Osterman Research

WHITE PAPER

White Paper by Osterman Research
Published **March 2020**
Sponsored by **MailStore**

The Benefits of Third-Party Email Archiving for Businesses Using Microsoft 365

Executive Summary

Despite the increasing use of solutions like Microsoft Teams and Slack, email continues to be the primary method that most users employ for sending and receiving documents and for collaboration with others. Email contains a wealth of critical information and this information must be protected through robust email backup and archiving capabilities so that businesses and users have ready access to this data at all times.

Even though a growing number of businesses are moving to Microsoft 365, they will continue to need employ best practices for email backup and archiving to protect, preserve and keep available their corporate data – backup and archiving don't just happen automatically in Microsoft 365. Moreover, email backup and archiving capabilities must accommodate scenarios that Microsoft 365 does not handle as well as some third-party solutions, such as hybrid environments and those that include non-Microsoft data.

This white paper discusses why small and mid-sized businesses (SMBs) should deploy an email archiving solution, and why they should consider the use of a third-party solution instead of the native email archiving solutions within Microsoft 365.

KEY TAKEAWAYS

Here are the key takeaways discussed in this white paper:

- Microsoft 365 is being adopted by SMBs because it offers a wide range of communication and collaboration capabilities, it is reasonably priced, it requires only minimal IT involvement to maintain, and it is offered by a trusted and reliable vendor.
- Moreover, using a single vendor in the cloud for email, collaboration, email backup, email archiving and other capabilities makes sense because it makes IT's work simpler. However, even though moving to Microsoft 365 may be a good decision, this does not free decision makers from their obligation to take good care of their data.
- As a result, SMBs should have robust email backup and archiving capabilities in place to protect and preserve their critical data assets, many of which are stored in their email systems. Email backup and archiving are separate solutions, and both should be implemented.
- However, the "shared responsibility model" inherent in Microsoft 365 means that Microsoft is not responsible for protecting and preserving its customers' data. Instead, customers must take proactive steps to ensure that their data is appropriately backed up and archived.
- The consequences of not proactively protecting data can be significant: accidental or malicious deletion of important data, ransomware that can render data inaccessible, an inability to respond to legal or regulatory demands for data, and other problems.
- Every organization should deploy and maintain a robust email archiving solution to ensure that it is preserving its business records in email and to ensure that these records can be searched and produced quickly and efficiently. Moreover, decision makers should consider the use of third-party solutions that can more adequately preserve and archive their data.

SMBs should have robust backup and archiving capabilities in place to protect, preserve and keep available their critical data assets.

ABOUT THIS WHITE PAPER

This white paper was sponsored by MailStore; information on the company is provided at the end of this paper.

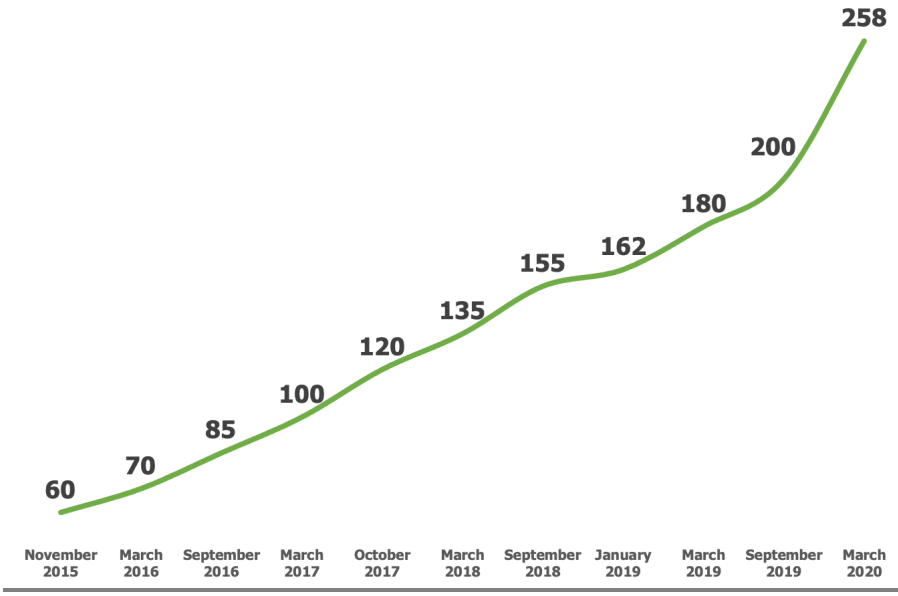
The Growing Importance of Microsoft 365 for Businesses

A GROWING NUMBER OF ORGANIZATIONS ARE DEPLOYING MICROSOFT 365

Microsoft 365 is a robust and capable platform that provides a wide range of capabilities, including email, desktop productivity applications, collaboration, security, archiving, encryption, voice and other services. Microsoft 365 is delivered in a variety of offerings for small businesses, enterprises, government entities, educational institutions and home users.

