Brought to you by:

VEEAM

Microsoft 365® Backup

for dummies®
A Wiley Brand

Manage and safeguard your data

Understand data loss in the cloud

Choose a third-party backup solution

Veeam Special Edition

Jennifer Reed

About Veeam

Veeam® is the leader in backup, recovery and data management solutions that deliver Modern Data Protection. The company provides a single platform for Cloud, Virtual, Physical, SaaS and Kubernetes environments. Veeam customers are confident their apps and data are protected and always available with the most simple, flexible, reliable and powerful platform in the industry. Veeam protects over 400,000 customers worldwide, including 81% of the Fortune 500 and 69% of the Global 2,000. Veeam's global ecosystem includes 35,000+ technology partners, resellers and service providers, and alliance partners and has offices in more than 30 countries. To learn more, visit www.veeam.com or follow Veeam on LinkedIn @veeam-software and Twitter @veeam.

Microsoft 365® Backup

Microsoft 365® Backup

Veeam Special Edition

by Jennifer Reed

for dummies®
A Wiley Brand

Microsoft 365® Backup For Dummies®, Veeam Special Edition

Published by
John Wiley & Sons, Inc.
111 River St.
Hoboken, NJ 07030-5774
www.wiley.com

ISBN 978-1-119-89536-7 (pbk); ISBN 978-1-119-89537-4 (ebk)

Manufactured in the United States of America

10 9 8 7 6 5 4 3 2 1

Publisher's Acknowledgments

We're proud of this book and of the people who worked on it. Some of the people who helped bring this book to market include the following:

Project Editor: Martin V. Minner

Editorial Manager: Rev Mengle

Associate Publisher: Katie Moore

Business Development Representative: Karen Hattan

Production Editor: Tamilmani Varadharaj

Special Help: Edward Watson

Table of Contents

Introduction

There is no greater equalizer for businesses today than cloud technologies. Long gone are the days when cutting-edge collaboration tools and productivity solutions were reserved for Fortune 500 companies with big IT budgets and highly trained staff. Today, nonprofits and small businesses, including "mom and pop" stores and solo-preneurs, have access to the same solutions big corporations use, for the cost of a cup of coffee. In Microsoft 365, for example, the Microsoft Teams web conferencing tool that a global corporation uses to broadcast an annual shareholders' meeting, powered by artificial intelligence and translated into several languages in real time, is the same tool that a small nonprofit organization is using to communicate and collaborate with non-English-speaking beneficiaries in far-flung locations.

With a level playing field, the adoption of cloud technologies has exploded, and with it, the rapid growth of data. As organizations, big or small, go through digital transformation, fresh approaches to customer engagement and employee experiences are making their way into people's daily lives and the workplace. Want to buy insurance? No need to hop into your car and visit the town's only trusted insurance agent. You can buy insurance from the comfort of your home using your smartphone. Need to pull your company's top salespeople into a planning meeting? Skip the drive or the flight (and hotel expenses) and hold a video conference integrated with business intelligence tools and whiteboarding capabilities. An employee lost his laptop at the airport and is freaking out about confidential data? Simply reset the laptop remotely to factory settings and have the employee pick up a new laptop that's provisioned with company security settings as soon as the device is powered on.

Cloud computing has democratized technology. Purchasing hardware, installing software, patching servers, and other repetitive low-value-added IT tasks are now outsourced to the cloud provider. This model frees up IT professionals to focus more on tasks that drive business outcomes such as modernizing home-grown apps or managing the organization's security posture. The role IT professionals play in a landscape where data loss, security breaches, and invasion of privacy are the new normal has never been more critical. With that spotlight comes great pressure to

deliver on the organization's expectations that the IT team will ensure data is safe, privacy is not compromised, productivity is unencumbered, and brand reputation is intact.

About This Book

Microsoft 365 Backup For Dummies, Veeam Special Edition, addresses the data security challenges organizations face in today's computing landscape by outlining the out-of-the-box security features in Microsoft 365 and uncovering the gaps that require action to achieve an effective backup and recovery strategy. It explains the game-changing functionalities in Microsoft 365 to drive productivity while tackling the repercussions of data loss either intentionally or accidentally.

If you are an IT professional whose goal is ensuring business continuity through successful recoveries from data loss, this book serves as one of the critical inputs toward that goal. A business owner or decision-maker with a keen interest in data protection will gain an understanding of who does what in the era of cloud provider/cloud consumer ecosystems. An end-user who wants to stay productive will find tips to avoid the pitfalls of data loss. Regardless of your role in the organization, if you are using Microsoft 365, this book is a valuable read to optimize your investment in the technology.

Icons Used in This Book

This book features the familiar For Dummies icons that offer visual cues about the text.


TIP

The **Tip** icon marks tips (duh!) and shortcuts that you can use to make tasks simpler.


REMEMBER

Remember icons mark the information that's especially important to know. To siphon off the most important information in each chapter, skim through these icons.


WARNING

The **Warning** icon tells you to watch out! It marks important information that may save you headaches.

IN THIS CHAPTER

- Stopping a bad actor from joining your team
- Knowing the difference between moving and copying data
- Incorporating data backup into the migration plan

Chapter 1
Setting the Stage for Backup in Microsoft 365

"Teams too?" That's the incredulous reaction from a customer whose Microsoft 365 users had recently been targeted with a phishing attack using Microsoft Teams. Apparently, legit-looking Teams invitations and file sharing notifications with an almost pixel-perfect rendition of the real Teams emails have started cropping up in the customer's Microsoft 365 tenant. Just think — this customer had invested in driving Teams adoption to reduce email, believing this strategy would reduce the organization's vulnerability.

Well, it's about time. With 20 million daily active users (50 percent growth in three years), Teams is not a bad place for hackers to play. With a familiar-looking Teams email notification, it isn't difficult to get unsuspecting end-users to click a link that takes them to a spoofed but slick login page where they enter their credentials, thus letting the bad guys in through the front door.

Before you start mocking end-users who fall prey to phishing emails, know that hackers were able to breach a limited number of subscribers to Microsoft webmail services by compromising a

support agent's credentials early in 2019. Although the breach did not affect enterprise users and the subscribers' login credentials were not compromised, the incident points to the fact that even people in IT are not immune to phishing emails. You'd better have a good backup and recovery strategy in place to fall back on if you ever end up in this less-than-ideal situation.

Understanding the Need for Backing Up Data

Cloud technology is great. It has freed IT departments from implementing and managing complex and critical IT infrastructure by outsourcing those tasks to a cloud provider. What isn't great, however, is when there is a mismatch between what you think your cloud provider backs up and what the provider is contractually responsible for backing up. Microsoft 365 is a great example of this unclear shared responsibility.

Comparing high availability and redundancy to backup

Cloud service providers pride themselves on having the infrastructure to offer a highly available system that ensures their services will always be available no matter what happens. One of the principles they apply to achieve high availability is to build redundancy into the design of the infrastructure.

Redundancy can be on a physical or data level. On a physical level, for example, a replica server is present, ready to take over if the main server fails. The replica can also act as a load balancer for an overloaded main server.

On the data level, redundancy is achieved by replicating copies of data in multiple systems or locations so that users are not affected when a server or data center goes down.

