Osterman Research

WHITE PAPER

White Paper by Osterman Research
Published **December 2019**
Sponsored by **Zix**

The Importance of Doing Email Migrations the Right Way

Executive Summary

Migrating an organization's email and/or archiving systems to Office 365, Exchange Online, Google G Suite or some other email, collaboration or archiving platform is not an easy thing to accomplish. There are a number of critical decisions to make in advance of migrating to a new platform, and the migration process itself requires careful planning and execution over an extended period in order to avoid data corruption, lost chain-of-custody for sensitive data, and ensuring a minimal impact on employee productivity. There is a sequence of activities that must be scoped, agreed upon, and carried out properly in order for the migration to be successful. Aligned with the activities in the migration process are a range of third-party products and services that can simplify and streamline the migration process, improving the end result, while decreasing the risk of human error during the process.

KEY TAKEAWAYS

Here are the key takeaways from this paper:

- Organizations are choosing to migrate to new platforms for a variety of reasons, including improvements in cyber security capabilities, improving communication, managing corporate records more effectively, enabling better user productivity, and streamlining the cost of IT operations.
- Adoption of Office 365 is one of the primary drivers for undertaking a migration project. Given that more than 200 million users have adopted and/or been migrated to the platform, migration to the Office 365/Exchange Online has been one of the most common migration projects over the past several years.
- Migration can be difficult and involves a significant number of detailed steps for the planning, execution and management of the overall project. Nearly one-half of those surveyed for this white paper view the need to keep everything up and running during the migration as the most challenging aspect of a migration.
- On-premises archiving systems are being migrated to cloud-based solutions: our research shows that while slightly less than one-half of content is archived on-premises in 2019, this figure will jump to nearly two-thirds of archived content in just two years.
- The use of third-party consulting services and migration tools is essential for most migration projects given the difficulty of migration efforts, the general lack of expertise about the nuances involved in accomplishing a migration successfully, and the serious consequences of getting things wrong.

The use of third-party consulting services and migration tools is essential for most migration projects given the difficulty of migration efforts.

ABOUT THIS WHITE PAPER

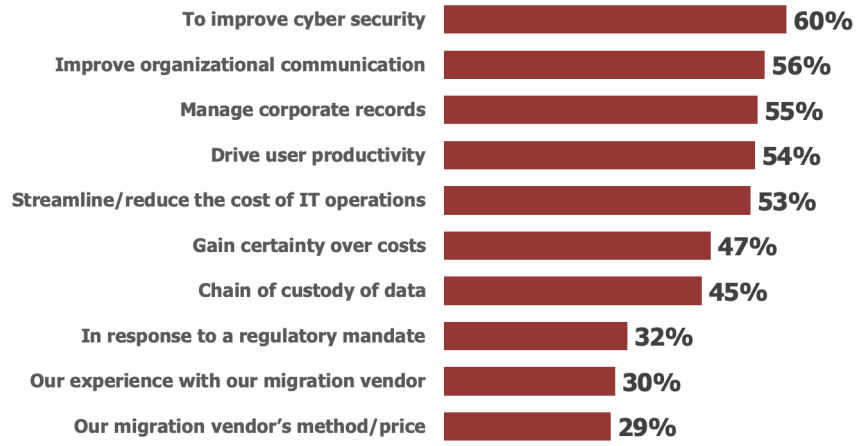
This white paper was sponsored by Zix; information about the company is provided at the end of the paper.

A Guide to Migration

WHY DO ORGANIZATIONS MIGRATE TO NEW SOLUTIONS?

There are numerous reasons that organizations migrate to a new platform, as shown in Figure 1. However, the most commonly cited reasons are to improve cyber security, to improve organizational communication (which is one of the key reasons that organizations are migrating to Office 365), to manage corporate records more effectively (a key driver for the migration to cloud-based archiving), to improve user productivity, and to reduce the cost of IT operations (again, a key driver for the migration to Office 365).

Figure 1
Drivers for the Decision to Migrate
Percentage Responding an "Important" or "Extremely Important" Driver



Source: Osterman Research, Inc.