Although Microsoft has been providing hosted solutions in one form or another since the late 1990s, Microsoft 365 represents the most successful iteration of the company's non-on-premises email and collaboration offering. As shown in Figure 1, based on Microsoft's own data, the company had 258 million users as of the end of the first quarter in 2020, as shown in Figure 1. This is a more than quadrupling of the user base in less than four-and-a-half years.

Figure 1
Number of Global Microsoft 365 Users
Data shown in millions of users

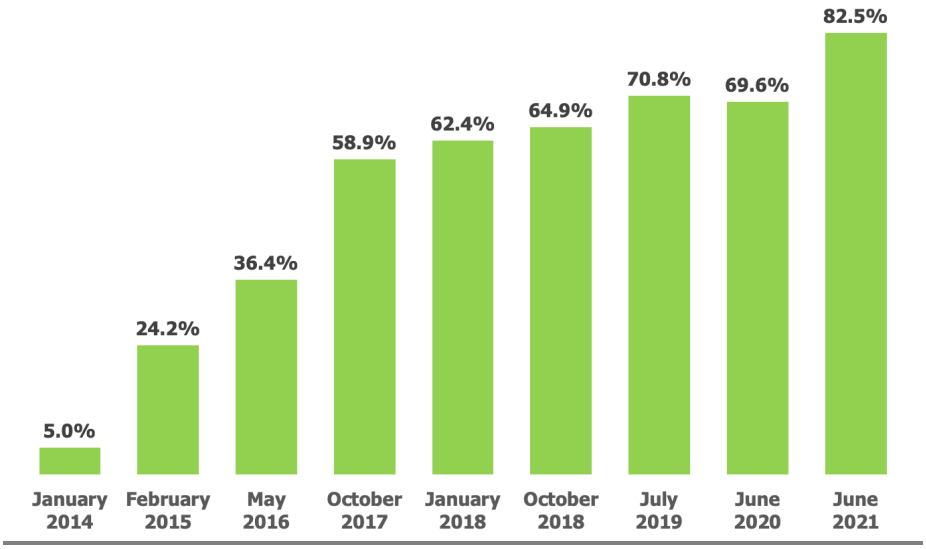


Source: Microsoft Corporation

Microsoft 365 is a robust and capable platform.

Coincident with the growth of the Microsoft 365 installed base is the penetration of Microsoft 365 into the business-grade email and collaboration market. As shown in Figure 2, a recent Osterman Research survey on Microsoft 365 found that approximately 71 percent of these users were equipped with Microsoft 365, up dramatically from just five percent five-and-one-half years earlier.

Figure 2
Penetration of Microsoft 365
Percentage of business-grade email users in North America equipped with Microsoft 365



Source: Osterman Research, Inc.

MICROSOFT 365 FREES ORGANIZATIONS FROM STORAGE-DRIVEN CONCERNS, BUT THERE IS A DOWNSIDE

One of the fundamental benefits of Microsoft 365's email component, Exchange Online, is its very large mailboxes. For example, Microsoft's plans offer a minimum of 50-gigabyte mailboxes and some include as much as 100 gigabytes.

While such large mailboxes can be a boon to user productivity by not limiting users' ability to store information freeing organizations from storage-driven concerns, there are some downsides to having such an enormous quantity of storage available to each user. For example, if a mailbox of 50 gigabytes needs to be restored from a backup, it will take much longer – and the user will be offline much longer – than if information is continuously migrated to an archive. Moreover, there can be decreased performance in Outlook if there are too many items in a folder[i], such as an increasing number of application pauses as the size of the Outlook data file grows beyond 10 gigabytes[ii].