In contrast, a backup is simply a copy of data on a disk, a tape, or in cloud storage. With the right tools and processes, you can restore backup data into a new system in case of a failure to minimize business disruptions.

REMEMBER

Redundancy is the game plan in case something fails. In Microsoft 365, this capability is built in to minimize downtime and ensure rapid recovery in the event of a failure. The replica server and replicated copies, however, do not solve for data loss. If something is deleted or corrupt on the production side, then you'll also get deleted and corrupt data on the replica servers!

Having your own separate backup, in addition to Microsoft's redundancy and replication, is the ticket to a comprehensive and complete approach to data protection in Microsoft 365. That should be the focus for your IT teams.

Exploring archiving and In-Place Holds

When you subscribe to Microsoft 365 services, Microsoft ensures you are storing your data in a redundant environment designed for high availability to meet the Microsoft service-level agreements.

Exchange Online, for example, replicates mailboxes to multiple databases hosted on multiple data centers. That way, database failures or catastrophic events affecting a data center do not interfere with your ability to access your data. For IT administrators, this feature means no on-premises servers to patch ever again. How great is that!

As a subscriber to Microsoft 365 services, you do not have access to these databases and data centers if you need to restore lost data. You can move data around to save on cloud storage or enable features to preserve data, but these methods are not meant to create a copy of your data for backup. Archives and Holds are two features in Microsoft 365 that are commonly misunderstood to be a backup alternative. Consider the following:

- Enabling the archive mailbox feature provides up to 1TB of archive storage. When this feature is enabled, an Exchange retention policy is applied by default. This policy moves email data older than two years from the primary mailbox to the archive mailbox. Take note that no data is copied in the process. Data is merely moved from one location to another.

» Preserving data using the In-Place Hold feature keeps the contents of the mailbox (and its corresponding archive mailbox if enabled) indefinitely or for a specified number of days. The primary purpose for this functionality is to protect and preserve data in case of litigation where the data may be used as evidence. Holds do not make copies of data, so they aren't a backup solution.

WARNING

If you're thinking of using the OneDrive for Business sync tool as a workaround for backing up your cloud files to your hard drive, stop right there and don't do it. The tool is called a *sync tool* for a reason. Deletions on your local copy will be synced to the cloud, so this tool defeats one of the purposes of backup, which is to prevent data loss.

Planning the Microsoft 365 Migration

Although there are standard best practices and proven approaches to Microsoft 365 migration, no two organizations are exactly alike, so the unique needs of an organization must be factored into the migration plan. In this section, I cover some of the key considerations when planning an Microsoft 365 migration and how they affect your backup strategy.

Choosing between cloud-only and hybrid

Organizations coming from another cloud-based email system like Gmail, or those using IMAP mailboxes, typically opt for a cutover migration where all mailboxes are moved at the same time to Exchange Online. Because all the data will be in the cloud, data backup is simplified. There is only one source for the data: the cloud.

Large organizations running an on-premises Exchange email system, however, may decide to coexist between the cloud and on-premises. This scenario typically requires a hybrid migration approach where some user data may be in the cloud, some on-premises, or some on both. When you plan for backup, don't forget the on-premises data. Limitations like In-Place Holds can affect your backup strategy.

Determining what data goes where

Microsoft 365 is not just email or Exchange Online. It also comes with SharePoint Online, OneDrive for Business, and Microsoft Teams. Depending on the license, Microsoft applications such as Word, Outlook, and Excel may be included in the service.


TIP

Organizations that are already running an on-premises SharePoint environment need to decide whether to migrate SharePoint Server data to SharePoint Online on top of email data. That's one more data source to account for backup. I have seen organizations with terabytes of SharePoint data, which means you must think about where backup data is stored. Should the backup be on another server on-premises, or should it be stored in Microsoft Azure or Amazon Web Services?

Incorporating data security into the migration plan

Data is a valuable commodity, so you shouldn't be surprised if security threats come not just from hackers but also from inside the organization. Even if a well-meaning employee unintentionally leaks data, the repercussions for data loss can be staggering. For that reason, data security shouldn't be an afterthought in your migration planning. If basic policies such as identity and access management are defined up front, you'll save yourself from a major data vulnerability. In fact, data security may just be the one thing that will save you when a bad actor tries to trick your end-users into letting him or her join your Teams hub in Microsoft 365.

IN THIS CHAPTER

- Taking stock of your responsibilities as a cloud customer
- Avoiding the pitfalls of data loss

Chapter 2
Managing Your Data in Microsoft 365

IDC (www.idc.com) predicts that data created, captured, or replicated in traditional and cloud data centers, enterprise infrastructure, and end points (PCs, smartphones, and Internet of Things devices) will grow to 175 zettabytes (ZB) by 2025.

Just how big is a zettabyte? Consider the 64GB smartphone you or someone you know might be using. Now, fill 17.2 billion of those smartphones to capacity and you'll have an idea of how big a zettabyte is.

Your organization, with its Microsoft 365 subscription, is undoubtedly a contributor to this data explosion. The data you generate to run your business is the same data you must manage and protect. You know that great power you wield to steward your company data? That comes with great responsibilities. In this chapter, I cover how data is protected in Microsoft 365 and show you the impacts of data loss.

Breaking Down Data Protection in Microsoft 365

Microsoft 365 data at rest or in transit are protected with encryption. The complex and costly work of building the encryption infrastructure is already built into the service. Imagine having emails sent by your employees automatically encrypted if the word "confidential" is in the message without requiring the sender to do anything special. How about automatically revoking access to the encrypted email after a week? You can do all that with Advanced Message Encryption in Microsoft 365.

Data loss prevention (DLP) policies can be configured in Microsoft 365 to ensure sensitive information is protected from accidental leakage. Between DLP and encryption, you have a robust set of capabilities to protect data. But don't stop there. Consider the tenant admins who have privileged access to the Microsoft 365 tenant. They are a prime target for hackers. So, what do you do? Identity and access management policies to the rescue!

TIP

Microsoft 365 identity and access management policies are configurable to meet your organization's needs. As you think through your data protection strategy, don't forget to take advantage of the Zero Standing Access, a principle of privileged access management, a capability which, in essence, is identity and access management on steroids.

Because Microsoft 365 is a software-as-a-service (SaaS) solution, you can expect more security features and functionalities to be rolled into it on a regular basis. The work of IT administrators is never done — even in a cloud world.

ZEROING IN ON STANDING ACCESS

The Zero Standing Access principle means that you don't have to make everyone in the IT team a global admin all the time to share the workload. With Zero Standing Access, you give someone privileged access to perform certain tasks but only for a limited time. Actions taken by the admin during that period will be logged so you can monitor what's going on or be alerted when security events occur.

Clarifying the shared responsibility model

When you buy a new car, you expect certain security features from the manufacturer, such as brakes that work to help prevent you from running into another car. It is your responsibility as the driver, however, to step on the brakes when needed to avoid a collision.

Using Microsoft 365 is similar. You can expect certain things from Microsoft as the cloud service provider, and certain things are expected from you as the cloud customer. These expectations are rooted in the notion of a *shared responsibility* model.

