WHITE PAPER

The Need for Third-Party Archiving in Office 365

An Osterman Research White Paper

Published March 2015

actiance®

Osterman Research, Inc.
P.O. Box 1058 • Black Diamond, Washington • 98010-1058 • USA
Tel: +1 253 630 5839 • Fax: +1 253 458 0934 • info@ostermanresearch.com
www.ostermanresearch.com • twitter.com/mosterman

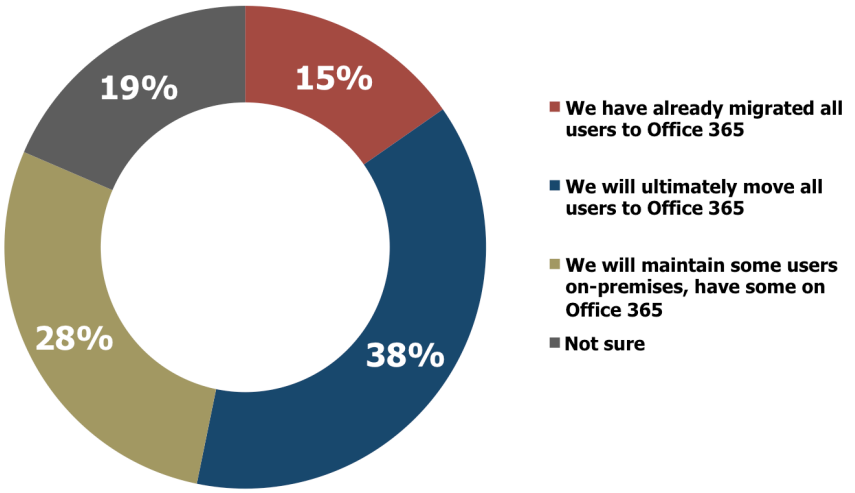
EXECUTIVE SUMMARY

As early as the 1980s, the business world began recognizing the value of corporate email to provide faster communication capability both internally and externally over traditional forms of communication. As email became a must-have business application, the courts, and later the federal government, also recognized the value of email as a potential repository of evidence in lawsuits and government inquiries. This acceptance of email as a viable target of records search pushed the business world to recognize the need to archive their corporate email to reduce the cost and risk during litigation and government inquiry.

The era of on-premises email archiving has been with us for at least 15 years and has made great strides in functionality, reliability and cost. During that time, cloud-based email archiving has also been on the rise, offering the same capabilities on-premises solutions offer.

Now, the business world has begun to recognize the possibilities of cloud-based office productivity suites and are adopting them in large numbers to take advantage of the benefits a cloud infrastructure can offer, including lower costs, easier application management, better security, collaboration capability, and integrated email archiving. For example, both Microsoft Office 365 and Google Apps provide integrated email archiving with capabilities that attempt to address both eDiscovery and regulatory requirements. This is important, because the penetration of these platforms is anticipated to grow significantly by 2016, as shown in Figure 1. Many analysts are estimating Office 365 will take the lion's share of the cloud-based office productivity market – mainly due to Microsoft's current market share dominance of on-premises Office and Exchange installations.

Figure 1
Plans for Migrating to Office 365 and Google Apps Among Organizations That Are At Least Considering Migration



Source: Osterman Research, Inc.

A related indicator of Office 365's popularity is the opinion that many companies moving to Office 365 are migrating their on-premises email archives to the integrated Office 365 email archive with the expectation (or hope) of reducing overall operating costs over that of their on-premises archiving solutions. Office 365 does include several built-in general-purpose email archiving capabilities and some basic functionality, such as simple eDiscovery and high-level retention capabilities for regulatory compliance. However, for many these simple capabilities may not be enough. For example, the Search capability built into Office 365 presents several

important limitations that many will find difficult to accept, especially for those trying to respond to eDiscovery requests. The most important question organizations contemplating an email archive migration to Office 365 should ask themselves is this: will the Office 365 email archiving capability meet or exceed the capabilities that were originally required when the stand-alone email archive was purchased in the first place? Obviously the answer to that question will drive the decision whether to migrate an email archive to the Office 365 cloud archive or keep them in a stand-alone, third-party email archiving platform.

In today's complex business, legal and regulatory environments, basic email archiving functionality is not enough and may end up costing an organization more than expected.

KEY TAKEAWAYS

- The legal, regulatory and business requirements for email archiving continue to grow and are becoming more complex.
- The risk and costs associated with inadequate email archiving capability continue to rise.
- In today's legal and regulatory environments, a powerful and comprehensive search capability is a must. Known Office 365 search limitations pose additional risks and costs not found with more powerful third-party archiving solutions.
- Office 365 email archiving capability does provide many basic archiving capabilities, but does not meet the additional eDiscovery and regulatory requirements with which many organizations are faced.
- Many third-party email archiving solutions have designed their solutions to meet the most stringent and complex email archiving requirements.

ABOUT THIS WHITE PAPER

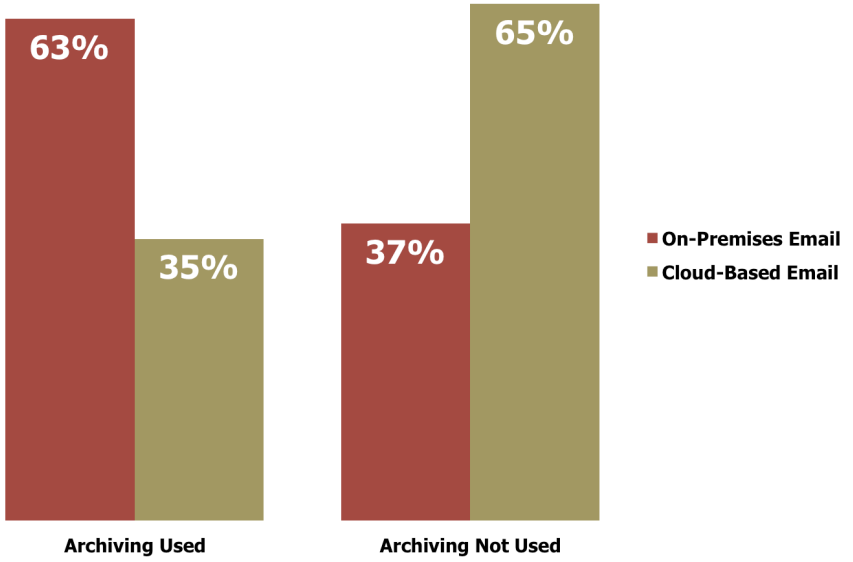
Email archiving has become an essential tool for helping organizations meet the constantly changing legal, regulatory, and business requirements most organizations are facing these days. This white paper will revisit the main reasons companies have adopted email archiving solutions in the past and compare those requirements to the archiving capabilities currently offered by Microsoft's Office 365 cloud-based office productivity suite. We will then establish how third-party email archiving solutions can address customer needs not addressed by Office 365. We will close out the white paper with a checklist of issues organizations should consider before choosing Office 365 as their email archiving solution.