UNDERSTAND THE ADVANTAGES AND DISADVANTAGES OF NATIVE MICROSOFT 365 EMAIL ARCHIVING

It is essential for decision makers that are considering or using Microsoft 365 to understand what the native email archiving capabilities within the platform can do – and cannot do – and determine if those capabilities will meet the organization's retention and usability requirements. We will explore the key email archiving capabilities in Microsoft 365 in the next section.

Email continues to be the primary method for communications and collaboration in the vast majority of organizations, including SMBs. Email systems contain a wide variety of data types, such as contracts, purchase orders, marketing plans, shipping records, communications with clients and prospects, responses to technical support inquiries, HR records, and many other types of information – all of which are business records. As a result, because business records must be retained for the appropriate length of time as determined by court decisions, regulatory obligations, industry best practices, or the advice of legal counsel, every organization should maintain an archive of its emails and attachments in order to retain and preserve these records.

It is essential for decision makers that are considering or using Microsoft 365 to understand what the native archiving capabilities within the platform can do – and cannot do.

A failure to retain records can carry with it a number of consequences. These include the inability for an organization to adequately defend itself in a legal action, a court fine or sanction for a failure to retain required records, regulatory fines, and the inability to fully retain a record of information that can be crucial in the normal operation of a business. However, there are also day-to-day situations in which having ready access to email data is useful. For example:

- A salesperson needs to find all information when a customer has a dispute about an order.
- A supplier asks about a commitment that was made to them.
- A user accidentally deleted or moved an email from his mailbox.
- An email is unavailable on the mail server and also not present in the latest backup.
- There is a need to determine if the company is complying with the European Union's General Data Protection Regulation (GDPR) or other compliance obligations.

WHY SHOULD MICROSOFT 365-ENABLED SMBs CARE ABOUT EMAIL ARCHIVING?

It's important to note that while Microsoft offers a robust and capable communication and collaboration solution in Microsoft 365, email is not automatically archived in the platform, either by the included In-Place archiving capability or the premium Exchange Online Archiving. Organizations that have deployed Microsoft 365 must either invest the time to fully understand how to reliably apply combinations of Compliance Center features, such as retention rules and litigation holds, or use a third-party email archiving solution that may be more intuitive to use, especially for SMBs with limited or no dedicated IT department.

While Microsoft offers a robust and capable communication and collaboration solution in Microsoft 365, email is not automatically archived in the platform.

IS EMAIL ARCHIVING UNNECESSARY WHEN USING BACKUP?

Businesses relying on email should be doing *both*, and here's why:

- Email backups are intended for tactical purposes to restore against issues that could cause data loss, such as a software upgrade that goes awry or a rogue administrator or other employee that deletes data. Backups have a short-term focus, they contain unindexed data, they are typically retained for no more than 30 to 90 days, and they are intended to capture data only at a given point in time.
- Email archives, on the other hand, are intended for strategic purposes to preserve business records in response to legal, regulatory and best practice requirements. Email archiving is essential to preserve data in its original form, to index that contain for purposes of search and retrieval, and to keep it available and retrievable at any time. While email backups have a short-term focus, email archives are designed for data that is to be retained for much longer periods – typically one year to indefinitely. Moreover, while email backups are designed to capture snapshots of data at one point in time, email archiving captures all business records on a continual basis and are there to work with for browsing, restoring them when necessary, complying with retention requirements, etc.

In short, email backups and archives are complementary best practices, not competing ones.

What are Microsoft's Options?

Depending on the Microsoft 365 plan chosen, either In-Place Archiving or Exchange Online Archiving (EOA) are available as archiving options. EOA is included with some Microsoft 365 plans, but is available as an add-on option in others. Here are the various options for archiving in Microsoft 365:

- **Archive to .PST**
  Users can "archive" their email content to .PST files that are stored locally or in the cloud, but this is not a recommended option. This content is not indexed and so is difficult to search and produce when needed. Moreover, .PST files are intended only for archiving in an Outlook context, since the initial Outlook archiving feature (called AutoArchive) is based on .PST files. This feature, while referred to as archiving, really isn't a true archive, but is designed only to relieve mailboxes of less-used or older emails.

  How it works: users can choose folders or individual emails to archive and these can be manually or automatically moved out of the primary mailbox. This content will be stored in a .PST file and location of the user's choosing.

