MICROSOFT 365 BACKUPS

7 KEY REASONS WHY YOUR ORGANISATION NEEDS TO PROTECT ITS MICROSOFT 365 DATA

itLeaders

INTRODUCTION

How much control do you have over your Microsoft 365 data? Is everything that you need accessible? Typically, people say, "Of course I do," or "It's all handled by Microsoft.".

But consider it more carefully - are you actually certain about that?

As a company, Microsoft provides excellent service to its customers and takes care of a wide variety of things. Its primary focus is to manage Microsoft 365 infrastructure and maintain uptime for its users. At the end of the day, they're 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. There's a common misunderstanding and widespread belief that Microsoft fully backs up your data. However, without shifting your mindset, this can ultimately have damaging repercussions when this responsibility isn't upheld.

It is vital to maintain secure access to and control over your Microsoft Teams, SharePoint Online, Exchange Online and OneDrive for Business data.

In the following report, we examine the hazards of not having an Microsoft 365 backup and explain why and how backup solutions for Microsoft 365 provide long-term retention and data protection for your business.

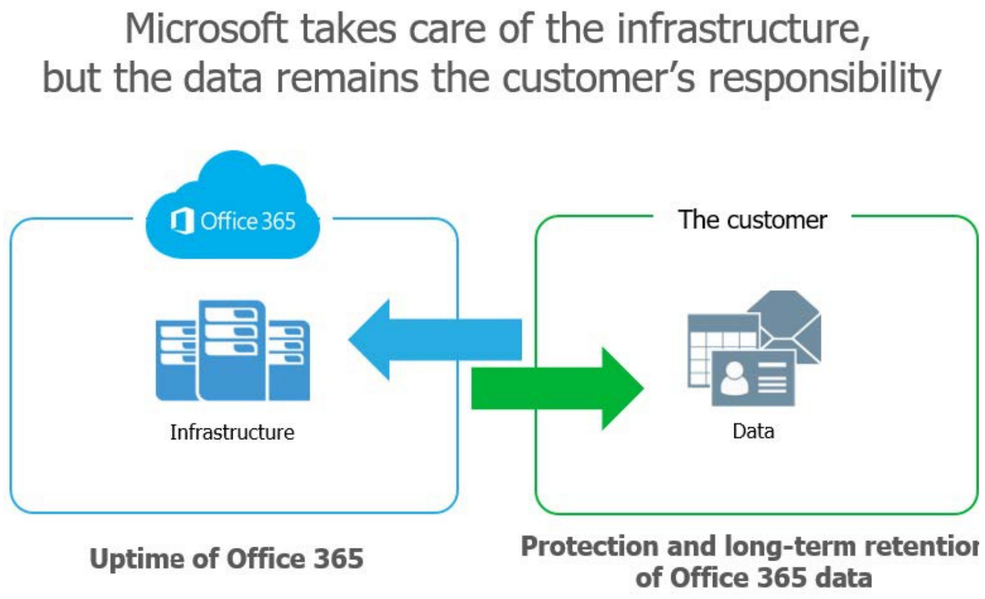
COMMON MISCONCEPTIONS ABOUT MICROSOFT OFFICE 365

A pertinent problem lies in the perception between Microsoft's responsibilities and the actual responsibility of users concerning the protection and long-term retention of their Microsoft 365 data. Users' expectations of backup and recovery are often different from what Microsoft provides.

Hence, apart from the usual security measures and safeguards that Office 365 has in place, you may need to rethink and review the level of control you have over your data and how much access you actually have to it.

With Microsoft Office 365, users are offered geo-redundancy, which is often mistaken for backup. The process of backup involves making a copy of historical data, then storing it somewhere else. Even more important, however, is that you have direct access to and control over the backup. Hence, in the event of data loss, accidental deletion or a malicious attack, you can quickly restore it.

On the other hand, geo redundancy provides protection against site or hardware failure, so even if there is a system crash or outage, your users will remain productive.



