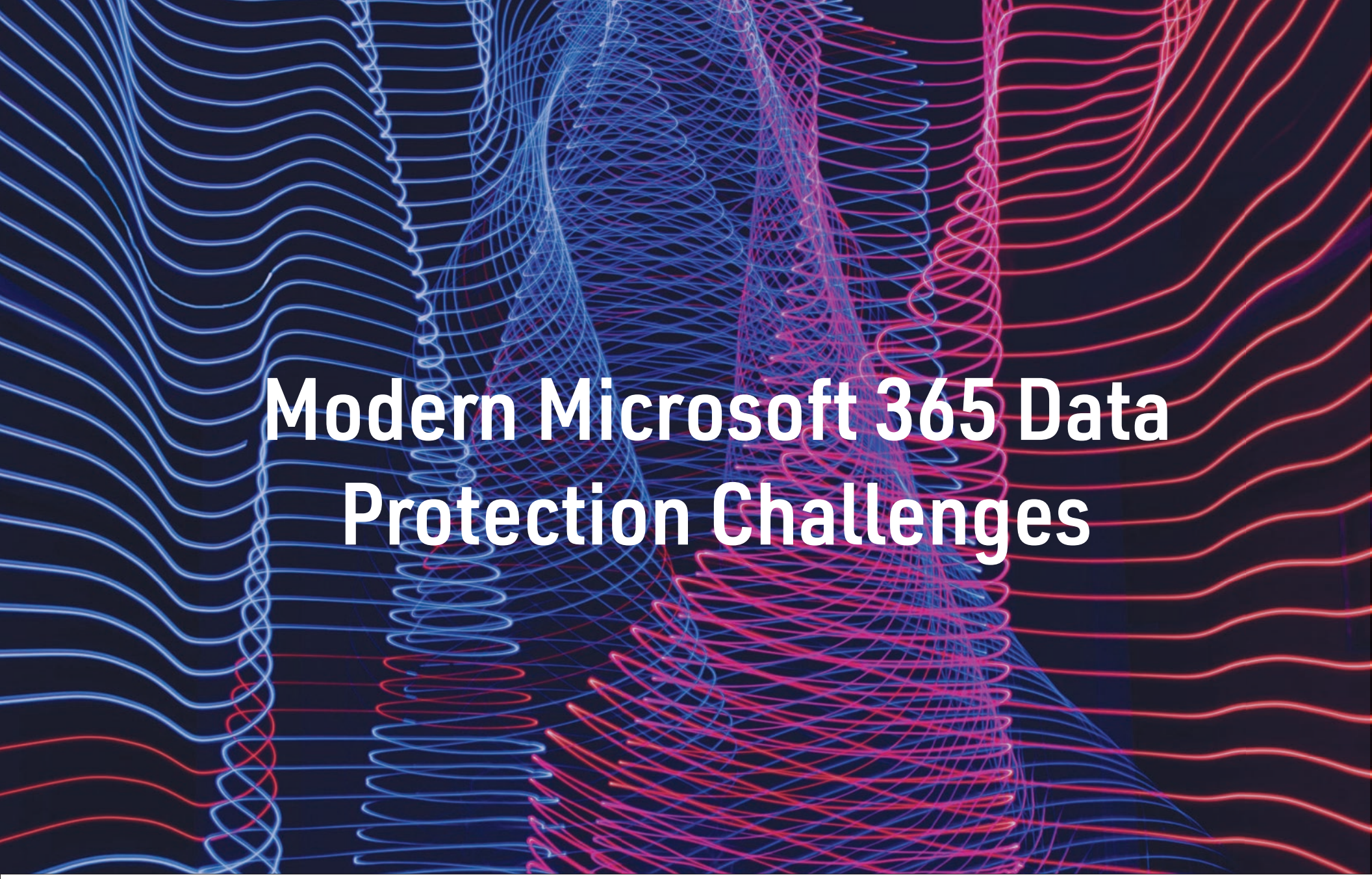


Modern Microsoft 365 Data Protection Challenges

CyberFortress™
The Recovery People

cyberfortress.com
855-223-9322
sales@cyberfortress.com

Table of Contents

Chapter 1:

The Modern Risk of Maintaining Data in Microsoft 365

For most organizations today, the phrase we run of Microsoft 365 is a given. With over 200 million active users and current shifts in business moving to a completely remote workforce, we're seeing a dramatic increase in the usage of Microsoft 365. Case in point, in response to the COVID-19 pandemic, Microsoft's promotional free use of E1 Microsoft 365 licenses caused Microsoft Teams alone to go from 32 million daily active users to over 44 million in just under a week.

For some organizations, Microsoft 365 was one of many cloud-based solutions used to keep operations moving. But in the new era of emote workforces and digital workspaces, the reliance upon Microsoft 365 make the business work at its peak. This makes Microsoft 365 the central repository for much of your organizations critical communications, files, and business processes.