THE NEED FOR EMAIL ARCHIVING

First, let's briefly describe what the standard email archiving solution actually does. Simply put, an email archiving solution captures/copies email, attachments, metadata, and other data directly from the target email server(s). That copied email and other data is moved to stand-alone archiving servers, which index and store all incoming content to make it accessible and searchable for later queries. Newer email archiving solutions provide additional benefits, such as higher levels of security, records management functionality (including disposition), transparent end-user access, search and granular legal hold, document review, and export in a legally defensible manner.

Over the last 15 years, constantly changing regulatory and legal requirements have driven email archiving solutions to add additional and more complex capabilities.

Figure 2
Current Penetration of On-Premises and Cloud-Based Email Archiving



Source: Osterman Research, Inc.

REGULATORY COMPLIANCE

Most industrialized nations have varying degrees of industry-related regulatory retention requirements specifying what organizational data (including email) should be kept and for how long. The United States has records retention laws that potentially touch every business, including retention laws targeted at the financial sector, healthcare, energy, pharmaceuticals, transportation, and general employment laws that span all industries.

For example, the financial services industry has both SEC and FINRA regulations that stipulate prescriptive requirements around the capture, monitoring and archiving of broker/trader communications, including email. To date, the only way to accomplish this requirement is by enabling the journaling capability within the Exchange email system. With journaling activated, any email sent or received within a mailbox is automatically copied and sent to the email system journal mailbox and then forwarded to a third-party email archive. The journaling function enables all email from target mailboxes to be captured and archived before the mailbox end-user could delete or edit it. In this way, the requirement to capture and secure all communications from broker/traders in its original state is met.

Another regulatory retention example that touches almost every business is around employment law. Human resources departments generate and receive enormous volumes of documents as email attachments, such as job postings, employment applications, resumes, results of reference checks, drug testing results, personnel files, vacation requests, payroll records and disciplinary files. All these document types (plus many more) have government regulatory retention requirements associated with them.

Corporate governance retention laws, such as the Sarbanes-Oxley Act (SOX), require specific record types to be retained for up to seven years. The Sarbanes-Oxley Act of 2002 is a United States federal law that sets new and enhanced standards for all U.S. public company boards, executive management, and public accounting firms. SOX focuses mainly on financial records of publicly traded companies and ensures those

documents are retained for possible review by the SEC if, at a later date, questions arise.

Other federal regulations with associated records retention requirements include the Homeland Security Act, the PATRIOT Act and the Federal Acquisition Regulations (FAR). The Homeland Security Act imposes security regulations (and record keeping requirements) on designated high-risk operations, such as chemical facilities, energy distribution facilities, and transportation operations. The PATRIOT Act sets the minimum records standards for financial institutions and their customers regarding the identity of customers opening new accounts at financial institutions. Requirements include the development of a compliance program with accompanying documented internal policies and procedures. Organizations are subject to independent or random reviews by multiple regulatory agencies. The Federal Acquisition Regulations (FAR) Subpart 4.7 provides policies and procedures for retention of records by all federal government contractors. All business entities who contract to supply goods or services to the federal government must retain all related records, hardcopy or electronic, for specific periods of time (varying from two to four years). These federal retention requirements all include email that in many cases can contain target content.

All government regulatory retention requirements now classify email as a record. A stated requirement of governmental data retention requires the ability of the organization holding the records to find and turn them over to a federal agency in an expedient manner and in their original state or condition. Email archiving provides organization with the ability to designate a *copy of record* by capturing, securing and making the archived email searchable.

To complicate the US regulatory landscape further, all 50 states and many local governments have regulatory retention laws that, in some cases, go beyond the federal regulations.

LITIGATION PREPAREDNESS

When litigation (or a government investigation) is pending or anticipated, an organization can greatly affect/reduce the probable costs of responding to an eDiscovery request or regulatory information request by managing their information in a manner that makes it easier to manage and query. Especially for those organizations that are regularly involved in eDiscovery, proactive actions can greatly reduce eDiscovery costs. There are three rules of thumb in eDiscovery (and regulatory) requests:

1. Large amounts of information will be requested.

2. An organization's email will be a major target.

3. How an organization secures its information and responds to the request can mean the difference between winning and losing the case.

An important step in litigation preparedness is stopping deletions of all potentially relevant information as soon as litigation is anticipated or known. In other words an organization should be able to apply a legal hold quickly, no matter where potentially relevant data is stored. A documented and tested legal hold process that secures data that *could be relevant* in litigation will dramatically reduce an organization's risk of spoliation (destruction of evidence). Email systems are notorious for letting end-users inadvertently (or on purpose) delete emails without restriction. Because of this, email archiving solutions are used to ensure security/litigation hold requirements.

The process of Early Case Assessment (ECA) is comprised of two different aspects: estimating the cost and time needed to defend (or prosecute) a legal case and, more importantly for this discussion, quickly searching for and analyzing potential evidence from all locations to develop a case strategy and create an eDiscovery and litigation plan to best achieve a successful resolution. In other words, searching for as much

information and potential evidence as quickly as possible to determine early on if the case has merit and therefore should be settled or continue to trial. Obviously the more relevant evidence an organization can collect in the very early stages will provide the basis of a more successful ECA strategy. Because email is almost always a major target of eDiscovery, the ability to access and search email stores is extremely necessary for ECA.