In a SaaS solution like Microsoft 365, Microsoft is responsible for maintaining the global infrastructure to keep its services running. You, on the other hand, are responsible for maintaining and protecting the data you store in Microsoft 365. For example, identity and access management is built into the service, but you must enable features such as Zero Standing Access policies to realize the value of those features.

Microsoft creates replicas of your data to achieve redundancy and to minimize (or ideally eliminate) downtime of its cloud services. That replica lives in Microsoft's infrastructure. They own it, you don't. They have access to it and use it as a failover when a server is down. But you don't have access to that replica to restore a report you're working on if your laptop encounters the blue screen of death and causes you to lose data. Replicas don't solve for data loss. Do you have deleted and corrupt data in the production server? If so, your replica server will have those as well.

Demystifying backup and retention in Microsoft 365

One of the reasons people need backup is to mitigate accidental file deletions. If that's all you're worried about, then the Microsoft 365 Recycle Bin should save you from a disaster, right? Unfortunately, no. Here's why.

In Outlook, permanently deleted items are moved to a Recoverable Items folder, which can be configured to retain data up to 30 days. If you need to recover an item older than 30 days, you're out of luck.

In SharePoint Online or OneDrive for Business, you have 93 days to restore a deleted item before it's gone. Don't be misguided by talks of Stage 1 and Stage 2 Recycle Bins in SharePoint. They simply mean that if an end-user deletes an item from a SharePoint site, that item goes to the site Recycle Bin where it's retained for 93 days, during which it's recoverable by the end-user. If you delete that item in the site Recycle Bin before the 93 days are up, that item is moved to the site collection Recycle Bin where it stays recoverable by a SharePoint admin for the remainder of the 93 days.

WARNING

Data has a way of becoming important when it's gone. Not to strike fear in your heart, but consider the following scenarios:

- Remember Johnny, the ex-employee who was running a critical project for your VIP customer? His reports would be a big help now, but you'll have to start from scratch. He stored the files in OneDrive, and he left the company six months ago.
- What about Paul, your VP of Finance who last year emailed you the financial audit that your lawyers need today? Do you want to call him at his retirement villa in the Bahamas, hoping he kept a copy of the audit, because you permanently deleted your email copy? Good luck with that.

Realizing the Cost of Data Loss

Microsoft 365 can't protect you from data loss that results from accidental deletions, malicious users, configuration errors, or cyberattacks. Even if you can recover lost data, you may be dealing with a corrupted file that takes hours to rebuild. Worse, you may have already lost hours better spent on other things than trying to recover that data. I've been down that road and it isn't pretty.

Understanding the impacts of data loss

Data loss has severe impacts. It's expensive and unproductive, raises compliance risks, and harms your organization's reputation. The consequences can be so dire that according to a study conducted by the University of Texas, 94 percent of companies that suffer data loss do not survive — 43 percent never reopen, and 51 percent close within two years.

Trying to recover lost data is no fun. I have yet to meet an IT administrator who loves finding and recovering data so much he or she wouldn't mind missing a child's soccer game.

Taking control of your data in Microsoft 365

Knowing that data loss can be catastrophic, coupled with the understanding that even in Microsoft 365 you can suffer data loss, you now have the opportunity to start taking control of your data. The first step is to acknowledge that you need a third-party backup and recovery solution. Until Microsoft markets itself as a backup and recovery company, it doesn't make sense to try to use workarounds in Microsoft 365 to protect your business data. If you want your company to be thriving in 2025 and be contributing to the 175ZB of data IDC predicts will exist by then, then use the insights from this book to formulate your strategy for data protection.

IN THIS CHAPTER

- Stepping through data loss prevention policies
- Exploring the retention policies capabilities
- Knowing where and how data is stored in Microsoft 365

Chapter 3
Safeguarding Your Data in Microsoft 365

In the world of cybersecurity, you often hear pros talk about defense in depth (DiD) strategies. For laypeople, that means having a defense mechanism that can withstand an attack by establishing a series of security measures so if one mechanism fails, another one steps up to block the attack.

The DiD story for Microsoft 365 is remarkable when you realize the layers of mechanism that are in place to protect customer data. On the physical layer, only authorized personnel who have gone through background checks using biometric authentication are allowed inside the data centers. On the network layer, machines communicate only with other trusted machines in the Microsoft 365 network in an encrypted connection that's logged and audited. From an access standpoint, engineers are required to use multi-factor authentication and are granted only just-in-time access to troubleshoot issues. While they're working on an issue, all their activities are logged and audited.

All these lines of defense continue to the data that's stored on hard drives in Microsoft's data centers. The hard drives are encrypted with BitLocker technology so if you were to take a hard drive out of the data center (assuming it got past security), the data would be useless.

Although Microsoft spends more time, resources, and technology than you can possibly imagine to make all this possible, the shared responsibility model shows that safeguarding data does not fall solely on Microsoft's shoulders. You don't need *Mission Impossible*-level tech or gadgets to ensure the safety of your data because there are straightforward policies you can configure and implement to prevent data loss and mitigate security risks.

In this chapter, I explore the compliance capabilities available in Microsoft 365. The Microsoft 365 Compliance Center is not a backup center, so I also cover the gaps in the compliance story with third-party backup solutions.

Governing Data in Microsoft 365

If you're in the IT industry, you've probably heard of the General Data Protection Regulation (GDPR), a set of rules designed to give users control over their personal information and impose accountability on the organizations collecting personal information. Although the regulation is applicable only to European citizens, this landmark regulation is shaping global data protection requirements.

Most likely, your company is already collecting personal information from your employees, customers, and vendors. As a result, you have a responsibility to safeguard this data if for no reason other than for compliance.

Organizations operating in regulated industries such as healthcare, finance, and legal are required to comply with stringent retention requirements. The Health Insurance Portability and Accountability Act (HIPAA), the Payment Card Industry Data Security Standard (PCI DSS), the Federal Financial Institutions Examination Council (FFIEC), and the Federal Information Security Management Act (FISMA), for example, specify retention policies that may require a third-party backup solution.

Unpacking Retention Policies

Retention policies allow you to determine what data to retain or delete permanently. The process of retaining or deleting is automated by letting users classify their data and then programmatically applying retention policies based on the classification of the data.

Newer Microsoft 365 tenants are provisioned with several retention labels already configured to work in Outlook, SharePoint, and OneDrive. These labels dictate how long an item is retained within the Microsoft 365 tenancy.

One might conclude that applying a label that retains items forever gives you a copy to go back to if you accidentally delete the item. If that's the case, retention policies would be a good backup workaround without using a third-party tool, right?

Wrong — unless your desire is to make your backup and recovery strategy unreliable, costly, and painful. Asking end-users to apply labels as a backup solution doesn't scale and produces inconsistency. If you configure the retention policy to automatically apply to everyone in the organization, you're putting the onus on the IT administrator to deal with the complexities of the different retention scenarios for each of the Microsoft 365 workloads and the changes and updates regularly rolled out in the service. And that's just the beginning of your woes. Think of a scenario where you implemented a retention policy that permanently deletes files after three years. You assign that policy to everyone's OneDrive accounts. As soon as that policy is applied, a lot of content will be immediately deleted if your organization has been using OneDrive for more than three years.