It's important to see Microsoft 365 your new working environment. And, as with any working environment, there is the potential for risk to the business. Even in a completely on-premises network, organizations face risks related to the productivity, security and compliance of the business. Even though you're using a service in the cloud, the same potential risks exist.

In this chapter, we'll provide a high-level outline of the risks associated with maintaining data within Microsoft 365. In the subsequent chapters, we'll dive into each of the types of risks, providing guidance on how to mitigate the risk and protect your data residing in Microsoft 365. To better understand the risk, let's first define exactly what kind of data you have residing inside Microsoft 365.

Microsoft 365 Data Protection Experts: CyberFortress and Veeam

With your most valuable data residing within Microsoft 365, it's important to be ble to recover it wither for disaster, a migration, or eDiscovery. CyberFortress and Veeam together provide organizations with managed backup and recovery of Microsoft 365 data to ensure an ability to recover your data with minimal intervention by internal IT. Look for insights from CyberFortress and Veeam throughout this eBook!

So, what's the risk to an organization when your data is in Microsoft 365?

	Intellectual Property	Financial Data	Personally Identifiable Information	Customer Data	Business-Sensitive Data
Exchange	✓	✓	✓	✓	✓
SharePoint	✓	✓	✓	✓	✓
OneDrive	✓	✓	✓	✓	✓
Teams	✓	✓	✓	✓	✓

What Are You Storing Inside Microsoft 365?

While each organization may use Microsoft 365 a little differently, there are some common use cases that spell out what kinds of operational data can be found in Microsoft 365. The easiest way to demonstrate this is to breakout the various services and the kinds data the can reside within each using the table above.

While the table above appears a bit ridiculous at first, it's there to make the point that data deemed critical, sensitive, proprietary, a n otherwise of value can be anywhere within Microsoft 365. If you walk through each data type and Microsoft 365 service combination, it's pretty easy to come up with a use case scenario.

Because important data will exist inside Microsoft 365 in some manifestation, it's important to understand the risk to the to this data so you can develop a proper data protection plan to mitigate them.

Because the organization relies upon their data being available, unaltered, and current inside of Microsoft 365, several threats exist tha can have a significant impact on your organization. These include:

Cyberthreats - The deletion, modification, or encryption of data within Microsoft 365 is an often-used tactic as part of a larger attack campaign. Additionally, misused access to services is often used to separate malware.

Operational Threats - Anything from accidental deletion to intentional malicious activity by internal actors, as well as simple data corruption within Microsoft's servers remain a possibility today.

Business Evolution - As the organization grows, mergers and acquisitions can have an impact on data retention, the need to mitigate tenants, or even move the organization out of Microsoftr 365.

In all of these cases, the result of these threats can be slowing down or halt in operations that result in a material strain on an organization's productivity and profitability. So, what kinds of data can you back up from within Microsoft 365?

What's Able to be Backed Up in Microsoft 365?

Microsoft has gone to great lengths to make data accessible to backup providers. Below is a list of each service and some detail around the types of data that can be backed up:

Exchange Online - Mailboxes of every kind (user mailboxes, shared mailboxes, Microsoft 365 group mailboxes, resource mailboxes and SharePoint site mailboxes), as well as public folders including both folder structures and items.

SharePoint Online - Site collections, sites, list, and libraries (along with associated content and permissions) can all be backed up. Depending on the solution used, recovery can be down to a single item.

OneDrive for Business - All user-owned data is included in backups. Granularity can be achieved down to the file level, if needed.

Microsoft Teams - Chats, files and sites are all included in backups.

Insights: Protecting Hybrid Exchange/ Microsoft 365 Environments

CyberFortress leverages Veeam Software for its Cloud to Cloud Microsoft 365 Backup to protect data that Microsoft does not.

Why Do Organizations Need to be Thinking About Backups?

Because you have Microsoft doing all the hosting, organizations can fall into a false sense of security the information stored within Microsoft 365 is being protected. But there are a few small simple reasons why you need to be thinking about backing up and protecting data used within Microsoft 365.

It's Your Data

Microsoft own service agreement for its various services - including all of Microsoft 365 - takes the time to define how the data (referred to as content) used by your organization within Microsoft 365 is, well... yours.

From the Microsoft Services Agreement

> The Privacy Statement also describes how Microsoft uses your content, which is your communication with others: postings submitted by your to Microsoft via the Services: and the files, photos, documents, audio, digital works, livestreams and videos that you upload, store, broadcast or share through the Services ("Your Content")

It's Also Your Responsibility

If just telling you that the data is yours isn't enough to make you draw the logical conclusion "maybe we should do something about kit" Microsoft makes it crystal clear that they aren't responsible for your data. Again, from the Microsoft Services Agreement:

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

Additionally, Microsoft warns about the possibility of data loss and how organizations should proactivity address the issue:

> We strive to keep the Services up and running; however, all online services suffer occasional disruptions and outages, and Microsoft is not liable for any disruption or loss you may suffer as a result. In the event of an outage, you may not be able to retrieve our Content or Data that you're stored. We recommend that you regularly backup Your Content and Data that you store on the Services or store using Third-Party Apps and Services

In short, Microsoft isn't in the business of protecting your data - it's yours and you need to back it up.,

Insights: The Shared Responsibility Model

The concept of a Shared Responsibility model for cloud services has been around for a number of years. Even so, many organizations are unclear as to where the proverbial dividing line exists between what Microsoft and the organization each are responsible for.