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

7 Key Reasons Why Your Organisation needs to protect its Microsoft 365 data

THE IMPORTANCE OF BACKING UP OFFICE 365 FOR YOUR BUSINESS

Microsoft Office 365 is an extremely dynamic, comprehensive, user-friendly and scalable SaaS (Software as a Service) solution for a wide range of businesses. The platform has the capabilities to meet the needs of many different types of organisations, in various industries and niches.

In addition to ensuring your users never miss a beat, Microsoft 365 provides uptime and application availability, but having a Microsoft 365 backup can also safeguard you from many other security threats.

Many people mistakenly assume that the recycle bin will suffice, however, there is an alarmingly lengthy amount of time between data compromise to discovery, with the average time being over 140 days. You are likely to overlook something missing or gone until it is too late to retrieve it from the recycle bin.

The top seven vulnerabilities in data protection, according to hundreds of IT professionals worldwide, that have migrated to Microsoft 365 include:

Threats To Internal Security

External Security Threats

Accidental Deletion

Confusion & Retention Policy Gaps

Compliance & Legal requirements

Microsoft 365 Migrations and Managing Hybrid Email Deployments

Teams Data Structure

#1 THREATS TO INTERNAL SECURITY

Hackers and viruses come to mind when thinking about a security threat. However, it's important to note that businesses also face threats internally, and they are alot more common than you think.

Both intentionally and unintentionally, organisations are exposed and regularly fall victim to threats posed by their very own employees. File access and contacts change rapidly in workplaces and notably, it can become very challenging to fully monitor this consistently.

Unfortunately, it is impossible for Microsoft to tell the difference between a regular user and a terminated employee trying to delete critical company data before they depart.

Additionally, past employees could engage in evidence tampering, where they strategically delete incriminating files or emails, before their departure. Other users unknowingly create serious security threats by downloading malicious or infected files or accidentally sharing their usernames and passwords to sites that they assumed they could trust.

#2 EXTERNAL SECURITY THREATS

Globally, malware and viruses, such as ransomware, have caused significant damage to numerous organisations. It is not only the company's reputation that is at risk, but also the privacy and security of its internal data and customers' confidential information.

Emails and attachments can carry many external threats, and educating users on what to look out for doesn't always work, especially when the messages they receive seem so legitimate and convincing.

Microsoft Exchange Online features very limited backup and recovery capabilities which are insufficient in handling serious attacks. Hence, by periodically backing up your data, you will be able to ensure that a separate copy remains uninfected, which you can then restore quickly and easily, in the event of a data breach or security threat.

#3 ACCIDENTAL DELETION

In the event you delete a user, unfortunately this deletion is replicated across the network, as well as the deletion of their OneDrive for Business and Inbox accounts.

With Microsoft 365, version histories and its native recycle bins provide limited data loss protection. You can also easily restore from an exact backup to a larger one, or if the retention period has expired.

There are two methods of deleting files on Microsoft Office 365 - a soft delete and a hard delete. Emptying the Deleted Items folder is an example of soft deletion. This is also known as "permanently deleted". The item will still appear in the Recoverable Items folder in this case, so it isn't actually permanent as such.

On the other hand, a ‘hard delete’ results in the full deletion and permanent removal of an item from the mailbox database. Once this occurs, you cannot undo it.

#4 CONFUSION & RETENTION POLICY GAPS

With business operations moving at such a rapid pace in this digital era, policies, including retention guidelines, are continually evolving and have become difficult to manage and keep up with.

In the same vein as hard and soft delete, Microsoft 365 features limited backup and retention policies that cannot prevent all kinds of data loss, and it is not designed nor intended to be an all-encompassing backup solution. The ‘point-in-time restoration’ of mailbox items is another type of recovery option that is not included in Microsoft's scope of services.

Having an effective backup solution in place can enable you to rollback to a previous point-in-time before the issue occurred, saving you from a potentially catastrophic event. Using a Microsoft Office 365 backup solution eliminates gaps in retention policies and restore inflexibility.

Whether it be short-term backups or long-term archives, granular or point-in-time restores, everything is at your fingertips to make data recovery as fast, simple and reliable as possible.