- **In-Place Archiving**
  Another option is In-Place Archiving that allows users to archive their mailboxes using Outlook on-premises or on the web. This capability enables users to copy or move email content between their primary mailbox and their archive mailbox. While this is an individual capability, administrators can also use PowerShell to enable or disable archive mailboxes for all of the users across an organization[iii]. The problem with In-Place Archiving is that there are limited retention options compared to EOA and third-party archiving solutions, there is no platform independence, it will not be suitable as a way to satisfy most compliance obligations (since it provides essentially a mailbox storage extension), and it can be complex (using PowerShell is not a skill that most SMB employees possess).

  How it works: an archive mailbox is created in addition to the user's primary mailbox, but the archive mailbox is still accessible from the Outlook client or via Outlook on the web. Content can be copied or moved to the archive mailbox and back to Outlook, but the archive mailbox is accessible only in online mode. Retention policies can be created to move content from the primary to the archive mailbox based on user-defined parameters.

- **Exchange Online Archiving**
  EOA is a better option than In-Place Archiving (and a *much* better option than archiving to .PST files) because it offers a number of useful capabilities, such as In-Place Hold, which prevents the deletion of data that should be retained for long periods; it provides an integrated management interface to allow administrators to manage archives across an organization; it includes some eDiscovery tools; and it provides retention policies that enable more granular retention capabilities; among other capabilities.

  How it works: EOA enables users to have their content archived into an archive mailbox that is visible with the users' primary mailbox using the Outlook client or Outlook on the web. The archive mailbox can receive email by dragging-and-dropping .PST files or individuals into it, by using the Import and Export wizard in Outlook, or by using Archive Policies to move content into the archive automatically. EOA does not permit the use of transport rules, journaling or auto-forwarding to move content into the EOA archive.

The following table summarizes the capabilities of these three options:

EOA is a better option than In-Place Archiving (and a much better option than archiving to .PST files).

Figure 3
Comparison of Microsoft Email Archiving Solutions

	Archive to .PST	In-Place Archiving	EOA
Content indexing	No	No	Yes
Will satisfy legal requirements	No	No	Yes
Will satisfy regulatory requirements	No	No	Yes
Includes eDiscovery tools	No	No	Yes
Robust retention options	No	No	Yes
Archives emails from non-Microsoft sources	No	No	No[iv]
Provides platform independence	No	No	No
Accidental deletion protection	No	No	Yes

Source: Osterman Research, Inc.

In short, EOA and third-party email archiving solutions are the only real point of decision for corporate managers, since archiving to .PST files and In-Place Archiving can co-exist with either EOA or third-party email archiving solutions to provide limited, personal productivity benefits for single users in some situations.

ANOTHER OPTION FOR "ARCHIVING"

We should also mention another option to archive messages within Outlook, although we have separated it from the options discussed above because we don't consider it to be a true archiving option. Microsoft Outlook includes an Archive button that enables users to move an email message from the Inbox to an Archive folder. While referred to as an "archive", this option is intended just to move more important emails out of the Inbox and into a separate folder, not into a true archive.[v]

IMPORTANT LIMITATIONS IN NATIVE MICROSOFT 365 EMAIL ARCHIVING

There are some limitations that SMB decision makers must consider:

- **Problems for administrators**
  Some third-party email archiving solutions offer a faster and easier learning period for administrators than is the case for EOA, as well as enabling easier and more granular archiving policies. Moreover, for organizations that are already using a third-party archiving solution that will support Microsoft 365, switching to EOA will possibly result in an increased administrative effort with limited benefit.

- **Litigation holds**
  Third party solutions can provide a better experience when the legal function determines that a litigation hold is necessary. For example, when restoring data from a litigation hold in Microsoft 365, there are a number of complex steps that must be undertaken to restore the data.[vi]

- **The archive is not truly independent**
  Archived data still exists on the Microsoft tenant along with other Microsoft 365 data, and so can still be affected by problems like ransomware, account takeovers, service outages and the like. Moreover, a third-party email archiving solution is not tied to Microsoft 365, and so is truly independent with no vendor lock-in, offering the flexibility to move to another solution at any point with no effect on the archive.

- **Data residency challenges**
  From the beginning of Microsoft 365, the design of the tenant architecture was that each organization used one and only one tenant, homed in one geographical

Some third-party archiving solutions offer a faster and easier learning period for administrators than is the case for EOA.

region, and to which all out-of-region traffic would route for access to the organization's data. This design works perfectly for organizations that are solely active in one geographical region, but can cause significant data sovereignty and data residency challenges for multi-national and cross-regional organizations. The sole tenant location for the organization is set when the organization first signs up for Microsoft 365, and even then, some content types in Microsoft 365 have only been served out of the North American region, regardless of the organization's master region, although this is slowly changing over time.