The actual eDiscovery process encompasses several distinct but dependent processes. At its most basic, eDiscovery is reliant on the ability to find (search), access, and review potentially relevant (case-specific) data. The costs (and risks) during the eDiscovery process skyrocket when an organization is unable to find, secure, and review all potentially relevant information in the time allotted by the court. The downside for not finding all responsive information or taking too much time can lead to a court to take actions that put a case defense at risk, such as disallowing evidence or issuing and adverse inference instruction. Because of this possibility, many organizations will collect too much data to ensure they cannot be charged with hiding or misplacing evidence. In an over-collection situation, more must be spent to either have groups of external attorneys manually review each of the potentially millions of pages of email and other documents, or to purchase specialized technology to determine if any of the over-collected information is privileged, confidential, or relevant to the lawsuit.

Over-collection can add millions of dollars to the cost of defending a single case. An under-collection situation can cause the organization to lose the case before it goes to trial because of an inadequate eDiscovery ruling from the court. Knowing what information an organization possesses and where it is stored, as well as granular information management is the key to reducing both the cost and risk of eDiscovery.

FUNCTIONAL BENEFITS OF EMAIL ARCHIVING

Besides the legal and regulatory benefits from email archiving, there are others that can benefit the organization as well. These benefits include storage management, performance enhancement, end-user and IT productivity, and knowledge management.

- **Storage management**
  Most IT professionals will say that the biggest benefit of email archiving is the ability to reduce enterprise storage requirements. On-premises Microsoft Exchange email systems can consume enormous amounts of storage resources, particularly if an organization has also enabled archive mailboxes for each user. For this reason alone, as well as for performance levels, most Exchange administrators will also impose a mailbox limit of end-users restricting the amount of email each end-user can save in their email inbox. Third-party email archiving solutions can save large amounts of storage space used by the Exchange servers because by allowing the off-loading of email to the archive sooner while still providing end-user access to it. The email archive is a better choice for email storage due to the effective single instance storage functionality, deduplication and compression capabilities, as well as the transparent end-user access to archived email.

- **Performance enhancement**
  Email systems were never designed to act as a huge file system, and so storing huge amounts of data on an email system can dramatically affect the system's overall performance. One of the primary benefits of employing a third-party email archiving system is to off-load the email server of email and attachments so that the service level agreement (SLA) can be met.

- **End-user and IT productivity**
  Because of the need to control the growth of network storage, many companies will set Exchange mailbox limits to limit the size of mailboxes and so that system performance is not adversely affected. When mailbox limits are imposed, end-users will tend to move email out of the email system and store it elsewhere

instead of deleting it to free up mailbox space. Many end-users will move email and attachments out of their email box in the form of a .PST file. These .PSTs are then stored in various interesting places like file system share drives, removable media, personal cloud accounts, and even personal email accounts. This strategy makes searching for email/attachments at a later date time-consuming and can be a hit and miss activity. In many cases, end-users that cannot find email they need to reference, and must recreate the data, taking even more time. An email archive acts as the central repository of record so that it far easier to search for and if the content is not in the archive it doesn't exist anymore.

- **Knowledge management**
  It has long been recognized that an organization's email system is the one repository that contains the organization's knowledge. The problem is that it is highly unstructured and unmanaged and even though contains huge amounts of valuable organizational information, email was not designed to make it easily available. With the advent of Big Data Analytics and other tools, email archives are now better positioned to enable the mining of this vast corporate knowledge base.

EXCHANGE HAS MOVED TO THE CLOUD

The move from on-premises Exchange email systems to the cloud-based versions of Exchange is difficult to estimate because Microsoft has not published those numbers. However, many believe the move is large and accelerating. In fact, Tony Redmond of Tony Redmond's *Exchange Unwashed Blog*[i] has estimated that Office 365 paid subscriptions have reached 29.76 million seats, or almost 10% of the installed Exchanged seats. Again, because Microsoft has not broken out the actual numbers, it is difficult to estimate how many of those 29 million Office 365 subscribers have replaced their on-premises Exchange system. However, needless to say, it's probably a significant number of them.

WHAT IS OFFICE 365?

Office 365 refers to cloud-based subscription services offered by Microsoft that include access to the ubiquitous Office suite of applications (plus other productivity services) that are enabled through cloud-based services. Many of the Office 365 subscription plans also include the desktop version of the latest Office applications that users can install across multiple computers and devices. Exchange Online, the email application of Office 365, is a hosted messaging solution that delivers the same capabilities of the on-premises Microsoft Exchange Server as a cloud-based service. It gives users single sign-on access to email, calendar, contacts, and tasks from PCs, the Web, and mobile devices. To effectively utilize the Exchange Online capabilities, Internet access is required.

OFFICE 365/EXCHANGE ONLINE AND EMAIL ARCHIVING

Office 365 provides for each user's Exchange Online mailbox also to be supplied a basic archive mailbox as well. This basic archive capability has received some positive comments from end-users and has caused some organizations to consider moving away from their current third-party email archiving solutions. Organizations considering this move should be aware of several important email archiving features not currently available with the email archiving capability in Office 365.