Enhancing Compliance with Third-Party Backup Solutions

The current data explosion is both a blessing and a curse. It's a blessing because the amount of data available provides more insights that drive business outcomes. It is a curse because now more than ever, there is a strong pressure to meet compliance requirements from a multitude of regulatory boards. A 2019 Thompson Reuters study entitled "Cost of Compliance" reported that more than 1,000 regulatory bodies worldwide generate more than 200 updates per day.

For some organizations, relying solely on the Microsoft 365 Compliance Center for a complete compliance strategy is not enough. Proving that data is indeed protected and retention policies are truly applied may require a third-party backup solution. In this section, I show how your compliance strategy can be enhanced with a third-party backup solution.

Expanding the protection scope

Microsoft 365 has come a long way in building intelligence into its compliance and risk management solutions. Artificial intelligence and machine learning capabilities can quickly identify and act on critical insider risks based on data, activities, and behaviors within the Microsoft 365 environment. Therein lies the challenge.

The compliance capability of Microsoft 365 for eDiscovery is limited to Microsoft 365 data only. It also requires a more expensive licensing requirement (E3 or E5) that may be cost prohibitive if you have thousands of employees. Even if you pay for the licenses, you will likely run into a scenario where your legal team is asking for data beyond Microsoft 365, such as data on end points, network drives, and other third-party applications. If your organization uses Microsoft 365 for productivity but uses Salesforce for customer relationship management (CRM) or Slack for collaboration, for example, then you'll have a challenge rounding up the data to be protected. You can upload non-Microsoft 365 for advanced eDiscovery, though it isn't an easy process and you'll need to install a tool.


TIP

Third-party backup solutions can be your answer to enhancing your compliance strategy. Some third-party backup solutions provide comprehensive coverage across various software-as-a-service (SaaS) applications and end points. Some solutions can also help segment the data to be protected and backed up within Microsoft 365 so you can stay within the compliance boundaries when working with mergers and acquisitions.

Delivering data in a litigation

Data collection and data analysis for eDiscovery in Microsoft 365 is not natively integrated with third-party tools. You can bring in a third-party legal matters solution, but that can be costly and complicated to implement.

When you're involved in a legal proceeding, time is of the essence. You build your case with an eye to its defensibility, and usually that requires access to data in a matter of days if not hours or minutes. You'll also need data in a host of file formats that can be ingested into other applications. In Microsoft 365, the file formats you can export are limited.

If this is a scenario for you, then look for third-party backup solutions that allow faster export speeds, multiple file format support, and integration with other eDiscovery tools.

Rounding up data sources in Microsoft 365

Typically, a day in a life of an information worker revolves around checking email, responding to it, filing it, deleting it, and every so often, retrieving files from the Deleted Items folder. If a mailbox has no retention policy applied, items in the Deleted Items folder continue to be available for the end-user. If, however, an end-user permanently deletes an Outlook item, either by deleting it from the Deleted Items folder or pressing Shift+Delete on an Outlook item from any folder, that item is moved to the Recoverable Items folder. The item lives there for 14 days, after which it will be gone forever. An IT administrator can extend this period to 30 days. As the name suggests, items in the Recoverable Items folder can be recovered by the end-user without IT support.

Files stored in SharePoint Online and OneDrive for Business, on the other hand, are protected in multiple layers. When you delete an item in SharePoint Online or OneDrive for Business, the item is moved to the site Recycle Bin, where it is retained for 93 days. During this period, an end-user can retrieve the item from the site Recycle Bin and restore it. After 93 days, the item is unrecoverable.

If you delete an item in the site Recycle Bin, say on Day 30, the item is moved to the site collection Recycle Bin where it will spend the rest of its lifespan — in this case 63 days, before it's completely unrecoverable. During those 63 days, an IT admin or the Site Collection Admin can restore the item to its original location.


TIP

There is a window of 14 days where Microsoft Support may be able to assist you in restoring its backup of your site collection. Be aware that Microsoft's backup replaces the entire site collection rather than just restoring one item or file.

When it comes to Teams, rounding up data for protection can be a little challenging. Here's why.

Files shared in a Teams channel are stored in a document library of the SharePoint Online site associated with the Teams hub. If you share files in a private or group chat, those files are saved in your OneDrive for Business folders.

Chat conversations in Teams are persistent and are retained forever by default. They are saved in a hidden folder in Outlook that can be exposed only by performing an eDiscovery.

If you record a web meeting, the recording is saved in Microsoft Stream. If you have telephone services integrated with Teams, your voicemail data will show up in in your mailbox in Exchange.

Is your head spinning yet? Although the slick user interface of Teams makes this level of complexity transparent to your end-users, be prepared for an increase in support tickets as you drive Teams adoption. You'll likely get requests for help finding or recovering files from those who are confused about where Teams data is stored. Fortunately, you can implement a non-head-spinning data protection strategy using a third-party backup solution.

IN THIS CHAPTER

- Getting on the same page about data loss in the cloud
- Learning about the common ways data is lost
- Formulating a backup and recovery strategy

Chapter 4
Understanding Data Loss in the Cloud

Whether or not you agree that *OK Computer,* the third album by the English rock band Radiohead, released in 1997, deserved its critical acclaim, know that the Library of Congress had already deemed the album "critically, historically, or aesthetically significant" when it was included in the National Recording Registry in 2014.

What can't be undisputed is that Radiohead is the boss when it comes to dealing with data loss. More than 20 years ago, *OK Computer* oozed with a sense of dread about issues at the time, including the dark side of technology. That foreboding became a reality in June 2019 when a hacker stole 18 hours of recordings, which included unreleased content that went into the album. Rather than caving into the hacker's demands for a $150,000 ransom, Radiohead pre-empted the hacker and released all 18 hours of recording and donated the proceeds to address global warming.

IT professionals do not have the luxury legendary rock bands have. I doubt you'd be regarded a hero if you tried to call a hacker's bluff. Although Radiohead's fans may be happy to shell out $23 to hear lead singer Thom Yorke beatboxing, your company likely has content you would not want to see become public at any cost.

Mitigating Data Loss in the Cloud

Data loss is simply the permanent loss of data because of unforeseen circumstances. You can think of it as a huge, hairy support ticket that hasn't been created yet but could end up in your queue at any given moment. The question for you: Are you ready when that moment comes?

In the project management practice, risk management is a knowledge area that focuses on finding ways to minimize the impacts of risks to the project. The most common risk responses that project managers typically have in their risk management plan is to either avoid the risk by eliminating it, transfer the risk (getting insurance is an example), or mitigate the risk by acknowledging that there are certain risks you simply cannot avoid or transfer, so you plan to minimize its impact as much as possible.

REMEMBER

Data loss in the cloud is a risk you cannot eliminate. The burden of mitigating the damage to a company's reputation or preventing a complete work stoppage still falls on the shoulders of IT professionals like you. If you've ever worried your job is going to be taken over by robots, you can relax. You are more valuable today than ever before — at least, until robots can calm down a sales rep who is freaking out because he can't find his Excel file with the details of the biggest deal ever.

Giving end-users peace of mind about data loss

You must strike a balance when fostering a culture of security in your organization. Productivity can be greatly reduced if employees are in constant fear of being hacked. One way to strike that balance is by assuring users that there is life after data loss. Educate them on the self-service data recovery option in Microsoft 365 so you're empowering them to solve their own data loss issues. Let them know that if recovering files is beyond their power, you have their backs.