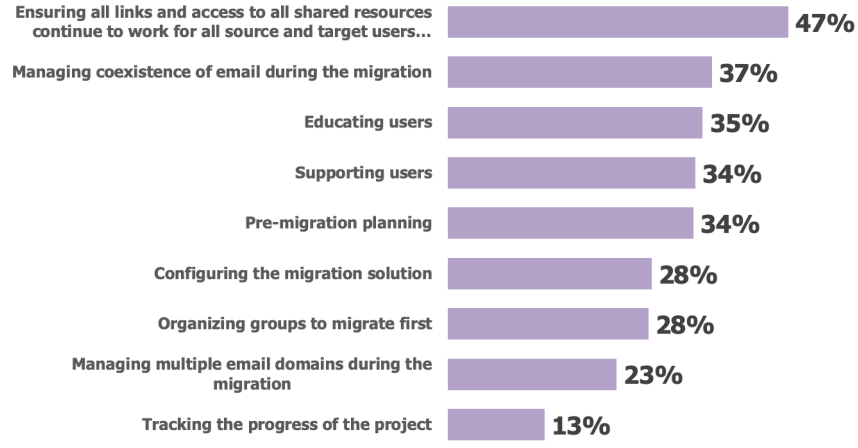
MIGRATION IS NOT FOR THE FAINT OF HEART

Virtually every organization, because of their current on-premises or cloud infrastructure, established business processes, and historical data faces a major planning exercise in evaluating the shift to any new communication, collaboration or archiving platform. This includes a significant set of discrete tasks in actually performing the migration. There are numerous critical decisions to make while planning the migration, including how to achieve value from doing so, the approach to take, whether to involve third parties, and the selection of third-party migration tools.

As shown in Figure 2, the most difficult part of a migration is considered to be ensuring that everything continues to work properly while the migration is underway, as shown in Figure Q16. Not unrelated is the second most difficult aspect, managing the coexistence of email during the migration, followed by educating users, supporting users and pre-migration planning.

The most difficult part of a migration is considered to be ensuring that everything continues to work properly while the migration is underway.

Figure 2
Views on the Most Difficult Part of a Migration
Percentage Responding Difficult or Extremely Difficult



Source: Osterman Research, Inc.

THE RIGHT TOOLS ARE ESSENTIAL

The process of the migration itself requires the right mindset, approach, and a set of technical skills, tools, and experiences that are not always readily available among an organization's current IT professionals. Moreover, some firms migrating their email, archive and other systems have discovered that these skills are lacking even among some third parties. However, getting it right is essential: if the migration process doesn't work smoothly, there can be a number of consequences:

- Employees won't have the ability to read and respond to email, schedule meetings and book resources.
- Assistants and other proxies won't be able to manage their managers' calendar.
- Even more critically, chain-of-custody for critical information can be lost, rendering it useless for eDiscovery or regulatory compliance.

WHAT NEEDS TO BE DONE PRIOR TO MIGRATION?c

Achieving a smooth migration can be fairly straightforward once all of the planning work has been accomplished. In fact, most organizations will spend more time planning their migration than actually accomplishing it. Here are the key tasks to consider in checking the current environment and developing a plan for migration:

- **Determining if all content needs to be migrated**
  In many migration efforts, organizations will leave content behind as the cost and complexity is simply not worth it, especially for content with a short life span. As part of the early stages of a migration, stakeholders should determine what content should and should not be migrated.

- **Determine bandwidth availability**
  One of the most common migration efforts underway today is migrating from on-premises email to cloud-based email (usually Office 365), or from on-premises archiving to cloud-based archiving. Migrating to a new email, collaboration or archiving solution can be a bandwidth-intensive task in these situations, as hundreds of gigabytes or even terabytes of data are shifted from on-premises servers to the cloud. Planners must check that there is sufficient bandwidth available for the migration, and explore alternatives for moving current and historical data without using an Internet connection. For example, Microsoft offers the option of delivering data on hard disks directly to Microsoft for upload into the customer's account at an Office 365 data center, and some third-party migration tools support faster upload to Office 365 by moving data into Azure first. Amazon uses its "Snowball" technology, consisting of on-site, physical storage to which customers can transfer their data for delivery to an Amazon data center; for very large data transfers, Amazon will send a tractor-trailer to a customer's site to transfer multiple petabytes of data.