According to the Shared Responsibility model, the organization needs to address the data protection needs of any data residing with Microsoft 365. Additionally, Microsoft is not responsible for data-level security and compliance, including permission assignments, delegation, monitoring, remediation, auditing, and – again – backups; the organization is.

In the next chapter, we'll dive in a bit deeper and look at the current state of cyberthreats faced by Microsoft 365 and provide guidance on how to best protect your data.

Download: Protecting Microsoft 365 Data Checklist

Without Data Protection, Microsoft 365 Becomes a Business Risk

According to Gartner, by 2022, 75% of organizations utilizing some form of outsourced email and collaboration solution (which includes Microsoft 365) won't be able to meet their recovery needs should there be an outage. This prediction speaks to how organizations think so casually about their data in the cloud.

Storing vast amounts of critical data in Microsoft 365 and doing nothing about it creates a massive risk to the organization's productivity, profitability, and reputation. Use of Microsoft 365 demands that organizations pay close attention to the risks that exist and the business impact those risks would exact should they come to fruition. It's critical that organizations do something about this risk by seeking to employ backups for their Microsoft 365 data, so that backups become a natural part of the business evolution (which includes the increased use of Microsoft 365) that is occurring today and in the future.

Ready to figure out what backups of your Microsoft 365 data are necessary?

Chapter 2:

Modern Cyberthreats to Microsoft 365 Data

Cybercriminals today are looking for one of two things: either a) data they can immediately turn into money or b) access that will eventually get them to the data that can make them money. For example, in the case of ransomware, the goal is to hold as much of an organization's data for ransom as is possible to ensure an ability to collect the ransom. So, simply infecting a single machine likely won't do it. Cybercriminals will instead leverage known vulnerabilities to intentionally access additional machines to spread the infection far and wide and then encrypt everything they can. See? Data and access.

Microsoft 365 provides cybercriminals with an opportunity to reach both.

In this chapter, we'll look at several types of cyberthreats that are in use today, providing insight into how this impacts your data. We'll also offer guidance around how to best backup this data to ensure an ability to recover impacted parts of Microsoft 365 to a "known-secure" state.

How Cyberthreats Emanate in Microsoft 365

Sticking with "data and access" as cyberthreat goals, there are a number of ways we see Microsoft 365 data sitting firmly in the crossfire of attacks. In some cases, the data accessible to a compromised account inside a user's mailbox, SharePoint site, or OneDrive is enough for the cybercriminal. In other cases, it's the account itself that is the valuable asset – being able to send emails as someone within the company from a valid email address can help to get past security safeguards, establish credibility with the user, and convince them to open the attachment, click the link, or take the desired action that helps the attacker.

After an attack, Microsoft 365 is left with a number of data repercussions, that include:

Manipulated Data – From newsworthy "data held for ransom" to an attacker simply hiding their tracks, everything from email communications, to team chats, to files can fall into a modified state of unknown that includes malicious activity.

Sent/Received Email – In many cases, messages are sent and received by a threat actor impersonating the compromised user. And in many cases, these same messages are deleted post conversation.

Created OneDrive/SharePoint files – Both of these solutions offer the ability to share documents with users inside and outside the organization. That makes them a perfect repository to store malicious payloads, script files, etc.

Modified Credentials and Security – While outside the scope of this eBook, it's important to be thorough here. Attackers will try to gain elevated access to create Microsoft 365 accounts, modify security settings, permissions, and more – all in an effort to gain control and establish persistence within your Microsoft 365 instance.

So, what are some of the specific attacks that yield this insecure and unknown state of your Microsoft 365 data?

Insights: Cyberthreats Can Impact All Of Microsoft 365

In the data affected by a cyberattack may exists in the repositories of multiple services. So, backups need to extend well beyond just protecting Exchange mailboxes and look to protect every bit of accessible data that can be backed up.

CyberFortress' Cloud to Cloud Microsoft 365 Backup, Powered by Veeam allows for the granular protection of data all the way down to the message, chat, file, site, and list. Whether recovery encompasses the organization or a single user, an entire mailbox or a single message, CyberFortress powered by Veeam is able to ensure the protection and recoverability of your data.