Did you just distractedly soft-delete an item in Outlook while in a phone call? No problem. Go to the Recoverable Items folder and restore the item yourself. Unhappy with the changes you or your coworker made to a document shared in SharePoint? No need to fret. Simply restore the previous version of the document. Can't

find an email with a critical attachment from two years ago and you need it for your meeting in an hour? No need to panic. Give me the keyword, and I'll run a search-and-restore operation from a third-party backup solution.

The long and short of it is that when you have a working backup and recovery strategy, you can give your users peace of mind about the looming threat of data loss.

Freeing the IT team from mundane tasks

Sure, retention policies can retain files forever, but are you up to speed on all the nuances about retention? If you are, are you allocating time to make sure you know what's new and what's changed? Remember that Microsoft 365 is on a two-week release cycle, so you need to be vigilant about not getting immune to those "Change Update Notification" emails you've automatically dumped into a separate folder via an Outlook rule and forgotten about.


TIP

Be wary of someone who tells you Litigation Hold in the eDiscovery solution is the panacea to all your backup and recovery problems. Most likely, they've never gone through the nightmare of doing the work. Never mind the licensing cost and the data storage limitation; the soul-draining task to restore an email from a single mailbox in Litigation Hold, the bare minimum of which is outlined in a 50-page documentation from the following link, is enough to turn an IT admin's hair gray (if it isn't already).

```
https://docs.microsoft.com/en-us/exchange/
   security-and-compliance/in-place-ediscovery/
   in-place-ediscovery
```


REMEMBER

The good news is, there is a better way. You can free your IT team from the mundane task of restoring lost data by using the right tool for the job. It starts with following the Dataholics Anonymous 12-step program. Step one is to admit Microsoft 365 was not designed to be a backup and recovery solution. Step 2 is to find a third-party backup solution. Step 3 is . . . there *is* no Step 3. Skip everything else and use a third-party tool.

Defining Data Protection Gaps

In Microsoft 365, Microsoft is responsible for ensuring the infrastructure is always up and running. You, on the other hand, are responsible for protecting the data generated and stored in Microsoft 365. You'll face consequences if there is a mismatch on the understanding of who does what. To understand those consequences, consider the following common data protection gaps in Microsoft 365.

Addressing accidental deletions

A customer who writes speeches for politicians came to me frustrated because he couldn't find a beautiful speech he'd written a month earlier and saved in OneDrive. He had assumed the Autosave feature in Microsoft 365 was his insurance and he'd be able to get lost files back with the Files Restore feature. He had spent at least an hour with his IT admin trying to recover the file before going the destructive File Restore route. When that effort failed, they proceeded with the File Restore to a date 30 days prior, knowing that he'd lose the files he'd created after the restore point. In the end, after spending three hours on the effort, they still couldn't find the file. Rather than invest more time, my customer concluded that further troubleshooting was not worth it, so he started from scratch and rewrote the speech.

REMEMBER

The moral of this story is that accidental deletions and user error are a gap in Microsoft 365. Although my customer can recreate his work, no matter how many hours of painstaking work it may have taken, the productivity loss is not desirable.

Accounting for internal and external threats

The headline news about security breaches in the past few years may have led some to believe that cybersecurity threats are mostly coming from hackers. Although it's true that bad actors have inflicted a lot of damage, not just on companies but also on people's personal lives, a data breach report from Verizon shows that 50 percent of security incidents were caused by people inside an organization.

Consider the cautionary tale of the hapless executive admin who works for one of my customers. She got an email from her

traveling CEO to process payment of an overdue invoice so the CEO's credit card wouldn't be blocked during travel. She did as she was asked, as any well-meaning admin would. As it turned out, however, she was a victim of a spoofing attack that resulted in a breach that took six months to recover from. Key data were lost in the process, as well as a few customers who lost confidence in the company's commitment to data security.

REMEMBER

Spoofing and phishing attacks are successful only if a hacker has an unwitting accomplice: your end-user. The frailties of human nature usually pose the weakest link in any security strategy.

Discovering the gaps in retention policies

Threats don't just come from external bad actors. You could also be dealing with a disgruntled employee who purposely deletes or tampers with data on his way out of the door. You might be thinking you've done your job retaining the ex-employee's data through archiving, but all you really have is a false sense of security because data would have already been lost by then.

Maybe you have a salesperson who left the company four months ago to join the competition. When she left, she took with her an Excel file that contains a list of key accounts she developed through your proprietary sales methodology and then deleted the original file. You might think you'd be able to find that list by going through her retained OneDrive folder. Think again. If the file was deleted and the deletion happened more than 93 days ago, then you're out of luck.

That's because when you set a retention policy in a SharePoint Online site collection or a user's OneDrive account, and a user either edits or deletes a file, a copy of that file is created in the Preservation Hold library. When the retention period for that copied file is up, it is then moved to a Recycle Bin (or two, depending on whether you made edits to the file while it was in retention) where you have 93 days to retrieve it. You cannot extend the 93 days so after that grace period, your file is destroyed and utterly unrecoverable.

But wait, there's more. Teams has its own retention policies, too, and they're managed separately. That's because Teams data is stored in multiple places: Exchange, SharePoint, OneDrive, and Azure.

These are clear examples of a gaping hole in Microsoft 365 backup. They also illustrate that retention policies and a backup solution are not one and the same.

Complying with legal and regulatory requirements

In Microsoft 365, you play a critical role in the shared responsibility model when it comes to data. In terms of regulatory compliance, Microsoft plays the role of the data processor while you play the role of the data owner in this model.

As the data processor, Microsoft's focus is on ensuring measures are in place to keep your data private, regulatory controls are implemented to meet requirements, and industry certifications are current.

You, as the data owner on the other hand, are responsible for ensuring that when a compliance requirement states data should be kept forever, then that data is immutable regardless of what the user tries to do with that data. The user can delete the content, or soft-delete, or hard-delete, or even throw the laptop into a river. The data still must exist to meet compliance requirements.

Microsoft 365 has no Backup Center where your IT team can natively take action or configure policies to ensure copies of your organization's data maintain its immutability. This is a gap that you, as the data owner, are responsible for closing.

Managing hybrid Microsoft 365 environments

Digital transformation is a journey. It doesn't happen overnight, so organizations usually implement new technologies in stages to minimize risks and provide the best employee experience. Therefore, it's common to find a hybrid Microsoft 365 environment where an on-premises environment continues to run alongside the cloud. These hybrid scenarios increase the surface area of the data that need protection.

Using native tools like retention policies in Microsoft 365 for backup of cloud data is already challenging. Incorporating on-premises data to that challenging mix brings a whole new level of complexity. In fact, issues have been reported where retention policies applied to on-premises mailboxes were overwritten by the default retention policies in Exchange Online during the migration. You need to address this gap when formulating your backup and recovery strategy.

Developing a Backup and Recovery Strategy

The cost of data loss, the gaps you see in Microsoft 365, and your pride as an IT professional should, at this point, bring you to the conclusion that having a solid backup and recovery strategy is paramount to your organization's survival in today's computing landscape. Here are some ideas to consider when formulating your strategy.