WHERE OFFICE 365 STILL FALLS SHORT

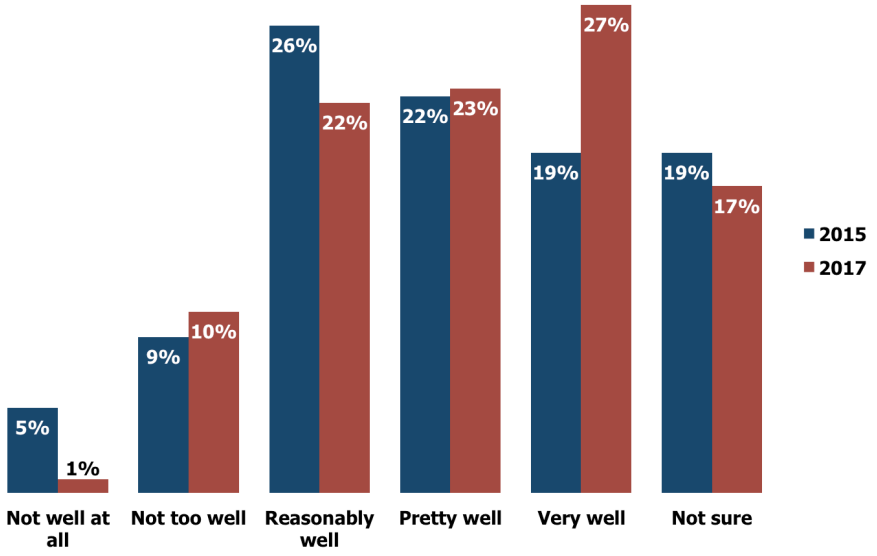
GENERAL USABILITY ISSUES

Because Office 365 is a cloud-based solution, access to your archive is not available from within your Outlook client if you are not connected to the Internet. This is because the online email cache is not copied to your local computer's Outlook client. This could be a problem for travelers trying to access an archived message when not

actively connected to the Internet. This also means that even when you are online and synced, clicking on an archived email message could take longer than expected because it must be located and copied from the cloud.

The Web browser determines where on a computer the offline information is stored and how much space it can use. If offline information will not fit in the space that's been set aside, users may be prompted to increase it. If the space cannot be increased, less information will be available when offline.

Figure 3
Anticipation that Office 365 Will Meet Current and Future Archiving Requirements



Source: Osterman Research, Inc.

STORAGE MANAGEMENT

Much has been made of the claim of unlimited storage for mailbox and archive mailbox in Office 365. This is true with certain subscription plans. However several Office 365 subscription plans limit the total user mailbox/archive mailbox to 50 gigabytes each. These limited storage plans are:

- Office 365 Business Essentials
- Office 365 Business Premium
- Office 365 Enterprise E1
- Office 365 Educational E1
- Office 365 Government E1

The remaining plans place a default 50-gigabyte storage limit on each user's mailbox, but offer unlimited archiving storage for each mailbox. In the past, a 25-gigabyte mailbox and a 25-gigabyte archived mailbox might seem like a great deal of space, but as email attachments have grown dramatically, a 25-gigabyte or even 50-gigabyte storage limit may not be sufficient for some end-users. Once a user reaches the mailbox limit, they are faced with deleting data or paying for more storage space.

LACK OF GRANULARITY IN RETENTION/DISPOSITION

Generally speaking, centralized retention/archiving of emails in Office 365 is based on simple policies and the placement of end-user tags. There are two system-based

retention tags available; the default policy tag and the retention policy tag. Retention tags specify how long a message is kept and the action taken when the message reaches the specified retention age. When a message reaches its retention age, it is moved to the user's archive mailbox, or it's deleted.

A retention tag is used to apply retention settings to messages and folders. The three types of retention tags available are the Default Policy Tag (DPT), the Retention Policy Tag (RPT), and Personal Tags (PT). In Office 365, a retention policy is a group of retention tags that can be applied to a mailbox. A retention policy can have one DPT to move items to the archive, one DPT to delete items, one DPT to delete voicemails, one RPT to for each supported default folder, and any number of PTs to be applied by the end user in custom folders.

The default policy tag (DPT) applies to all items in a mailbox that don't have a retention tag already assigned. Retention policy tags (RPT) are applied to default folders, such as Inbox, Sent Items, Deleted Items, and Junk Mail and again are based on time spent in the folder. An RPT takes precedence over a DPT. A caveat for RPTs is they don't support a retention action that moves items to the user's archive mailbox. The only retention action for RPTs is to delete items.

The third type of retention tag, the personal tag, is available for end-users to use within custom folders and can be applied all the way down to a single email message. The personal tag allows the end-user to assign retention tags to their email messages.

These three types of retention tags are basic and don't really address the granularity of retention requirements in today's corporate information governance environment in that they are applied to an entire folder instead of an individual email message.

ARCHIVE MAILBOX ISSUES

The most apparent limitation to Office 365 and email archiving is that the archived mailbox and its contents are not available when offline[ii]. For employees that travel, this limitation can be extremely frustrating. Many third-party email archiving solutions offer local archive caches to address this specific limitation.

Another major issue with Office 365 email archive mailboxes is the possibility they could fill up and stop accepting additional email. Administrators have the capability to assign archive mailbox quotas so that email box archives cannot grow beyond a certain size (or age), causing additional subscription costs. For some subscription plans, an unlimited archive mailbox size is the default, but on other plans a maximum mailbox/archive mailbox size could be the default. The issue surfaces when a quota-limited archive mailbox nears its limit – a warning message is be sent to the user. By default in Exchange Online, the archive-warning quota is set to 45 gigabytes and the archive quota is set to 50 gigabytes.

This circumstance could create a situation in which an In-Place Hold is applied to the archive mailbox at the same time the archive mailbox is unable to accept new email into the archive due to the size quota. This inadvertent failure to move new responsive email into the archive mailbox could be interpreted by the court as the data not having been placed on litigation hold. If content not allowed into the archive due to a quota situation is inadvertently deleted, a spoliation or destruction of evidence charge could be brought. Again, this situation would surface only in those situations where a size-limited archive mailbox exists or a quota limit has been set on an unlimited archive mailbox. But the fact that only the mailbox owner is made aware of the situation is very troubling for both regulatory, as well as legal/eDiscovery, situations.

DEFENSIBLE DISPOSITION

Organizations have been over-retaining electronic data for many years, even though it is no longer needed for business, regulatory or eDiscovery requirements. In fact,

the Counsel for Information Auto-Classification (CIAC) published a 2011 survey[iii] that found 58% of organizations are keeping information indefinitely. In a 2012 ESG survey[iv], 65% of respondents replied that their organization did not dispose of data because of a fear of an inability to furnish data requested as part of a legal or regulatory request, or for business needs. The same CIAC survey also reported that 79% of organizations report that they spend too much time and effort manually searching for and disposing of information and 58% still relied on individual employees to decide on retention-disposition questions. These statistics all point to the ongoing problem that organizations are still not disposing of electronic data properly.