Credential Attacks

In this attack, the goal is to trick the victim to give up their Microsoft 365 credentials – usually using little more than a simple phishing attack. Cybercriminals use various scam to convince users they need to log onto Microsoft 365 – fake invoices, important emails held up as spam that need to be "released", and even Microsoft 365 security alerts sent to administrators. In every case, some sense of urgency is created in the hopes the user will want to act.

The credential theft is accomplished using a very convincing lookalike logon page (shown at right. Other than the URL being incorrect, but good enough to pass a cursory check, this page looks authentic.

With a valid set of Microsoft 365 credentials, cybercriminals often use the compromised access to send malware-laden emails to additional victims, steal data, leverage SharePoint Online and/or OneDrive to host malicious files, and more.

OAuth Attacks

Similar in intent as stealing credentials, this attack instead uses OAuth application access to Microsoft 365. OAuth is the web-based authentication protocol that can be used between platforms and applications to grant access. The difference in this attack is in the persistence established. With credential attacks, once the credential password is reset, the cybercriminal loses access. But with application access via OAuth, a malicious web application is given access to the user's Microsoft 365 account.

The attack again begins with a phishing scam. In one example, the email presents itself as a Microsoft Online Protection update, asking the user to update their spam protection. When the victim performs the "update," a permission request (shown at right) is presented, asking for access to the user's mailbox and data.

Notorious hacker Kevin Mitnick performed a great demonstration of how application-level access to an Microsoft 365 mailbox is used as part of a ransomware attack, in what he dubbed "ransomcloud." In his demonstration, he uses this method to gain access to a mailbox and then automatically encrypted each message in the victim's mailbox, leaving a note to pay the ransom to decrypt the mailbox.

Man-in-the-Middle Attacks

Access to an Microsoft 365 mailbox can be used to facilitate a "manin-the-middle" attack, where the cybercriminal monitors email communications and uses scripting to send, forward, and delete messages in a user's inbox.

One recent example of this happened to an Israeli tech startup that was about to get their VC funding. The startup's email was compromised and the attacker monitored email communications with the VC. The "man-in-the-middle" was achieved through a few steps. First, all emails coming in from the VC were automatically forwarded to an outside account, and the relevant received and sent emails being promptly deleted. Second, lookalike domains were created for both the startup and the VC, where the cybercriminal controlled the conversation, tricking the VC to send the money to an attacker-controlled bank account, while simultaneously convincing the startup that things were taking longer than expected.

Business Email Compromise / Impersonation Attacks

Many cybercriminals target an individual within one company to become an asset in a larger attack against a second company. Using spear phishing to gain access to a mailbox in the initially targeted company, attackers can email suppliers, vendors, partners, or customers with intent to commit fraud (usually in the form of convincing the victim to change banking details on a pending payment to an attacker-controlled bank account).

The fact that an email is coming from, say, the Accounts Receivable person, helps to establish credibility to the fraud victim. Another type of attack where impersonation helps is island hopping – where an email is sent to recipients at one or many companies with a malicious link or attachment included. The intent is to gain access in one or more of the companies and "hop" from the initial company to the next one.

OneDrive / SharePoint as a Malware Repository

Security solutions monitoring email will often flag attachments coming from unknown domains. So, cybercriminals will leverage valid OneDrive and SharePoint instances to "convince" email scanning solutions that malicious links in email are actually benign in nature and, therefore, are allowed for victim users to click. Using either credential or OAuth attacks, cybercriminals take full advantage of the compromised user's access to sharable cloud storage to place malicious documents. Additionally, in cases of island hopping, having access to a user's mailbox and sharable file storage is a helpful plus to an attacker.

Insights: Designing Backups To Address Cyberthreats

It's not enough to simply create backups of your Microsoft 365 data. To protect against cyberthreats, it's necessary to identify roles within the organization that are commonly targeted by cybercriminals and build a backup strategy that allows you to recover any and all data – across Exchange Online, SharePoint Online, Teams, and OneDrive – that may be impacted.

CyberFortresss's Cloud to Cloud Microsoft 365 Protection, Powered by Veeam allows for multiple backup jobs to be created to ensure recoverability from an RTO s tandpoint, as well as with the needed user and resource granularity to get the business operational again.

Protecting Your Microsoft 365 Data from Cyberthreats

Because of the modern prevalence of remote use of Microsoft 365, the potential for cyberattacks intent on gaining access to mailboxes, OneDrive, SharePoint and Teams, it's imperative for organizations to backup your Microsoft 365 data. Cybercriminals leverage any and all accessible services, leaving them modified and in question of being operationally sound.

By backing up your Microsoft 365 data, you provide your organization with the ability to easily recover from cyberthreats by returning the impacted data back to before the attack, representing a known-good and known-secure state.

In the next chapter, we'll look at the operational changes that pose a threat to your Microsoft 365 data and provide guidance on how to best protect your data.

Are You Ready and Protected From a Microsoft 365 Cyberthreat? Take This Quiz to Find Out.