Auditing data sources in your environment

If you're a born-in-the-cloud organization, or have adopted a cloud-only model, then the first order of the day is to figure out what workloads should be included or excluded in the backup: Exchange Online, SharePoint Online, OneDrive for Business, and Teams.

For Exchange Online, think of email, calendar, contacts, tasks, notes, public folders, and shared mailboxes. In SharePoint Online, do you want to back up all your site collections or do you want to focus on certain sites, subsites, lists, or libraries? And yes, you need to ensure *all* versions of a document are backed up!

What do you want backed up in OneDrive for Business? Do you have a governance policy specifying what should be saved in OneDrive? Is it possible that one or two users have uploaded their entire movie collection in OneDrive? This has happened, so it's a legitimate question.

For Teams, think of conversations, calendars, files, notebooks, Planner tasks, and PowerBI dashboards integrated into Teams. Should all of these be backed up?

If you're in a hybrid environment, go through the same exercise and find out whether you should include any dependent data sources in the backup strategy. Do you have a home-grown application that you've integrated into Microsoft 365 that might stop working if an on-premises file server goes down?

Do you back up all of your users' data, or just a subset of users to save on backup licenses? If you went for the latter, then remember that all user data is vulnerable. Your effort to save a few dollars can cost you hundreds of thousands of dollars if missing data becomes a vulnerability.

If you're a seasoned infrastructure professional, put it this way. When you ran Exchange on-premises, did you back up *part* of the Exchange server only, or the entire server? Obviously, the entire server — and if so, that practice shouldn't change in Microsoft 365.

REMEMBER

In Microsoft 365, you don't have access to back-end servers and databases as you do on-premises. To back up data in your cloud environment, third-party vendors use Microsoft APIs. Keep in mind that Microsoft can, and often does, throttle the amount of data that is driven through these APIs, but the best backup vendors have built-in throttle prevention functionality to streamline the backup process.

Outlining recovery requirements

Earlier in this chapter, I tell the story of a speechwriter who had to use File Restore in OneDrive to recover a lost file. He had picked 30 days as the restore point, knowing that anything he created after the restore point would be lost. That decision was an unfortunate concession he had to make because no proper backup and recovery strategy was in place.

If his IT team had a proper backup strategy, a recovery point objective (RPO) would have been set. The RPO refers to the amount of time between backups or the amount of data that can potentially get lost between backups. For example, an RPO of 30 days means a backup is taken every 30 days — not a good RPO. An RPO

of five seconds means a backup is taken every five seconds — a *great* RPO. Most businesses use a one-day RPO for Microsoft 365 because anything shorter than that is caught in Recycle Bins.

Depending on how critical the data is, you may end up with different RPOs based on the data source. It's important to nail the appropriate RPO because it dictates how often you should back up and what the retention period should be for your backup. Although a one-day RPO is generally practiced, it could mean a disaster if you're dealing with high-volume transactional data, especially during peak hours if you can't restore data in the last ten minutes or so.

Which brings me to the next critical requirement in your strategy: The recovery time objective (RTO). RTO is the amount of time you can go without your data before it begins causing major issues. In the example, the speechwriter decided, after three hours of trying to recover the lost data, that he couldn't spend any more time on the effort, so he gave up and recreated the file. His RTO, therefore, is three hours.

When IT professionals set the RTO, they are considering the amount of time it takes to recover from the data loss. For example, how long does it take for an IT admin to find and recover a lost email? It's often quicker to get a cup of coffee than it is to recover data, if it can be recovered at all. If that scenario is not acceptable, then you need a third-party backup and recovery solution for Microsoft 365.


TIP

Be warned that in this example, the backup and recovery strategy failed — so don't think about coming up with a random RTO. The metric must match the threshold by which a business can tolerate losses. I've seen people lose their jobs over RTOs that are not met and recovery strategies that failed.

Making the case for third-party solutions

Certain things in this world are best left to the pros. Now that you know what the data protection gaps are in Microsoft 365, it's time to engage with a third-party backup and recovery solution

to minimize your data loss risks. Any minute you spend trying to fiddle with tools designed for a different purpose to meet your complex backup needs is time you aren't spending making sure your data is safe.


TIP

Several backup solutions in the industry offer cost-effective approaches, so why not take advantage of their time-saving, secure solutions? At the very least, the time you save by not reading 50 pages of documentation from Microsoft on retention policies is time you could spend listening to 18 hours of previously unreleased content from Radiohead.

IN THIS CHAPTER

- Knowing what to look for in a backup solution
- Taking on-premises data to your backup solution
- Developing your backup strategy from a checklist

Chapter 5
Choosing an Microsoft 365 Backup Solution

Microsoft 365 has a robust set of capabilities to protect customer data, but there is no workload, service, or app designated specifically as a complete backup and recovery solution.

If you're serious about backup and recovery in Microsoft 365, you must implement a third-party solution. A research paper from IDC entitled "Why a Backup Strategy for Microsoft 365 is Essential for Security, Compliance, and Business Continuity" makes the same recommendation.

Finding the Provider to Match Your Needs

Entrusting your valuable company data to a third party is like having a trusted daycare for your child. You're responsible for taking your child to the daycare center and while he's there, the daycare center is responsible for his safety.

The difference between a daycare provider and a backup provider is that the backup provider is much more flexible and the options are plenty. At the bare minimum, backup solutions include options for automation so you don't need to do repetitive tasks that take up a lot of time and are prone to errors.

In this section, I cover key considerations for choosing an Microsoft 365 backup provider. The topics are not listed by order of importance because priorities differ from one company to another.

Considering the technical completeness of the solution

The Microsoft 365 backup solution that you choose should address, at the very least, the gaps identified in Chapter 4. The technical completeness of the backup solution determines how successful you will be in implementing a sound backup and recovery strategy. Will the solution back up everything in Microsoft 365, or just a few of the workloads? Is the provider stable enough in the market to assure you that two or three years from now, they'll still be around and continuing to push updates that match the pace of Microsoft 365 improvements?

About 23 admin centers exist in Microsoft 365, some of which are shown in Figure 5-1. The question to ask your backup provider is: "Which of these workloads are covered in your solution?" If it's a challenge to find one backup provider that is 100 percent technically complete, then prioritize what's important to you and pick the solution that will back up the workloads in your risk threshold.

Factoring the ease of implementation

Your IT team will assume the brunt of the work managing the backup solution, keep it in tip-top shape, and be ready to spring into recovery mode whenever the need arises. With a good third-party backup solution, managing and executing backup and recovery can be simple enough for one person to do — even one with little to no experience.

If you have multiple people managing your backup solution, find a backup provider whose solution has a low learning curve. PowerShell scripts are great, but an intuitive user interface with tasks automated as much as possible may save you if, at the critical moment, you have to deploy a junior member of the IT team to perform the recovery.