Disposing of information is not just a question of storage management, but more importantly, it's a question of legal risk and cost. The issue is this: all existing data, not just records that could be potentially relevant to a legal case must be found and reviewed for relevancy and privilege during eDiscovery. Data not found during eDiscovery, but found later on, raises the specter of insufficient eDiscovery or worse, a charge of hiding responsive information. To lessen this risk, many general counsels instruct their eDiscovery teams to over-collect to ensure responsive data is not left behind. This conservative practice drives up the cost of document review.

Office 365's retention/disposition capability is basic in that the system can choose to retain, delete or archive based on email age and/or custodian, department, etc. This is not to imply the disposition process is not defensible (systematic disposal can be defensible if the reasoning is documented and it is always followed), but many CIOs and general counsels have expressed a need for a more granular retention/disposition capability.

PRODUCTIVITY/SEARCH

It is one thing to store large amounts of email and attachments in an archive; it's another to actually find specific content when it is needed. At last count, Exchange Online and Office 365 indexes 58 different file types[v] (many of them Microsoft file types). Decision makers may ask themselves why this is considered an issue…an email message is just an email message, right? The problem is that email messages can also contain important file attachments that in turn contain the data that may be needed. If the data needed is contained in an unindexed attachment, that message will never appear in the search results. This issue affects end-user productivity (and eDiscovery) in two ways. First, in many instances, an end-user may remember they had this data at one point in time, but because the desired content doesn't appear in their initial keyword search of their archive, they spend additional time (productivity) trying to find it. And second, when they finally realize they cannot find it, they spend additional time recreating the data they couldn't find. This time spent searching for and recreating data not found can add up quickly.

Some may also consider that 58 indexed file types covers the vast majority of email attachments one normally encounters, but in reality there are hundreds of different files currently types in use. The result is that one could miss the data needed in an Office 365 archive and end up in a risky eDiscovery situation. This indexing issue will be further discussed in the next section on eDiscovery.

Another issue that many will find troubling is the many limitations imposed by Microsoft on eDiscovery related searches (more detail is included in the eDiscovery Search and Indexing section below).

eDISCOVERY

Microsoft has made notable advances in its litigation/eDiscovery functionality with their Exchange-based solutions over the years. These additional eDiscovery capabilities coupled with free archiving in Office 365 have caused many organizations to want to forgo the expense of third-party solutions like email archives and advanced eDiscovery capabilities. In some circumstances, this strategy may make sense, but eDiscovery seldom follows the path of least resistance. A small lawsuit can

turn into a class action lawsuit quickly, taxing an organization's staff and systems beyond their breaking point. In these types of situations many attorneys have bemoaned the lack of technology, combined with a lack of time to respond to the eDiscovery order (and litigation hold) as their Achilles Heel. Those same attorneys agree that (proactive) litigation preparedness is the one area of the budget where no expense should be spared because just one lawsuit defense gone wrong can cost an organization many times the cost of proactive litigation preparedness. Because a lack of litigation preparedness/eDiscovery capabilities can be an extremely risky matter, let's look deeper into several notable Office 365 eDiscovery capability issues.

eDISCOVERY SEARCH AND INDEXING

As was discussed in the precious section on Productivity/Search, a potential eDiscovery issue lies with the number of attachment file types *not* indexed by Office 365. There are literally hundreds of file types currently in use, but Exchange is able to index only approximately 58 of them. This raises the question of how an organization finds those files not indexed by Exchange. It turns out there is a system command the eDiscovery administrator can run to list those files not indexed so that they can be exported from the system for further eDiscovery processing and review. The problem with this is that the eDiscovery administrator must remember to actually look for unindexed files during the search. This action will also drive up the cost of review by collecting files that may not be relevant to the case, but must be reviewed because they were not indexed.

More troublesome is the default timeout limit for Office 365 eDiscovery searches. Microsoft defines this default (set at 10 minutes) as *the number of minutes that an In-Place eDiscovery search will run before it times out*[vi]. In other words, unless the administrator changes this default as Office 365 is installed, a large eDiscovery search will error out if it takes more than 10 minutes.

Another issue around Office 365 index latency – the time it takes for new content to appear in the search index. Office 365 targets between 15 minutes and 1 hour for the time between upload and availability in search results[vii]. But several have reported up to a 24-hour lag in this time bringing eDiscovery search results for new content into question.

Yet another issue that many eDiscovery admins are not aware of is the problem of false positives of unindexed files. File properties, such as the filename, sent and received dates, sender and recipient, attachment file name, and text in the message body are all indexed and available to be searched. This capability could cause unindexed file attachments to have to be reviewed manually due to the fact that the email/attachment showed up in a set of search results. For example, a keyword search for intellectual property could return an email with an unindexed file attachment. That specific email and attachment would be included in the exported messages to be reviewed. That same email/attachment would also show up in a list of indexed messages and also be exported for manual review. This issue can complicate and drive up the cost of the review process if the attachment does not actually contain the keywords in question.

PROTECTION OF ARCHIVED CONTENT

Unlike most third-party archiving solutions, Office 365 does not by default protect items in the archive from tampering or alteration. This means that archived mailbox content cannot be classified as immutable, original content. Further, to protect archive mailbox content from alteration, the administrator must originate an In-Place Hold or Litigation Hold. Only from that point forward can the data be represented as unaltered.