That said, Microsoft recently announced that both Microsoft 365 and Dynamics 365 will now be served from a new German data center, alleviating data sovereignty issues for German customers of these platforms[vii]; existing German customers will not be served from German data centers, at least initially[viii]. However, Microsoft also announced in late February 2020 that "Microsoft 365 Germany is no longer accepting new customers or deploying new services", but new cloud regions in Germany will support Microsoft 365, and offer data residency within Germany[ix].

Microsoft stores data at-rest in a large number of locations. For example, customers in the Americas may have their data stored in the United States, Brazil or Chile; customers in the European Union may have their data stored in Austria, Finland, France, Germany, Ireland, the Netherlands or the United Kingdom. Importantly, however, Microsoft notes that "the locations where customer data may be stored can change.[x]"

Microsoft 365 includes the ability to recover accidentally deleted files, but there are some limitations that are important to consider.

However, in July 2020 things changed considerably. The EU-US Privacy Shield framework between the European Union and the United States had protected the transfer of data from the European Union to the United States, but was criticized by privacy advocates because US privacy laws do not provide the same level of privacy protection as those in the European Union, and do not satisfy the requirements of the GDPR. In July 2020, Privacy Shield was struck down unexpectedly by the Court of Justice of the European Union (CJEU); the Safe Harbor agreement was similarly struck down in October 2015.

The dissolution of Privacy Shield is significant, since about 5,000 companies in the United States and about 250 companies based in Europe were enrolled in the agreement[xi]. What this means for customers that must transfer personal data on residents of the European Union to the US is that they can no longer do so under the protection of Privacy Shield and must find other ways to transfer data. While this can still be accomplished, the process will now be more cumbersome, potentially slower, and possibly more expensive. For example, Standard Contractual Clauses (SCCs) may still be used to transfer this data to the US and other countries outside of the European Union (and were already in place with Microsoft 365 in conjunction with Privacy Shield). However, SCCs may be more difficult because the CJEU has required data protection authorities in the European Union to more carefully scrutinize these transfers and block them if needed. Binding corporate rules may be used, but the difficulty associated with implementing them makes them unreasonable for use by smaller organizations. There may be another version of Privacy Shield in the future, but as of this writing that is not the case. Consequently, organizations that must transfer data outside of the European Union will need to rely on potentially risky SCCs or find alternative ways of transferring data.

- **Data Privacy Agreements**
  Microsoft has been under criticism for quite a while especially from the EU concerning data privacy and data processing. Just recently, Microsoft published their *Online Services Data Protection Addendum (DPA)* for Microsoft 365, which includes their data protection terms, SCCs and European Union GDPR details. While this is an improvement as the content of the Online Services Data Protection Addendum can satisfy legal requirements under GDPR, this creates two potential problems for customers: 1) they are not able to negotiate terms of

the agreement as they usually can with a separate DPA, and 2) the potential transfer of data to the United States was covered only by the EU-US Privacy Shield framework, which no longer exists. Plus, while a customer might try to negotiate changes to their Online Services Terms, Microsoft might not be willing to negotiate such a change, particularly for SMBs[xii].

- **Limited storage of audit reports**
  Audit logs used to be retained for a period of 90 days across Microsoft 365 plans, but this limit has been increased to one year, but only for organizations running Microsoft 365 Plan E5[xiii], or for Microsoft 365 plans with the Compliance Add-On license[xiv].

- **Accidental/intentional deletion protection**
  Microsoft 365 includes the ability to recover accidentally deleted content, but there are some limitations that are important to consider. Content that has been deleted by a user is placed into the Recycle Bin (aka the Deleted Items folders) and is available for a default of 30 days – if it has not been emptied, it's a simple matter to recover this content from the Recycle Bin by simply dragging it back out to the desktop or a folder. If discarded content is more than 30 days old, it will still be recoverable from the Recoverable Items folder for a default of 14 days, meaning that accidentally deleted content is available for a maximum of 44 days by default[xv]. Users have the ability to delete emails from their archive, either manually or automatically via retention policies[xvi].

- However, there are some limitations to consider in the context of accidental deletion protection:

  - If a user purges their Recycle Bin or the Recoverable Items folder, content will not be recoverable.