Chapter 3:

Operational Threats to Microsoft 365 Data

While so much emphasis is placed on external cyberthreats (and with good reason), another threat to your Microsoft 365 looms inside the organization; your users. In many cases, we're talking about threats that are far less sinister and often far more mundane, with the possibility of a truly malicious insider still alive and well.

In the previous chapter, we looked at scenarios where an external threat actor gained access to an Microsoft 365 account, using it to further their malicious activities. In this chapter, we're going to switch focus and look inward at some of the situations that can easily arise where data you thought you still had is no longer available. We'll also look at why this happens, and why relying on native retention controls suffices.

How Operational Threats Emanate in Microsoft 365

When looking strictly at those activities performed by your users and how they threaten your Microsoft 365 data, it can be easily boiled down to the scenario where needed data no longer exists. This is the result of two basic actions:

Deletions – Whether accidental, negligent, or malicious, the deletion of attachments, messages, files, folders, lists, libraries, and more can have adverse effects.

Overwrites – Every one of us has at least once accidentally saved one file over another. Having the same effect as a deletion, but with a painful reminder in the form of the newly created (and grossly misnamed) saved file.

In order to negate these issues, Microsoft 365 does offer a few native bits of functionality designed to help an organization in these cases:

Deleted Item Retention - Exchange Online, SharePoint Online, and OneDrive all have a specified period of time in which deleted items are held onto and are "recoverable." The following table outlines the default and maximum configurable values for each.

Versioning - As documents are modified, both SharePoint Online and OneDrive support retaining 100 major versions of each document by default.

Recovery - OneDrive for Business does support users restoring their files and folders within a 30-day timeframe. This can include a user's entire OneDrive or individual files.

Archives - Exchange Online offers the capability to archive mailbox data for long-term storage and retrieval.

	Default DIRT	Max. DIRT	Microsoft Backups	Deleted User Data Retention
Exchange	✓	✓	✓	✓
SharePoint	✓	✓	✓	✓
OneDrive	✓	✓	✓	✓
Teams	✓	✓	✓	✓

Insights: Sometimes Recovery Isn't Fast Enough

The way Microsoft facilitates recovery in OneDrive is a step in the right direction. However, that same functionality is needed across all four of Microsoft 365's most-used services. CyberFortress' Cloud to Cloud Microsoft 365 Protection, powered by Veeam provides your organization recovery options assisting with recovery of data found in Exchange Online, SharePoint Online, OneDrive for Business, and Teams, with an ability to recover back into your Microsoft 365 tenant, another tenant, and even allow for one-off recovery of items using CyberFortress' services portal.

A Mix of People and Overreliance on Technology

As you can see, in addition to the user actions that are the initial cause of the problem, the other half of the "operation threat" equation revolves around which service is being used to host the data in question and whether the timeframe between deletion/overwrite and the realization of the need to recover exceeds a designated retention or recovery time.

So, what kinds of other operational threats still put your Microsoft 365 data at risk? Looking beyond deletions and overwrites, there are several other Microsoft 365 operational threats impacting your data that should be of concern. These include:

Insider Threats – Organizations are typically concerned about malicious insiders with regard to data theft. But situations do exist where an employee or contractor uses their access to maliciously delete and/or manipulate data they have access to. In cases where the malicious insider is an administrator, there are several actions they could take that would be harmful to your data over time.

- **Disabling version history** – Some business operations rely on the ability to go back to earlier versions. Should an admin either disable or significantly limit versioning, it could impair productivity.

- **Emptying a recycle bin** – in the case of SharePoint Online, OneDrive and Teams, emptying the Site Collection Recycle Bin permanently deletes items. The 14-day period in which Microsoft has backups could be a saving grace… that is, if you realize the malicious act in time.

Gaps in Retention Policies – As implied in the previous table, some data can be retained for much longer periods of time to meet both legal and regulatory requirements. But retention policies need to first define which data needs to be retained and for how long. It's plausible to conceive of a scenario where some of your data fails to be included within the policy definitions.

Deleting a User – When users are deleted, a fair portion of their data is put on the chopping block. In general, Microsoft offers 30 days of retention before the data is permanently deleted.

Insight: Retention and Archives Aren't Backups

Microsoft has put a lot of effort into giving both users and administrators an ability to "recover" deleted items over some pretty respectable amounts of time. But these capabilities are more safety nets in cases where something is mistakenly deleted. And, while archiving does offer long-term access to old email, it's not meant to be a backup. So, it's important to note that none of the methods mentioned in this chapter are true data protection strategies. CyberFortress's Cloud to Cloud Microsoft 365 Protection, Powered by Veeam ensures that your organization's data retention needs are met from operational, legal, and regulatory perspectives.

Mitigating Microsoft 365 Operational Threats

The operational threat is simple: data is modified or deleted, and when you realize you need it, you can't get it back. Microsoft has taken steps to mitigate this issue in the short-term. But a longer-term strategy is needed to address recovery needs next month, next quarter, next year, and in years to come.