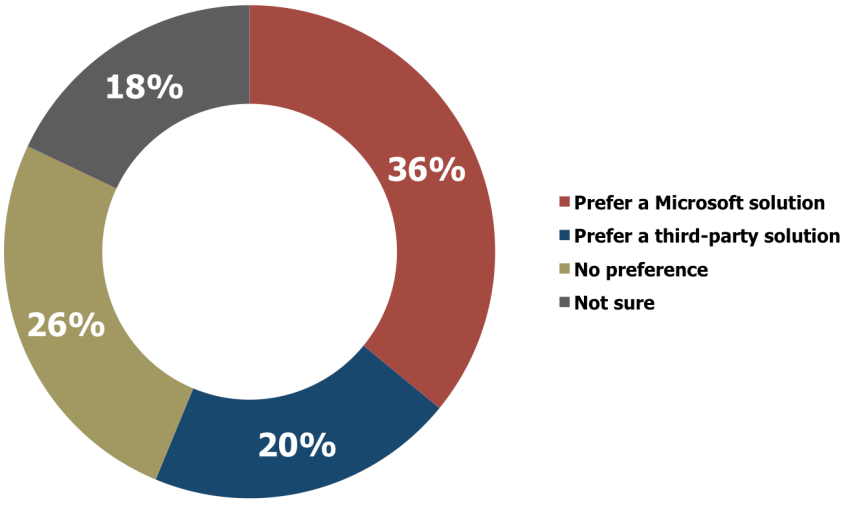
LONGEVITY OF ARCHIVED EMAIL

The immutability of archived email is an important aspect in eDiscovery, as well as regulatory investigations. On the eDiscovery side, the Federal Rules of Civil Procedure (FRCP) state that it is the responsibility of the discoveree to ensure potentially

relevant information is secured and protected from deletion or alteration as soon as litigation can be reasonably anticipated. This responsibility is the driving force behind litigation holds. If, after litigation hold *should have been applied*, evidence is altered or deleted, then a charge of spoliation can be raised and if found guilty (even if the act was inadvertent), various actions can be taken by the court, up to and including issuing and adverse inference instruction. This means that archived email does not have to be protected from alteration or deletion until a lawsuit is anticipated, but many assume they are. Unlike third-party archive solutions, Office 365 does not protect archived email from alterations by default. To ensure that all Office 365 archived email is protected as soon as they are archived, an In-Place hold must be applied as the archive mailbox is created.

The other situation that often arises is when an employee leaves the company. With the subscription-based Office 365, the departing employee's email box is often removed to save on monthly Office 365 subscription costs. In most third-party email archives, this action will not affect the employee's archived email or pricing of the archive. With Office 365, if an In-Place hold is not placed on a mailbox before it is deleted, the contents of the mailbox and the mailbox archive will not be preserved or discoverable. Microsoft refers to this action as designating an *Inactive Mailbox*[viii]. The deleted mailbox can be recovered within 30 days of deletion, but the mailbox and its contents will be permanently deleted after 30 days if it is not recovered. To complicate matters further, depending on the Office 365 subscription plan, to make a mailbox inactive (place an In-Place hold) an organization may need to up the subscription plan for that mailbox to a more expensive monthly plan.

Figure 4
Views on the Use of a Third-party Archiving Solution for Office 365



Source: Osterman Research, Inc.

SPECIALIZATION IN THIRD-PARTY EMAIL ARCHIVES IS A GOOD THING

The adoption of the cloud-based Office 365 by organizations to address the hassles and relieve administration costs of their office productivity tools will no doubt continue. The question many CIOs and general counsels are asking themselves is *do we still need to purchase a third-party email archiving solution if Office 365 already offers unlimited archiving functionality?* We have already addressed those areas of Office 365 archiving capability that fall short of the needed functionality for many organizations. A more important question they should ask themselves is; *what email*

archiving requirements do we have and does Office 365 archiving address them? The checklist of questions below should help to address the adequacy of Office 365 to meet an organization's email archiving requirements.

A checklist of issues for organizations to consider before fully relying on Office 365 Email Archiving:

- **Does your organization have other additional email systems besides Exchange?**
  Office 365 archives only Exchange-based email content, so if an organization has email systems other than Exchange because of corporate acquisitions or a long term transition strategy, then Office 365 will be only a partial solution and potentially drive up administration costs.

- **Has your organization ever been involved in eDiscovery?**
  Even though Microsoft has made great strides in adding basic eDiscovery functionality to Exchange Online and Office 365, it still falls short in functionality for those organizations that have moved some or all of their eDiscovery processes in-house to save money. Without the more advanced eDiscovery features many third-party email archiving solutions offer, the majority of the eDiscovery process will need to be handed off to outside counsel at a much higher cost.

- **Has your organization ever been involved in litigation where your email system was part of the collection/discovery process?**
  The email system is the most targeted data repository in eDiscovery. The ability to search across both the email system and email archive with advanced search capabilities and without limits (i.e., limits to search results size) can mean the difference between an incomplete or late discovery response and winning the case.

- **Have you had to restore email system backups for discovery response?**
  There are instances in which the immutability of data during discovery is a key topic. An email archive that is alterable (based on its default setting like Office 365) can be called into question and, if the data being put forth from the archive is in support of the discoveree, that evidence may be disallowed based on not being able to prove the originality of the email. Data restoration from an immutable source, such as a backup tape, is the only way to counter this argument. A third-party email archive that by default stores email content in an unalterable state can save an organization from these significant additional costs.
- **Does your organization want/need an absolute *copy of record* for all archived content?**
  As was mentioned in the previous checklist item, a copy of record can exist only in an unalterable repository. The Office 365 email archive is not an unalterable repository in its default state.

- **Has your organization taken more of the eDiscovery responsibility from your external counsel?**
  Many organizations have taken on more of the eDiscovery process responsibility to reduce their overall legal costs. Many of these organizations have relied on third-party archive capabilities to enable them to conduct content searches and place legal holds across their archives. Office 365 supplies some basic eDiscovery features but falls short in providing capabilities many have come to rely on. For example:

    - **The limitation of being able to search no more than 100 custodian mailboxes while responding to discovery.**
      Many eDiscovery searches focus on just a few custodians, but with larger and more complex lawsuits, the initial eDiscovery searches can span hundreds or thousands of custodian mailboxes. One of the most basic of eDiscovery processes during the collection process is the focusing in on

those custodians that, based on search queries, show the most potentially relevant content in results sets. For large queries, being able to view keyword statistics of the query is an important capability. One of the eDiscovery issues with Office 365 eDiscovery search is the limit of being able to provide keyword search statistics on 100 mailboxes or fewer. If more than 100 source mailboxes are included in the search, an error will be returned when you view the search keyword statistics. This limit on search statistics could force an organization to turn more of the collection process over to external counsel, sharply driving up the cost of eDiscovery[ix].