#5 COMPLIANCE & LEGAL REQUIREMENTS

Legal action can sometimes force you to retrieve emails, files, or other types of data unexpectedly. That is something you don't anticipate until it happens. In this instance, several safety nets have been built-in by Microsoft to utilise (litigation hold and retention). However, they don't provide a dependable and robust backup solution that can protect your business from legal trouble or prevent being sued.

For example, if you delete documents or emails before implementing the legal hold, you will still be able to retrieve them from your backup and meet any required legal obligations. Whilst legal and compliance requirements and access regulations vary from industry to industry and from country to country, fines, penalties, and legal disputes are definitely something you want to avoid!

#6 MICROSOFT 365 MIGRATIONS & MANAGING HYBRID EMAIL DEPLOYMENTS

In order to transition from on-premises Exchange to Microsoft Office 365 Exchange Online, organisations adopting Microsoft 365 typically require a migration window. In some cases, companies leave a small portion of their legacy system in place to provide them with more control and added flexibilityas well.

Despite being common, hybrid email deployments can present management challenges. Ideally, a backup solution for Microsoft 365 should be able to handle hybrid email deployments, and treat exchange data the same regardless of its source location. 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

The data you store should also be accessible anywhere - whether it is on premises, stored on a cloud solution or with a managed service provider like IT Leaders.

#7
TEAMS DATA STRUCTURE

With the growth of remote work in recent times, Microsoft Teams is gaining rapid traction and is being adopted by many businesses and organisations around the world. It has become an integral part of our workflow and transformed into a central hub of collaboration and productivity for many workplaces.

The Microsoft Teams user interface combines a number of Microsoft 365 services, including SharePoint Online and OneDrive for Business. Users can collaborate and communicate in real time using Teams. It is important to remember that data in these locations needs to be protected as well. It is vital that the settings, configurations and memberships that Teams have set up are protected and recoverable.

By implementing a dedicated backup solution, you are able to protect not only the data, but also these settings and the interconnections between applications.

As the number of Team users increases, more and more individuals are collaborating on projects and taking part in special initiatives.

However, once you finish a project, it is likely you will need to keep a copy for long-term purposes, for example, legal and compliance requirements.

Many times, these Teams are deleted by accident or their retention settings are misapplied, resulting in the loss of crucial files and documents. Short-term backups can be helpful in situations like these. Another example of this would be having a backup of an employee's Teams conversation.

A colleague may have said something inappropriate but then deleted those messages, however, having a backup in place would make those conversations retrievable and enable HR to review them as needed.

In addition to providing protection from the unknown, third-party backup vendors can offer options for restoring Teams or channels that may have been accidentally deleted.

DO THESE DATA SECURITY ISSUES HAPPEN FREQUENTLY?

As you can see, it's critical to backup your Microsoft Office 365 data. However, you might wonder how widespread these seven data protection vulnerabilities really are. Well, unfortunately, it is extremely common, with recent studies reporting that user error or accidental deletion, retention gaps and security threats accounted for up to 37% of data losses.

Unfortunately, even though 76% of Microsoft Office documents contain sensitive data, they are not backed up. Despite the fact that over 76% of Office documents contain sensitive cloud data, they are not regularly backed up.

Is your company one of those unprotected organisations with no backup solutions in place? We hope that this report has provided you with a better overall understanding of the ramifications of absent backups, as well as providing you with valuable insights into ways you can effectively protect your Microsoft 365 data.

CONCLUSION

It's definitely time to consider looking at your business systems and network more closely. Perhaps you were unaware of the existing security gaps or didn't know you needed a backup in place.

You have already made the smart business decision of deploying Microsoft Office 365, however, you now need an effective backup solution that offers you full control and access to your Microsoft 365 data whilst also minimising the risk of data loss or potential security threats.

If you need help with setting up a Microsoft 365 backup or are interested in acquiring Managed IT services from a provider you can trust, get in touch with IT Leaders today! We would love to help protect your business.

itLeaders

GET IN TOUCH

service@itleaders.com.au

1300 381 584

itleaders.com.au

Unit 3 / 42 Lawrence Drive,
Nerang QLD 4211