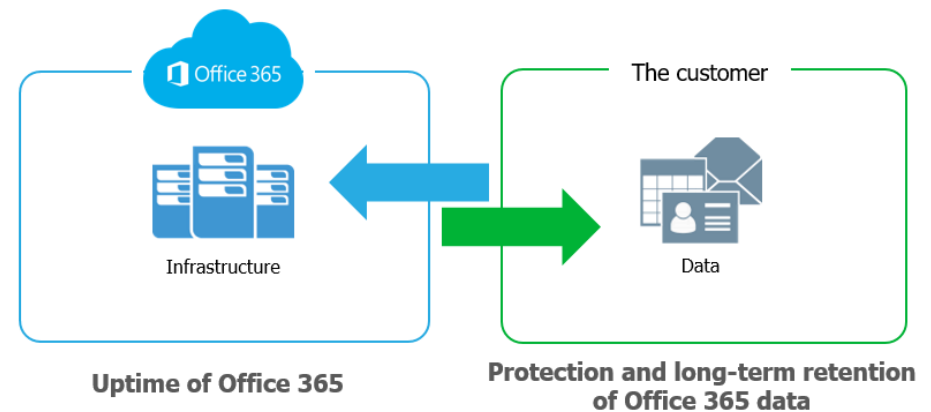
— **Karen St.Clair**, IT Manager,
Columbia Power & Water Systems

The big Office 365 misconception

The misunderstanding falls between Microsoft's perceived responsibility and the user's actual responsibility of protection and long-term retention of their Office 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 Office 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 Office 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.

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



"With Office 365, it's your data. You own it.
You control it."

– *The Office 365 Trust Center*

6 reasons why backing up Office 365 is critical

As a robust and highly capable Software as a Service (SaaS) platform, Microsoft Office 365 fits the needs of many organizations perfectly. Office 365 provides application Availability and uptime to ensure your users never skip a beat, but an Office 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 days¹. 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 Office 365, six 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 Office 365

¹ <https://discover.office.com/6-steps-to-holistic-security/chapter1/>



#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 personal SharePoint site and their OneDrive data.

Native recycle bins and version histories included in Office 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 Office 365 has geo-redundantly deleted the data forever, or it has fallen out of the retention period.

There are two types of deletions in the Office 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 mailbox.

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, Office 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 an Office 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 safety nets, (Litigation Hold) but again, these are not a robust backup solution capable of keeping your company out of legal trouble. For example, if you accidentally delete a user, their on-hold mailbox, personal SharePoint site and OneDrive account is also deleted.

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 mi- grations to Office 365

Organizations that adopt Office 365 typically need a window of time to serve as a transition window between on-premises Exchange and Office 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.

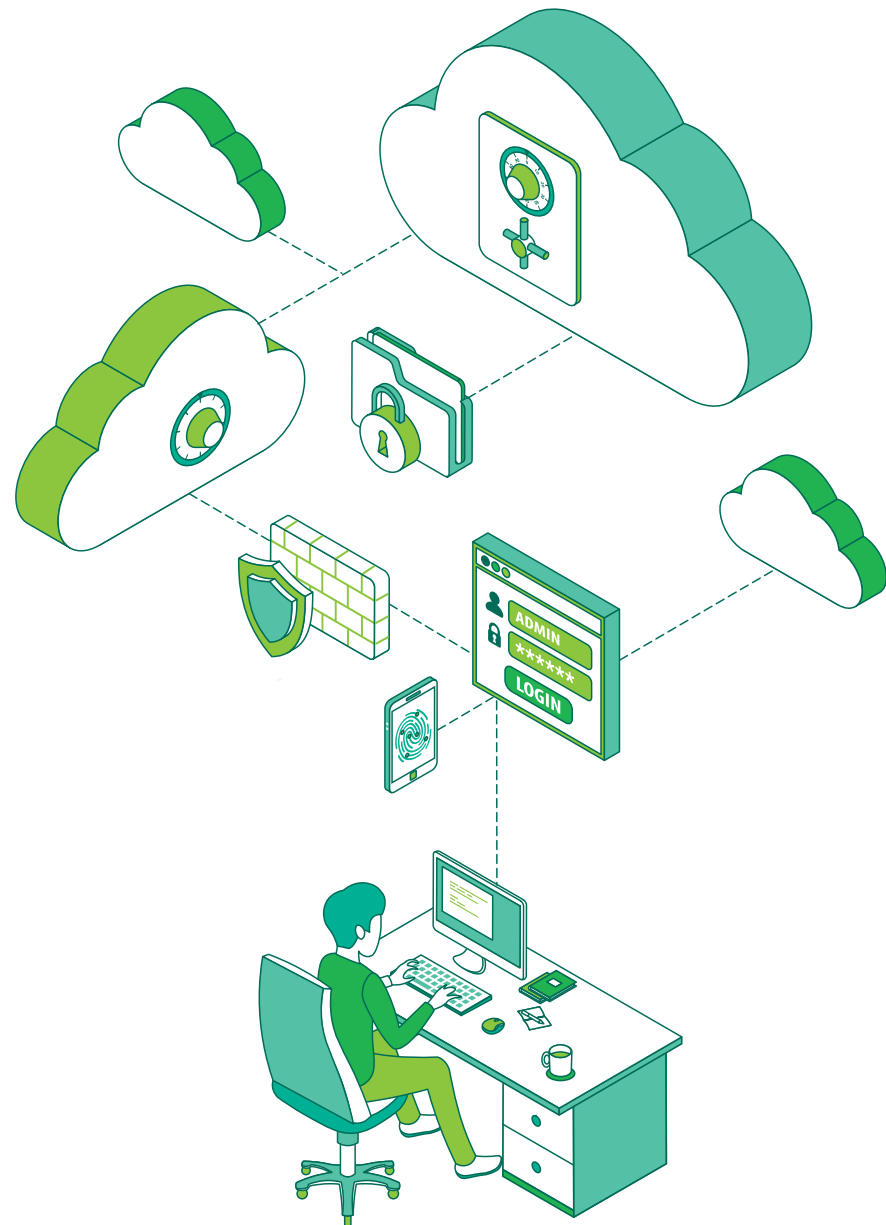
The right Office 365 backup solution should be able to handle hybrid email deployments, and treat exchange data the same, making the source location irrelevant.

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 Office 365, now find a backup solution that offers you both complete access and complete control of your Office 365 data and avoid the unnecessary risks of data loss.

Learn more about Office 365 backup at:
<https://www.veeam.com/backup-microsoft-office-365.html>



veeam

Virtual
Systems 