- **The limitation of only allowing two concurrent searches at a time.** Many organizations with large eDiscovery collection teams count on the ability to run many searches at a time against archives when responding to a large discovery encompassing many custodians. As well, many larger organizations provide access to other departments besides legal, such as HR, to conduct internal investigations. In large organizations, many search requests can be running concurrently. A notable limitation with Office 365 is that it has a maximum limit of running 2 concurrent searches at a time across the entire enterprise. This issue could prove to be a major bottleneck for many organizations.

  There are many more troubling eDiscovery native search limitations that you should be fully aware of before relying on the search capabilities of Office 365[x] for eDiscovery related searches.

- **The inability to search across more than 10,000 mailboxes in a single search.**
  An In-Place eDiscovery search is limited to a maximum of 10,000 mailboxes. Larger organizations will be forced to break the search into smaller groupings.

- **End-user search results limitation of 250 items.**
  By default, the Office 365 Outlook client is configured to return a maximum of 250 search items. This limit can be bypassed by configuring each individual Outlook client however many end-users would not expect a default limitation so would not know to change it so could be wasting time and money recreating data that actually exists but was not found.

- **Do you envision a need to export archived email in a file format other than .PST?**
  The default file format for email data in discovery is the .PST format. However, there are circumstances in which a different file format is needed. To respond to a regulatory information request, separate PDFs or .CAB files may be the format requested. The Office 365 In-Place eDiscovery search results are exportable only in the .PST format, causing at least one more, potentially costly, step to be included in the process of responding to an information request[xi].

- **As a part of litigation preparedness, does your organization archive (or keep an existing archive) of departing employees' email inbox content?**
  A best practice in both the HR and corporate legal communities is to capture and archive a departing employee's mailbox and other data based on the local statute of limitations in the event that the employee files a lawsuit at a later date. Office 365 does have a provision for creating this called Inactive Mailboxes. The inactive mailbox can remain on Office 365 indefinitely without any cost to an organization. However this capability is available only to Office 365 Enterprise subscription holders.

- **Does your organization use any non-Microsoft instant messaging platforms?**
  Office 365 archives only the Lync collaboration/instant messaging platform. For

organizations using one of the other popular instant messaging or collaboration platforms, a different third-party archiving solution will still need to be employed.

- **Does your organization use any non-Microsoft/non-standard work-place productivity applications?**
  As noted earlier, Office 365 is able to index (for search) approximately 58 different file formats. For those organizations that employ applications that produce a file format not included in these indexable file types, an employee search, a discovery search or regulatory search for content in an email attachment will not be recovered. This is an obvious risk in discovery and regulatory information response, as well as an employee productivity issue.

- **Does your organization have any regulatory data retention requirements?**
  For the vast majority of regulatory data retention requirements, email is considered a record, and so depending on the content of the email, may need to be kept for varying periods of time. Retention requirements, even in the same industry, can differ dramatically from email to email. This means that Office 365's email archiving retention lack of granularity will force all regulatory email to be kept for the longest period of time – otherwise known as a high water mark policy or rely on each employee to move each email to a custom folder and manually applying a custom retention tag. Reliance on individual employees' manual records retention practices have been deemed unreliable over the last several years.

- **Does your organization employ licensed brokers or traders subject to SEC and FINRA regulations?**
  Office 365 does not have a Journaled archive mailbox, so to meet SEC and FINRA requirements, a third-party email archive would be required. Office 365 also lacks mailbox-monitoring capability to meet the FINRA surveillance requirements that many third-party email archives do provide.

- **Has your organization been required to respond to a government agency information request in the last two years?**
  Much like eDiscovery requests, regulatory information requests can be fraught with risk and high cost without the ability to search and export required data quickly. Office 365 relies on its In-Place eDiscovery capability with the already noted inadequacies to respond to regulatory requests.

- **Does your organization need/want to manage archived email and attachments beyond *archive* and *delete* granularity?**
  Many organizations have moved beyond the keep it forever or delete it records retention policy. Organizations now want their archive automation to be able to make retention/disposition decisions at a more granular capability. Office 365 email archiving provides only for *delete it* or *archive it* records retention policies and instead relies on individual employees to manually drag and assign more granular retention policies.

- **Do you see a need to produce audit logs of archived mailbox activity?**
  Because Office 365 does not, by default, protect archived email data from deletion or alteration, the ability to produce audit activity reports on specific employee mailboxes would be a must have to be able to represent archived email as unaltered in legal and regulatory events. Office 365 provides for mailbox audit logging that allows customers to track access to the mailbox by people other than the mailbox owner, but does not audit mailbox owner activities.

Proponents of Office 365 email archiving claim that it addresses the majority of email archiving requirements that most organizations will face. That is not necessarily true. In fact, the limited functionality for litigation preparedness, retention disposition, and regulatory compliance highlight several areas where it falls short.

THE BENEFITS

A large proportion of organizations have some form of regulatory retention requirements. Add to that the rising levels of civil litigation, and the emergence of corporate information governance best practices, and it's obvious that most organizations will be better off with a third-party email archiving solution to meet their current and future email archiving requirements.

The main point of this white paper has been to ensure those organizations contemplating relying on the Office 365 archiving capability are aware of its limitations while also highlighting those areas that third-party archiving will continue to address. Third-party archiving benefits include:

- Flexibility of storage – A third-party archiving solution, whether on-premises or cloud-based, provides you the ability to choose and fine-tune your storage resources instead of needing to fit into a pre-determined subscription limitation.

- Granular retention/disposition of archived data – systematic retention/disposition policies provide for granular information management/regulatory compliance processes, including defensible disposition.

- Advanced search capability – ensures just those messages/attachments are returned in the results set reducing cost of review. No results sets limitation ensures ALL messages meeting the search criteria are returned.

- Granular legal holds – legal hold applied at the message level reduces risk and cost during the review process.