In the next and final chapter of this eBook, we'll look at business challenges that occur as the organization evolves over time that may impact your Microsoft 365 data.

Is Your Organization Ready For an Operational Threat to Your Microsoft 365 Data? Take This Quiz to Find Out.

Chapter 4:

Business Challenges and Microsoft 365 Data

The one thing IT knows all-too well is that the organization is constantly evolving. From market positioning, to go-to-market strategies, to products and services offered, to locations served, IT is expected to architect technology solutions that allow the ever-changing face of the company to not just grow, but thrive. And as these changes take place, there is the possibility that the way Microsoft 365 currently meets the organization's needs may not a year from now.

In this chapter, we'll cover a few high-level strategic business challenges that may impact your Microsoft 365 implementation and, therefore, your data. As you'll see, the threat to Microsoft 365 here is indirect in nature, in that Microsoft 365 is an innocent bystander to the business changing. But even so, there's an impact where having a backup of your Microsoft 365 data may put IT in a much stronger position to adapt to the changing needs of the business and deliver a solution.

So, what are some of the business challenges that are cause for concern for your Microsoft 365 data?

Mergers and Acquisitions

Nearly two-thirds (63%) of organizations expect to see M&A deal activity increase over the next 12 months while three-quarters (75%) expect to pursue divestitures . This interest in evolving the business is a natural tendency to ensure competitiveness on a national and global scale.

The result for IT, though, is a decentralized set of Microsoft 365 tenants each running as separate logical organizations. So, remember all those cyber and operational threats? Multiply them by the number of "quasi-rogue" organizations you have that now make up your company post-merger or acquisition.

Given you're reading this eBook, it's safe to assume that you buy into the idea of needing to backup Microsoft 365 to some degree. But that doesn't mean those managing all the other Microsoft 365 tenants in existence within your organization do as well.

Until there's some form of consolidation of tenants, you need to be backing up each one.

In the immediate timeframe, backups are needed to protect against data loss (whether caused by Microsoft or your users) and help to remediate cyberthreats. In the long run, the goal is to have backups that may be used to either assist with migration (in the case of recovering back to on-premises or to a private cloud) or facilitate reverting back to Microsoft 365 should a migration fail.

Avoiding Vendor Lock-In

Despite Microsoft being one of the most trusted vendors to provide cloud-based collaboration and communication via Microsoft 365, there is the possibility that one day the organization may feel that either Microsoft 365 – or any cloud service for that matter – no longer aligns with the corporate strategy.

Currently Microsoft provides no toolset to help organizations leave Microsoft 365 (and why would they?). But in circumstances where an exit is necessary – perhaps as part of an acquisition or merger where another service is the de facto standard, or where an on-premises solution is mandated – having a copy of your data may be needed to facilitate a migration.

New Compliance Regulations

We're seeing a number of new regulations come out across the world, partially in response to the EU's General Data Protection Rule (GDPR). It opened the door for location- and industry-specific laws to be made to protect personally identifiable information (PII). A great example of a post-GDPR law coming into effect is the California Consumer Privacy Act (CCPA). In it (and in GDPR) is a mandate for organizations to respond to requests in a timely manner. So, what happens if those requests go to a mailbox that befalls any of the issues outlined in this eBook (is encrypted with ransomware, has contents maliciously deleted, or becomes corrupted)? There needs to be a means for organizations to recover that data quickly, so the requests can be processed in an appropriate timeframe.

We should be expecting to see additional laws popping up over time as more industries and local governments look to protect PII from misuse. And with each one, ensuring the ability to recover, as well as retain data (as is required) should be a focus for your Microsoft 365 backup strategy..

Insight: Choosing a Partner Experienced In The Cloud

There are lots of reasons why data could need to be recovered outside of Microsoft 365. The "we use another platform" scenario is valid. Recovery could also just as easily be a part of eDiscovery or a public records request. Because of the myriad of reasons and the equal abundance of recovery target choices, it's important to choose a managed backup partner with the expertise to address and/or assist with any kind of recovery request.

CyberFortress's 20+ years in backup and recovery married with Veeam's 14 years in the cloud backup space provides organizations with the experience necessary to see any backup and recovery of Microsoft 365 data to success.

Avoiding Vendor Lock-In

Despite Microsoft being one of the most trusted vendors to provide cloud-based collaboration and communication via Microsoft 365, there is the possibility that one day the organization may feel that either Microsoft 365 – or any cloud service for that matter – no longer aligns with the corporate strategy.

Currently Microsoft provides no toolset to help organizations leave Microsoft 365 (and why would they?). But in circumstances where an exit is necessary – perhaps as part of an acquisition or merger where another service is the de facto standard, or where an on premises solution is mandated – having a copy of your data may be needed to facilitate a migration.