  It's important to note that, at least in the case of Microsoft, there are data throttling approaches in place that limit the amount of data an organization can upload each day, so a bigger pipe is unlikely to unilaterally solve the problem.

- **Review bandwidth design**
  Satellite and other remote offices with low bandwidth connections can cause problems in migrating to new platforms because of the length of time required to move data across the Internet. Understand what is in place currently across the organization, and determine whether a higher bandwidth connection is required during and after the migration for remote locations.

  Good bandwidth design for the entire organization is worth revisiting, as well, if key business processes and applications will be moved to the cloud. If an organization does not currently have redundant network links, it might be worth introducing those to ensure reliability.

Achieving a smooth migration can be fairly straightforward once all of the planning work has been accomplished.

- **Assess the health of Active Directory**
  Osterman Research surveys have found that about a quarter of all mid-sized and large organizations that are migrating to Office 365 will maintain hybrid deployments indefinitely. A hybrid Office 365/Exchange deployment will require highly reliable interaction between Active Directory and Azure Active Directory. As a result, it's essential to determine the current health of the Active Directory setup and resolve any issues before the migration starts.

- **Assess the health of Exchange Server**
  Prior to migrating from on-premises Exchange to Office 365, it's important to check the health of the current Exchange Server infrastructure. Any corruption, configuration problems or other issues can either degrade the migration experience or could be made worse after migrating to Exchange Online.

  For organizations shifting from a non-Exchange environment, such as IBM Notes/Domino or Micro Focus GroupWise, it's also important to ensure that the current system has sufficient integrity to handle the demands of the pending migration.

- **Assess the health of SharePoint Server**
  Microsoft SharePoint is a complex product, and so organizations that have taken advantage of its custom development capabilities are very likely to need to re-think their approach to SharePoint when embracing SharePoint Online. For example, they will need to consider how they have used customizations and other design approaches that work on-premises, but are unsupported on SharePoint Online.

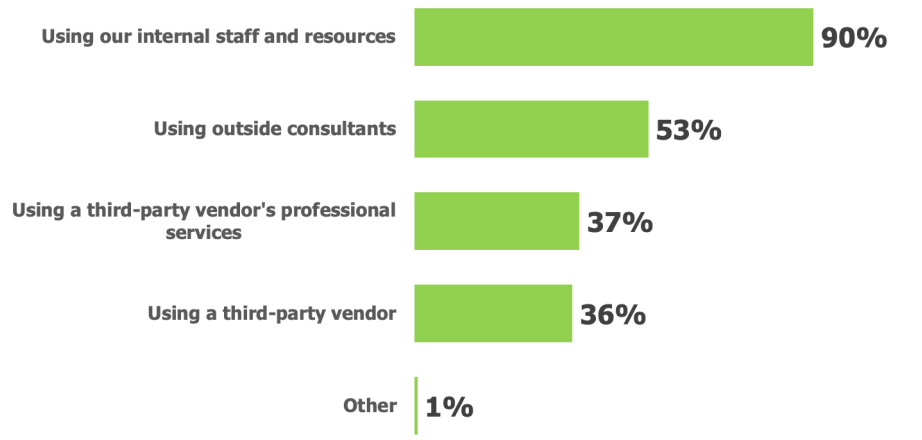
- **Determine dependencies that exist with key applications**
  Determine which applications and systems rely upon or work alongside the existing environment. If an organization is going to change its approach to Exchange by embracing Exchange Online, it will need to undertake remedial work to re-connect other systems. For example, on-premises archiving systems that work with the on-premises environment may need to be updated or replaced. Organizations that are migrating from IBM Notes/Domino for email are likely to have mail-enabled and workflow-enabled Notes applications that need to be redesigned. CRM systems that integrate with existing solutions may need different integration capabilities. Scanners and multi-function machines that send scanned documents through the email or collaboration system will need a rethink.