- Archive immutability by default – archived email can be considered a copy of record for regulatory and legal situations.

- Full audit/tracking of the archive – ensures the integrity and chain of custody of content and activities within the archive during eDiscovery.

- Choice of export formats – in many instances, an export format other than PST is required. The ability to export other than PST can save time and money.

The bottom line is third-party email archiving vendors are in the business of addressing a very specific set of user requirements. The above checklist points out those areas of email archiving that most organizations will want/need to insure are met. Those requirements include archive immutability, granular retention/disposition, offline access, mobile access, and a more powerful litigation hold/eDiscovery feature set.

Office 365 is a great cloud-based suite of office productivity capabilities, but was not designed as a complete compliance or eDiscovery archiving solution.

NOW WHAT – MIGRATING OUT OF OFFICE 365?

Moving email accounts from Exchange on-premises or third-party email archives to Office 365 has become a mainstream services offering from many migration vendors. However, based on the conclusions of this white paper, many organizations may realize that Office 365 archiving was not the panacea it was thought to be and so may want to move back to a third-party email archive. For those organizations, the question is *can we keep our Office 365 solution AND use a third-party to provide us with more powerful email archiving capabilities*? The answer is yes: an organization can migrate to Office 365 email archive and strengthen their compliance posture and search functionality by employing third-party email archiving with their Office 365.

SUMMARY

As has been pointed out several times in this white paper, Microsoft has made great advances in adding features/functionality to its market-leading solution for Exchange. The problem is that many organizations are relying on it to address potential regulatory and litigation requirements without first understanding what their requirements are and where Office 365 email archiving falls short. This lack of understanding will ultimately cause some organizations to wish they had researched their requirements and capabilities more thoroughly.

As organizations in general begin to adopt more inclusive information governance practices, the need for more powerful, cross-application, archiving and governance capabilities will become obvious. The industry is moving toward more centralized and more granular information governance automation, and third-party archiving solutions still offer the best, most cost effective way to meet these requirements while enhancing Office 365 capabilities.

SPONSOR OF THIS REPORT

With communications technology evolving and proliferating so quickly, you need to prepare for the future, today. Actiance, the foremost innovator in business communications management, allows you to unleash your business to better engage with customers and collaborate with colleagues. Our unrivalled portfolio of cloud services helps you reduce your eDiscovery costs and automate regulatory compliance so you can accelerate your organization's adoption of existing and new communication channels.

Your journey into the future starts with Alcatraz, the archive for the NEXT 10 years™. Alcatraz is the only archive built on the same elastic cloud technologies underlying today's most popular consumer applications. This unique architecture allows you to ingest, search and export information 10 times faster than with traditional archives. Alcatraz stores its content in a way that futureproofs the archive by allowing you to capture any type of communication that exists today, and is architected to accept other formats that are sure to exist in the future. It is the one and only ContextAware™ archive that presents social communications sequentially threaded in near-native format. This makes it a breeze to review conversations, in context, rather than trying to make sense of disconnected conversations stored as emails.

To meet your regulatory requirements beyond retention, Socialite and Vantage let you capture, control, and monitor email and all of your critical business communications. In addition, Vantage allows you to add disclaimers to outgoing messages, establish ethical walls and federate your communications with other organizations. Socialite also enhances your sellers' ability to engage in social selling by allowing them to work directly on social media websites or an iOS application to engage with their network and to share content from a library.

Actiance helps you manage Microsoft Exchange/O365, IBM Lotus Domino, and SMTP email as well as communications in the leading social media, unified communications, collaboration, and IM platforms provided by Facebook (FB), LinkedIn (LNKD), Twitter (TWTR), Google (GOOG), Yahoo! (YHOO), IBM (IBM), Jive (JIVE), Microsoft (MSFT), Cisco (CSCO) and Salesforce.com (CRM).

actiance®

www.actiance.com

@Actiance

info@actiance.com

+1 888 349 3223

REFERENCES

[i] Redmond, T. (July 31, 2014) *Office 365 by the numbers – an ever increasing trajectory*, retrieved from http://windowsitpro.com/blog/office-365-numbers-ever-increasing-trajectory

[ii] "Using Outlook Web App offline", retrieved from https://support.office.microsoft.com/en-us/article/Using-Outlook-Web-App-offline-3214839c-0604-4162-8a97-6856b4c27b36?CorrelationId=1b641b6d-3bfd-4333-acd7-7e36132b17cc&ui=en-US&rs=en-US&ad=US

[iii] (10/2011) "The Information Explosion: How Organizations are Dealing with it, retrieved from http://www.infoautoclassification.org/survey.php

[iv] (12/2012) "Defensible Disposition in Practice: Perspectives from Business and IT, retrieved from http://www.esg-global.com/research-reports/defensible-disposition-in-practice-perspectives-from-business-and-it/

[v] (03/21/2014) "File Formats Indexed by Exchange Search, Retrieved from https://technet.microsoft.com/en-US/library/ee633485%28v=exchg.150%29.aspx

[vi] "In-Place eDiscovery", retrieved from https://technet.microsoft.com/en-us/library/dd298021(v=exchg.150).aspx#throttle

[vii] "SharePoint/Office 365 Search Results Freshness Delay After Mapping Managed Property to Crawled Property" retrieved from: http://community.office365.com/en-us/f/148/t/277654.aspx

[viii] (01/07/2015) Manage inactive mailboxes in Exchange Online, retrieved from: https://technet.microsoft.com/en-us/library/dn144876%28v=exchg.150%29.aspx

[ix] (8/18/2014) Search limits for In-Place eDiscovery in Exchange Online, retrieved from https://msdn.microsoft.com/en-us/office/dn798915%28v=exchg.149%29.aspx

[x] "Message properties and search operators for In-Place eDiscovery" retrieved from https://technet.microsoft.com/en-us/library/dn774955(v=exchg.150).aspx

[xi] (4/25/2014) Export eDiscovery search results to a PST file, retrieved from https://technet.microsoft.com/en-us/library/dn440164%28v=exchg.150%29.aspx