New Compliance Regulations

We're seeing a number of new regulations come out across the world, partially in response to the EU's General Data Protection Rule (GDPR). It opened the door for location- and industry-specific laws to be made to protect personally identifiable information (PII). A great example of a post-GDPR law coming into effect is the California Consumer Privacy Act (CCPA). In it (and in GDPR) is a mandate for organizations to respond to requests in a timely manner. So, what happens if those requests go to a mailbox that befalls any of the issues outlined in this eBook (is encrypted with ransomware, has contents maliciously deleted, or becomes corrupted)? There needs to be a means for organizations to recover that data quickly, so the requests can be processed in an appropriate timeframe.

New Compliance Regulations (Continued)

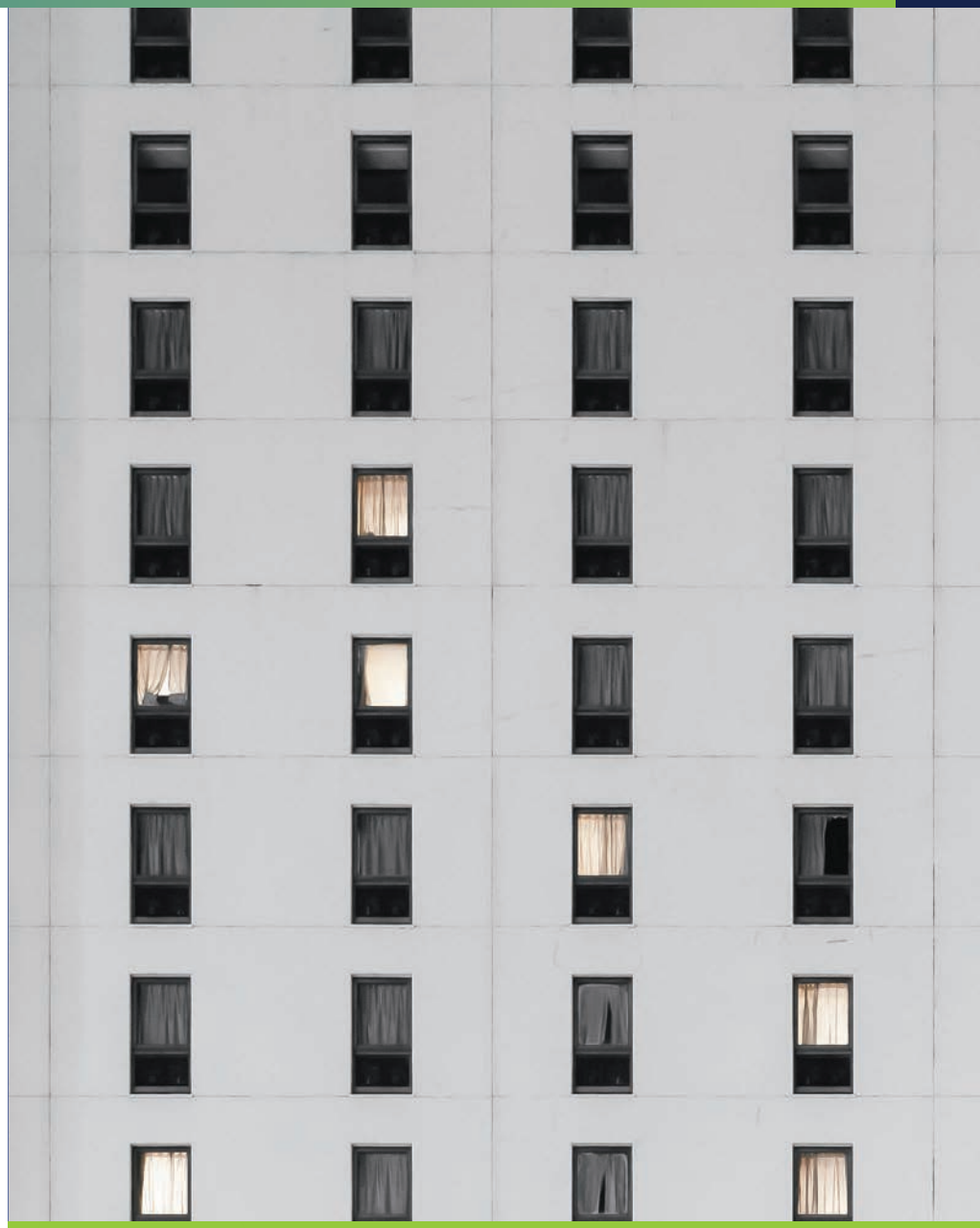
We should be expecting to see additional laws popping up over time as more industries and local governments look to protect PII from misuse. And with each one, ensuring the ability to recover, as well as retain data (as is required) should be a focus for your Microsoft 365 backup strategy.