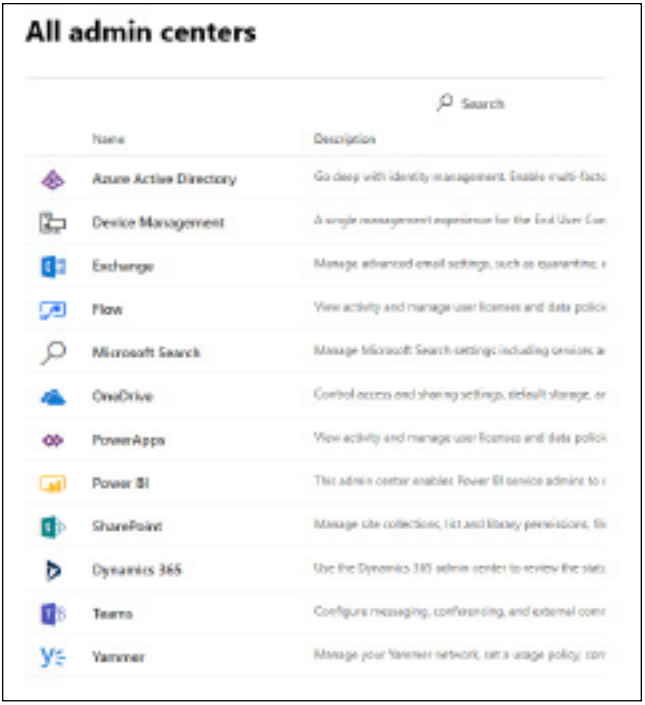

FIGURE 5-1: Microsoft 365 admin centers today.


TIP

A big part of what constitutes ease of implementation is the support you'll get from the provider on a regular basis. Is support part of the package? What are the service-level agreements? Especially on D-Day, which you hope never comes, you'll need to understand the escalation path. It's better to have backup support figured out now, and not need it, than need backup support later and not have it.

Keeping the bottom line in mind

If IT budgets were unlimited, you wouldn't need to justify your vendor selection to those who will approve the expense. The good news is that competition for your business is healthy, so you have a good range of vendors to choose from. For less than the price of a cup of coffee per day, you can cover two or three Microsoft 365 users with a robust backup solution for a whole month.

On the flip side, the bad news is that having so many vendors to choose from can make your decision challenging. If you're considering price alone, the comparison won't be clear-cut. Although most vendors charge on a per-user per-month pricing model, others offer backup as part of a managed services package.

Furthermore, some vendors allow you to bring your own storage, which can reduce the fees, and others allow you to choose the workloads to back up, which then dictate the price.

Don't be tempted to rank your list of vendors based on the cost. Look for the right fit because ultimately, you're looking to calculate your total cost of ownership, not just the monthly fees. If a solution is cheap but requires a highly paid engineer to manage it, then it isn't cheap. Read the fine print. Maybe the per-user per-month license fee is low but there are additional costs for storage and data transfer.

As you consider vendors for a backup solution, don't lose sight of the goal, which is to protect your data and your organization. The "cheaper" solution you pick today may not be cheap at all if you experience a data breach.

If you want to increase the odds of getting approval for a backup budget, you must first properly educate your business decision-makers as to why backup of Microsoft 365 is so important. Use this book to bolster your argument. Once your boss fully understands the notion of shared responsibility in Microsoft 365, you'll have a more receptive audience when you talk about picking a backup solution vendor.


TIP

Most reputable backup providers offer a free 30-day trial. You can also stand up a new Microsoft 365 tenant on a 30-day trial along with your backup trial. At zero cost, you can build a test environment, run some backups, and practice some restores. This is a great way to see how each product performs. This due diligence will pay off for you because only after you've determined the fit of a solution will you be able to calculate the total cost of ownership and compare that with the cost of the status quo.

Purchasing a Backup and Recovery Solution

You've done your homework and you've vetted potential backup solutions. You're now ready to go in front of your leaders to get the budget for a backup solution. In this section, I dive a little deeper into the considerations for picking a vendor so you'll rock your budget meeting. I also tie everything up with a checklist that you can customize or build from as you develop your backup and recovery strategy for Microsoft 365.

To BaaS or not to BaaS?

Backup-as-a-service (BaaS) can reduce the burden on the IT staff because infrastructure is outsourced to a BaaS provider. There are no servers to manage, patch, update, secure, or maintain, which works well for small and medium business (SMB) organizations that have little or no IT staff.

As Oleg Kuperman, Solution Architect for Softchoice Corporation (a recognized Microsoft Azure Expert MSP and BaaS provider), puts it:

SMB customers are not any less susceptible to data loss and malware attacks than large organizations. Unfortunately, most of them don't have the time, energy, or skillset to properly architect and manage a comprehensive disaster recovery, backup, and data lifecycle management infrastructure.

BasS, however, may not be a good option for you if you already have an IT team that can handle the backup process and need shorter service-level agreements (SLAs). If you have compliance concerns related to online backup, then you'll need to do due diligence to determine if BaaS is for you.

Taking control of the backup tool

A few years ago, I founded an IT service provider startup that catered solely to small business customers with fewer than 250 users and nonprofit organizations. I also wanted my company to serve as a training ground for senior high school students who wanted to explore a career path in the IT industry. My first two

employees were tech-savvy Centennials who didn't need much training on the ins and outs of managing the Microsoft 365 admin portal. One of the most striking differences in how these budding IT professionals operate, compared to the 20-year infrastructure veterans I know, was that they preferred the Microsoft 365 admin portal app to the web-based portal. They enjoyed training our customers on the Microsoft 365 web apps and rarely used desktop apps. And — they preferred Snapchat for communication over email.

Baby Boomers, Gen Xers, Millennials, and now Gen Zs or Centennials are the four cultural generations converging in the workplace today. If your company is lucky to have such a diverse workforce, the backup tool and its user interface may be a tie breaker in your selection. Some providers have a purely web-based interface while some have a server you need to install on a physical or virtual machine, or in the cloud on AWS or Azure. If you aren't sure which option is the best for you, take advantage of trial licenses to experience the tool before you commit.

TIP

Web-based tools are great for work on the go. You aren't tethered to your desk to do search and recovery tasks, but these tools often come with some backup and recovery limitations. You can be on vacation in Cabo and still do backup and recovery tasks using your Internet-connected iPad. Or maybe not.

The tools I've seen that require server installation tend to have more robust capabilities than the web-based ones. Some tools like Veeam use the familiar Windows Explorer interface, so the learning curve is low.

REMEMBER

The tool is where stuff happens. Heed the feedback from websites like G2 Crowd, TrustRadius and Gartner Peer Insights on the ease of using the tool because these comments come from IT admins who manage their organization's backup and recovery processes.

Putting what you've learned into action

If you're reading this book, then most likely you understand the importance of protecting data in Microsoft 365 and have a desire to do something about it. I'd like to help turn that desire into action, so I've compiled the salient points in this chapter into a list of factors to consider when choosing a backup provider. This list is by no means exhaustive, so feel free to add to it and delete the points that are not relevant in your scenario.

TIP

If you're reading a pdf version of this book, you may be able to cut and paste the following content into a table in Word or directly into Excel. I suggest adding a column for each vendor you're considering and note what they have to offer against the items on the list.