  - Content can be recovered only to the original user and is not accessible by others unless it is first recovered and then transferred to someone else.

  - Content in the Recycle Bin counts as part of each user's storage quota.

  Another option to prevent against accidental deletion of content is to use Retention Tags and Retention Policies within Microsoft 365, which will allow it to be secured against accidental deletion. However, the process for using these capabilities is somewhat involved: 1) One of three types of Retention Tags is created for each message or folder to be retained, 2) a Retention Policy is created for each group of Retention Tags, 3) Retention Tags are linked to Retention Policies, and 4) Retention Policies are then applied to different groups of mailbox users[xvii].

  A Litigation Hold can also be implemented that will take precedence over Retention Policies[xviii]. However, Litigation Holds cannot hold data retroactively and will not protect data for any content that has been altered or deleted prior to the implementation of the Hold.

- **Retention Policies result in a significant increase in storage**
  While Retention Policies are useful, they count against the storage allocation for each account, and so storage volumes can increase significantly if these policies are in use[xix]. In some instances, additional storage will have to be procured to accommodate the additional storage requirements.

  While Exchange Online Archiving permits (almost) unlimited archiving (there is a one terabyte limit in Exchange Online) via the Auto-Expanding Archive feature, there are some limitations that need to be considered[xx]:

  - Each user's archive mailbox is intended for use by only that user. IT administrators are not permitted to create shared mailboxes and allow users

There are several advantages to using third-party email archiving solutions.

to copy (through the cc: or bcc: field, or through a transport rule) to a shared mailbox for the purpose of archiving their content[xxi].

- The use of transport rules, journaling or auto-forwarding rules to copy messages to an Exchange Online Archiving account is not allowed.
- Administrators do not have the ability to adjust the storage quota using the Auto-Expanding Archive feature.
- The Auto-Expanding Archive feature does not support users whose mailboxes are provided via Exchange Server 2010, which can be an issue in hybrid environments.

- **Retention Policies alone do not protect against rogue administrators** While Retention Policies provide useful protections against accidental deletion of data, by themselves they do not offer protection against either rogue administrators who might maliciously delete data or modify Retention Policies; or against malicious bad actors, such as hackers, who might disable these policies. Microsoft 365 enables the use of the Preservation Lock capability that will prevent malicious users and hackers from modifying or disabling Retention Policies. However, the downside is that a Preservation Lock cannot be undone, which has two important implications[xxii]:
  - If the storage allocation for an account gets filled, additional storage will have to be purchased given that data under lock cannot be deleted.
  - If, under a privacy regulation like the GDPR or CCPA, a data subject requests their data to be deleted and there is no obligation for the data controller or processor to retain that data, or you no longer have a legal basis to keep the data, the data under lock cannot be deleted in compliance with the privacy regulation. This could lead to a compliance violation.

The native Microsoft 365 capabilities to protect data use the platform itself to provide data protection, which is a violation of the 3-2-1 Rule.

Recommendations and Next Steps

Osterman Research recommends that SMB decision makers take a number of steps as they evaluate their needs for an email archiving solution, and which archiving solution to implement.

UNDERSTAND THE NEED TO ARCHIVE EMAIL

Osterman Research has found that many organizations do not yet appreciate the importance of archiving emails and attachments. Interestingly, this is not an issue limited to SMBs, but even many large enterprises do not archive their emails and attachments. As discussed in this paper, a failure to archive email and attachments will prevent organizations from adequately satisfying their legal, regulatory and other obligations to find and produce data when needed. The consequences of being unable to do so include fines, sanctions, loss of corporate reputation and a number of other serious problems that almost always are more expensive than an archiving solution.

CONSIDER THE ADVANTAGE OF USING THIRD-PARTY TOOLS

While Microsoft's native email archiving capabilities provide some level of protection, there are several advantages to using third-party email archiving solutions:

- The ability to have an archive independent of the Microsoft 365 platform in order to satisfy the need to follow with the 3-2-1 best practice discussed later in this report. This is particularly important when using a cloud service like Microsoft 365, since the primary infrastructure supporting email should not be the same one supporting email backup and archive.

- The use of an independent archiving solution provides the ability to archive content from non-Microsoft email sources within the same archive. While multiple archiving solutions can be maintained, this adds to the cost and complication of retaining business records. Using a single archive reduces the number of siloes that IT must maintain and that must be searched.