Keeping Backups in Line with Business Changes

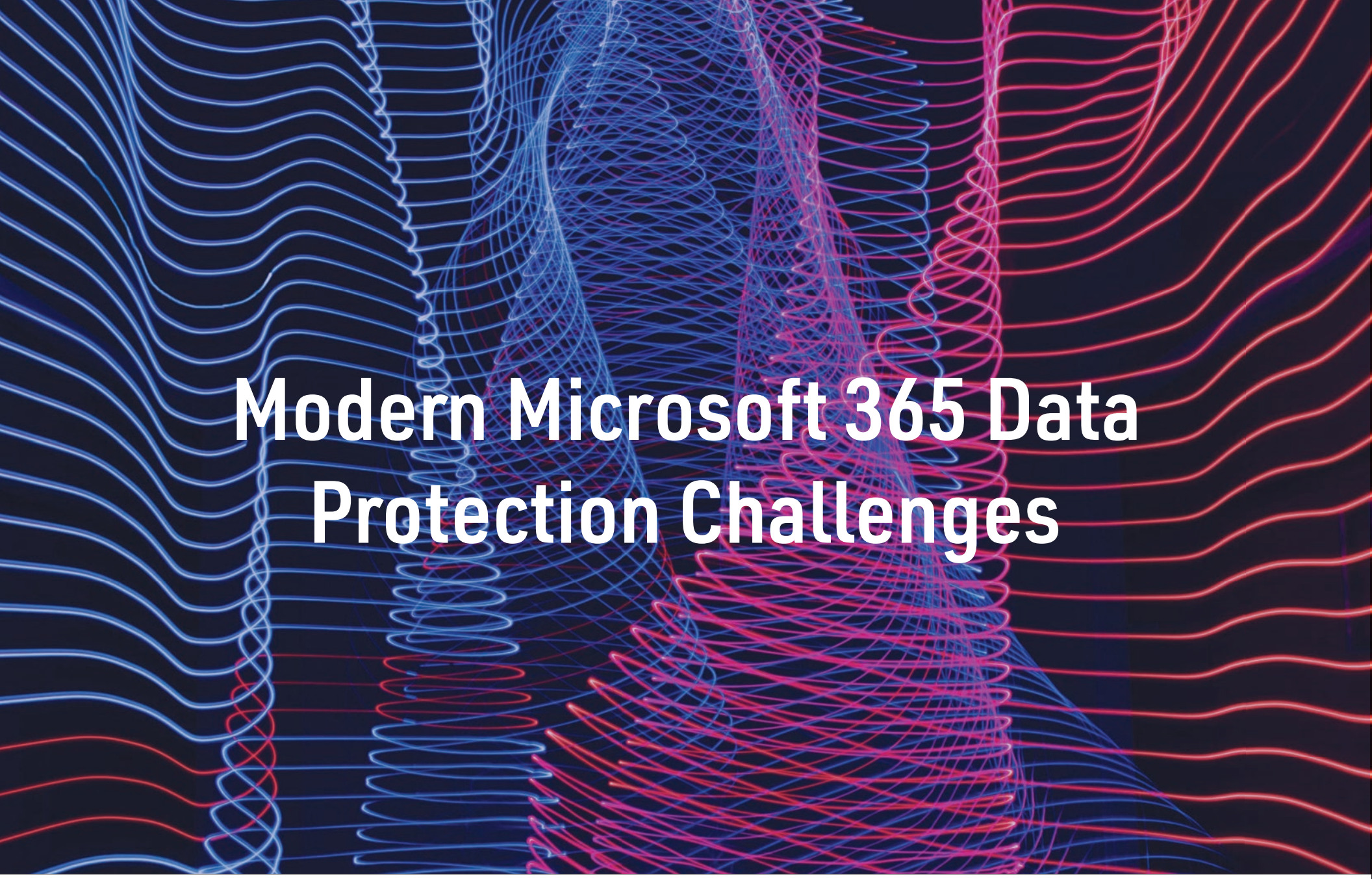
As the organization changes focus, the recoverability of that new iteration of the organization is critical. The dependence on Microsoft 365 as a central means for communicating, collaborating, and sharing puts the data residing in this service clearly in the center of your backup and recovery strategy.

The key here is planning ahead. Asked to perform diligence on a potential acquisition? Include backups of Microsoft 365 as a discussion point. Hearing about a new pending law that may impact your organization? Consider whether protected data or processes involving that data reside within Microsoft 365.

No matter what the change, the backup planning basics remain the same: if it's critical, back it up. The details about how often, for whom, where will it be recovered to, etc. all need to be sorted out as well – but the first step is to buy into the fact that Microsoft 365 needs to be backed up..



Download: Use This Identifying Microsoft 365 Business Requirements Worksheet to Make a Backup Frequency Plan.



Modern Microsoft 365 Data Protection Challenges

CyberFortress™
The Recovery People

cyberfortress.com
855-223-9322
sales@cyberfortress.com