Consider asking prospective vendors these questions:

- **Data sources.** Will the solution back up the following data sources?
  - Exchange Online: email, calendar, contacts, tasks, notes, public folders, shared mailboxes
  - One Drive for Business: files, photos, albums
  - SharePoint Online: files, folders, libraries, lists, sites, subsites, site collections
  - Microsoft Teams: conversations, calendars, files, notebooks, meeting notes, meeting recordings, voicemail
  - On-Premises data: Exchange, SharePoint
- **Data properties**
  - Will the backup retain the metadata for the items such as date created, date modified, and so on?
  - If the items were shared — for example, as a Word document — will the permissions for the document be retained during the restore process?
  - Will SharePoint sites, lists, and libraries retain their permissions upon restore?
- **About the solution**
  - When can I back up? How often?
  - Is the backup tool web-based, or a server that needs to be installed?
  - Where and how is the tool deployed (if it isn't web-based)?
  - What are the requirements for deploying the tool?
  - What is the architecture of the solution? How is data protected?
  - Where is my data stored? Do I have an option on where (or how — object storage for example) it's stored?

- What is your strategy to address Microsoft 365 throttling?
- What type of retention policy settings or options do I have?
- How fast is data restored?
- Can an end-user do self-service restore?

» About the company

- Will I have 24/7/365 support?
- What are your service-level agreements?
- If we cancel or don't renew our subscription, can we take our data?
- What is the cost? Does it include the storage of the backup data?

IN THIS CHAPTER

- Reinforcing the shared responsibility model
- Closing the gaps in Microsoft 365 backup
- Taking action on what you've learned

Chapter 6
Six Takeaways

The beginning of a security mindset is to acknowledge that there is no such thing as 100 percent security in the cloud. When you operate from that understanding, then your defenses are up and your offense game is on.

The takeaways in this chapter are a quick summary of actions you can take to get started on a path to better data protection in Microsoft 365. They aren't listed in order of priority, so use them as you see fit in your awareness campaigns, budget discussions, and backup vendor conversations.

Microsoft Is Not Responsible for Backup — You Are

A common misconception people have about the value of using Microsoft 365 is that there is no need to back up data because Microsoft does all that work. Chapter 2 clarifies the shared responsibility model and outlines what Microsoft is responsible for versus what you are responsible for.

In a software-as-a-service (SaaS) solution like Microsoft 365, Microsoft is responsible for maintaining the global infrastructure to keep its services running. You, on the other hand, are responsible for maintaining and protecting the data you store in Microsoft 365.

You don't own, nor do you have access to, the replicas Microsoft creates for redundancy purposes. To make copies of your data and store those copies in a separate location, you need to implement a backup and recovery strategy using a third-party solution.

Data Loss Is Costly — Don't Let It Happen to You

When people you talk to start balking at the cost of implementing a third-party backup solution, remind them that a Verizon report suggests that "small" data breaches can cost as much as half a million dollars while "large" data breaches can top at $200 million!

If your business comes to a standstill because of data loss, then you also have to think about the cost of downtime. A study from Information Technology Intelligence Consulting Research concluded that the average cost of a one-hour downtime is $100,000. That's assuming you aren't one of the 33 percent of survey respondents who reported that a one-hour downtime costs them $1–5 million!

Beyond dollars and cents, data loss harms your organization's reputation. It's hard to quantify the monetary impacts of reputation damage, but I'm sure you don't want to find out.

For such high stakes, it doesn't take much to avoid the pitfalls of data loss. There is no shortage of backup solution vendors today, so engage one of them and save yourself a lot of grief.

Microsoft 365 Has Backup Gaps — Close Them

You can't do much about the tendency of human beings to make mistakes, but you can help ensure that when mistakes happen, you'll recover quickly and minimize the harm done.

In Chapter 4, I outline the backup gaps in Microsoft 365, one of which is accidental deletions. More disturbing than human error, however, is the malicious intent of bad actors, internally and

externally, to wreak havoc in your environment. Stolen data is much more insidious than deleted data, so make sure you have controls in place to prevent that from happening.

Understand the purpose of retention policies (Hint: It isn't to make backup copies) so you can address this gap. If you must meet compliance requirements regarding retention, data protection, and data privacy, then that's even more reason to start vetting your backup vendors today.

Last but not least, don't forget data in on-premises environments. That's usually a forgotten data source but may just be as important as data in Microsoft 365.

Compliance Is Real — Take It Seriously

Thompson Reuters, in its 2019 "Cost of Compliance" report, states that there are now more than 1,000 regulatory bodies worldwide that send out more than 200 regulatory updates every day. And you thought the General Data Protection Regulation (GDPR) was too much!

Predictions for the next ten years related to compliance point to continuing regulatory changes and an enhanced role for compliance in business. Undoubtedly, the IT team will play a role in this new normal. So, if you're still fighting the compliance mandate, give it up and fall in line. It is your responsibility as a data owner to govern your company data and ensure they meet compliance requirements.

One of the most anticipated changes in the compliance world is the automation of compliance activities. While that's evolving, there is something you can do today to enhance your compliance strategy: Use a third-party backup solution to protect your data in Microsoft 365. For starters, you can increase the scope of your eDiscovery content without spending a ton of money integrating other eDiscovery tools or ingesting content into Microsoft 365. The way to do that is to leverage third-party backup tools.

Bad Actors Want to Enlist Your End-Users — Don't Let Them

Pixel-perfect fake login screens, socially-engineered phishing emails, and malicious links embedded in an innocent document or email are just a few of the tricks hackers use to get your end-users to give up their credentials and compromise your environment. Guess what? That isn't going to stop. What that means, then, is that the effort to build a culture of security and ongoing awareness campaigns need not stop either. Phishing and spoofing campaigns are successful only if end-users fall for them, so help your end-users not play a part in breaching your environment. Remember, even IT professionals fall for these scams. No one is immune.

There Is No Shortage of Backup Solutions — Pick One Today!

You've invested the time to read this book; now it's time to make that investment pay for you. Don't put it off for another day. Instead, get started on your backup and recovery for Microsoft 365 initiative today. There is no shortage of backup vendors eager to help you out. You can even use 30-day trial licenses if you want to test and compare. Every minute you wait to back up your data is a minute you leave open for disaster to strike.

If you suffer from "analysis paralysis" from having to deal with too much information, too many vendors, and too many options, then you can narrow your options by using services such as G2 Crowd (`www.g2.com`), Trust Radius (`www.trustradius.com`), and Gartner Peer Insights (`www.gartner.com/en/products/peer-insights`) to find reviews on backup providers.

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
30-day FREE trial!

Drive productivity while protecting your data

The role IT professionals play in a landscape where data loss, security breaches, and invasion of privacy are the new normal has never been more critical. This book addresses the data security challenges in today's computing landscape by outlining the out-of-the-box security features in Microsoft 365 and uncovering the gaps that require action to achieve an effective backup and recovery strategy.

Inside...

- Plan your Microsoft 365 migration
- Understand shared data responsiblity
- Explore data loss prevention policies
- Enhance compliance
- Mitigage data loss in the cloud
- Identify data protection gaps
- Develop a backup and recovery strategy

VEEAM

Jennifer Reed is a technology business leader who helps businesses achieve their goals by developing innovative solutions using the latest cloud technologies. She is the author of *Microsoft 365 Business for Admins For Dummies* and co-author of *Microsoft 365 For Dummies*.

ISBN 978-1-119-89536-7
90000
9 781119 895367

WILEY END USER LICENSE AGREEMENT

Go to www.wiley.com/go/eula to access Wiley’s ebook EULA.