- EOA does not provide for a shared email archive or group access to others' archived content. Microsoft explicitly intends EOA to be for individual users, noting that "A user's archive mailbox is intended for just that user.[xxiii]"

- The ability to index a greater number of file types, which leads to easier search and retrieval of content.

- The ability to prevent users from deleting content from their own archive manually without the need to use Retention Policies.

- Many third-party archiving solutions will enable deduplication, which can significantly reduce storage requirements and speed searching.

- EOA is not really designed as a mailbox quota management tool, while many third-party archiving solutions are designed to be used in this capacity. Minimizing the size of the Outlook mailbox can provide performance benefits as noted elsewhere in this paper.

CONSIDER THE IMPLICATIONS OF LOST OR MODIFIED EMAILS

An organization that cannot maintain copies of its emails, and ensure that these copies are authentic, can suffer a number of consequences that prevent it from fulfilling its legal, regulatory and best practice obligations. For example, an inability to retain all relevant business records will mean that there are holes in the data record that will provide an incomplete picture of a company's operations. Missing or lost emails, or those that were subject to modification, will be useless for legal or regulatory considerations. Employees who do not have access to their old emails may need to spend time recreating content that should have been captured in an archive, thereby reducing employee productivity.

CHECK YOUR DATA PRIVACY REQUIREMENTS

It's important to note that the Microsoft Online Services Terms contain a provision that allows Microsoft to make changes unilaterally. If a DPA is a requirement based upon an internal policy when personal data will be processed by a third party, IT managers and others charged with making decisions about Microsoft 365 should consult with their legal, compliance and/or Data Privacy Officer to determine if the absence of a separate DPA will be a critical issue – for some organizations in some jurisdictions, it might be.

IT managers and others charged with making decisions about Microsoft 365 should consult with their legal, compliance and/or Data Privacy Officer to determine if the absence of a separate DPA will be a critical issue.

ENSURE AN INDEPENDENT COPY OF EMAIL

The "3-2-1 Rule" is a well-accepted best practice that dictates that an organization retain three copies of its data: two of them locally and one that is remote and separate from the primary system that created and stores the data. In the traditional, on-premises email model, having a copy of email and attachments on the email server, one in local email backup and archiving solutions, and the backups and archived content stored in a remote location (e.g., in the cloud) satisfies this best practice.

However, the native Microsoft 365 capabilities to protect data use the platform itself to provide data protection, which is a violation of the 3-2-1 Rule. Osterman Research recommends the use of an external service or platform to protect Microsoft 365 data in order to be more in line with best practices. In fact, this practice is implicitly recommended by Microsoft itself in its customer support service agreement: "You

understand that data can be inadvertently lost, corrupted or breached, and agree that you are wholly responsible for the backup of any and all data…"[xxiv].

END-USER SELF SERVICE IS KEY

The ability for end users to search for and find their own emails alleviates this burden from IT staff members, and it makes employees more efficient by enabling them to gain access to their emails and files much more quickly. This results in a "win-win" for both IT and employees, ensuring that information is as accessible as possible with a minimum of effort.

FUTURE-PROOF THE ARCHIVE AND ENSURE ITS PORTABILITY

Using a third-party archiving capability ensures that the archive will avoid vendor lock-in. This is important to provide as much flexibility as possible.

PURSUE BOTH BACKUP AND EMAIL ARCHIVING STRATEGIES

As noted earlier, email backup and archiving are both best practices that serve different functions: backups are necessary as a tactical process with a short time horizon to ensure rapid recovery of data in the event of their failure, while archiving is a strategic process to ensure data preservation over long periods.

DO A THOROUGH COST ANALYSIS

While email archiving capabilities are included with Microsoft 365 Plans E3 and E5, the use of third-party archiving solutions can enable organizations to deploy less expensive Microsoft 365 plans for some companies, reducing the total cost of ownership for both Microsoft 365 and overall communication and collaboration capabilities. While the use of third-party solutions in conjunction with Microsoft 365 can add a bit of complexity for IT in terms of solution and licensing management, the cost benefits of doing so almost always outweigh these additional complexities.

CONSIDER SYNERGIES

Finally, consider the synergies that can be achieved by using Microsoft 365 and third-party archiving capabilities. For example, an organization that operates both Microsoft 365 and Google G Suite would need to maintain a) Microsoft 365, b) Google G Suite, c) an archiving capability for Microsoft 365, and d) a separate email archiving solution for Google G Suite. The use of a third-party archiving solution that accommodates both email platforms would eliminate the need for one archiving solution, it would eliminate IT requirements to manage an extra archiving solution, and it would streamline the ongoing process of searching for and producing information.

Using a third-party archiving capability ensures that the archive will avoid vendor lock-in.

Summary

Microsoft 365 is a robust and capable platform, but it has some limitations with regard to its email archiving capabilities that SMB decision makers need to consider. This puts uninformed business owners at unnecessary risk, and so these owners should seriously consider the use of third-party email archiving solutions.

About MailStore

MailStore is specialized in the development of innovative email archiving solutions for small and medium-sized businesses. With tens of thousands of customers in over 100 countries, MailStore is one of the global leaders in their field. Their products and solutions are used by small and medium-sized businesses from all sectors, as well as by public and educational institutions. Millions of private users are also using the free MailStore Home software.

MailStore's goal is to apply the best available technologies to support their customers in making efficient and sustainable use of email as one of the most valuable and comprehensive information resources of our time and to help them to meet a growing number of compliance requirements.

www.mailstore.com
sales@mailstore.com
+49 (0) 2162 502990 (Intl.)
+1 800 747 2915 (US)

REFERENCES

[i] https://support.microsoft.com/en-us/help/2768656/outlook-performance-issues-when-there-are-too-many-items-or-folders-in

[ii] https://support.microsoft.com/en-us/help/2759052/you-may-experience-application-pauses-if-you-have-a-large-outlook-data

[iii] https://docs.microsoft.com/en-us/microsoft-365/compliance/enable-archive-mailboxes

[iv] Using third-party data connectors, content from various non-mail sources can be archived

[v] https://www.brucebnews.com/2019/09/how-to-use-the-archive-button-in-outlook/

[vi] https://spanning.com/blog/office-365-data-protection-part-2-litigation-hold/

[vii] https://www.microsoft.com/en-us/microsoft-365/blog/2020/02/20/microsoft-office-365-dynamics-365-now-available-from-new-german-datacenter-regions/

[viii] https://www.datenschutzbeauftragter-info.de/microsoft-office-365-ab-sofort-ueber-deutsche-server-nutzbar/

[ix] https://docs.microsoft.com/en-us/microsoft-365/admin/admin-overview/learn-about-office-365-germany?view=o365-worldwide

[x] https://docs.microsoft.com/en-us/office365/enterprise/o365-data-locations

[xi] https://www.csoonline.com/article/3567061/eu-court-invalidates-privacy-shield-data-transfer-agreement.html

[xii] https://www.zdnet.com/article/microsofts-new-office-365-terms-we-wont-use-your-data-for-advertising-or-profiling/

[xiii] https://www.microsoft.com/en-us/microsoft-365/blog/2018/09/25/start-using-microsoft-365-to-accelerate-modern-compliance/

[xiv] https://docs.microsoft.com/en-us/microsoft-365/compliance/audit-log-retention-policies?view=o365-worldwide

[xv] https://docs.microsoft.com/en-us/exchange/security-and-compliance/recoverable-items-folder/recoverable-items-folder

[xvi] https://docs.microsoft.com/en-us/office365/servicedescriptions/exchange-online-archiving-service-description/archive-features

[xvii] https://docs.microsoft.com/en-us/exchange/security-and-compliance/messaging-records-management/retention-tags-and-policies?redirectedfrom=MSDN

[xviii] https://www.cloudessentials.com/blog/data-retention-policies-litigation-hold-office-365/

[xix] https://www.druva.com/blog/do-you-really-need-to-backup-office-365/

[xx] https://docs.microsoft.com/en-us/office365/servicedescriptions/exchange-online-archiving-service-description/exchange-online-archiving-service-description

[xxi] https://docs.microsoft.com/en-us/office365/servicedescriptions/exchange-online-archiving-service-description/archive-features

[xxii] https://docs.microsoft.com/en-us/office365/enterprise/office-365-data-immutability

[xxiii] https://docs.microsoft.com/en-us/office365/servicedescriptions/exchange-online-archiving-service-description/archive-features

[xxiv] https://support.microsoft.com/en-us/help/4203112/microsoft-customer-support-service-agreement