- **Do in-house IT staff have the requisite skills for migration?**
  Organizations undertaking a migration will need to determine if the skills of their IT staff are adequate, including their ability to backup and archive all relevant content. While some organizations have IT staff who have been doing email migrations for a long time, most are not in such a position, since migration is not a task that occurs frequently enough in most organizations to build a robust skill set among IT employees. Most will need to bolster their IT staff skill with the technical assistance of an external IT consulting firm.

  That said, the vast majority of organizations still rely heavily on their internal staff members to prepare for a migration and implement new solutions, as shown in Figure 3. However, a majority of organizations also use outside consultants, while more than one-third use third-party vendors and their professional services to assist in the planning and migration efforts.

Organizations undertaking a migration will need to determine if the skills of their IT staff are adequate.

Figure 3
Methods Used for Preparing for Migration and Implementation



Source: Osterman Research, Inc.

In selecting a third party for the migration, it's important to ensure that they have specific expertise in migrations featuring the same setup and constraints in place in the organization that is to become their customer. It's also essential to ensure that existing backup and archiving routines are not interrupted during the migration given the essential nature of both best practices.

It's important to note that moving from on-premises infrastructure to the cloud does not render IT staff irrelevant and unnecessary. Instead, it simply changes the kinds of work that they do. It's key to determine the retraining required to make sure that current staff can manage new cloud services, or in conjunction with on-premises infrastructure in a hybrid deployment. New administration and management tools often streamline the execution of these tasks over time too, and these are worthy of evaluation.

If organizations move forward with a hybrid approach, that by itself will create its own set of challenges. These tasks must be managed actively to avoid downstream troubles. For example, there are specific versioning requirements for Exchange Server on-premises in order to work in a hybrid configuration with Exchange Online. Ensure that all necessary processes are established to test, deploy, and manage the ongoing update stream.

Understanding compliance requirements, particularly in light of newer requirements like the GDPR or the CCPA, is an essential element of a migration effort.

- **Assess staff knowledge about the new platforms**
  IT, security and other staff members will need to be trained on the new platforms, and so determining the appropriate training resources as part of the migration planning effort is key to enabling a smooth transition to the new platform(s).

- **Understanding compliance requirements is key**
  Understanding compliance requirements, particularly in light of newer requirements like the General Protection Data Regulation (GDPR) or the California Consumer Privacy Act (CCPA), is an essential element of a migration effort. For example:

  - How will an organization manage its email archives? Move them to the new platform (e.g., native archiving in Office 365), move them to a cloud archiving solution, leave them on-premises, leave legacy data on-premises and begin archiving cloud content in the cloud, etc. If moving archives somewhere else is determined to be the best approach, decision makers will

need to plan how to migrate data without breaking chain-of-custody or violating the integrity of the data owners' privacy, which are by no means trivial issues.

- If encrypted data is moved, how will this be accomplished without breaking the current encryption safeguards?
- The need for data to be physically stored within specific geographical areas, in compliance with data sovereignty legislation, is a key decision point for many organizations. This may dictate where to establish a single tenant, or push an organization in the direction of multiple, cooperating tenants.

Organizations that do not have specific compliance requirements (and there aren't many of them) can move faster and more easily to new platforms.cThose with heavy compliance mandates need a solid approach to ensure their organization isn't opened to the legal risks and financial fallout that can accompany a poorly executed migration.

- **Developing a migration plan is key**
  After establishing a solid understanding of the current state of the IT and security infrastructure, the business goals that the organization hopes to accomplish from the migration, and the way in which the new platform will be leveraged, decision makers need to develop a migration plan. This plan should include:
  - How the migration will be conducted in phases, especially the order in which departments and divisions will migrate to the new platform. Phasing will need to be coordinated for some users in order to make sure they have uninterrupted delegate access for mailboxes and calendars.
  - The third-party IT consultants and the internal staff members who will be performing the migration duties.
  - The timeframes for consulting with all relevant stakeholders, such as business and content owners, about content deletion, archiving, and migration.
  - The features and functions in the new platform that will be made available to employees over set timeframes. For example, if an organization is migrating to Office 365, which plans will be adopted for which users? One of the benefits of Office 365 is the ability to "rightsize" plans for different users so that costs can be minimized.
  - As a corollary to the point above, determine which third party solutions will be used with the new platform.
  - Can the organization respond to a legal discovery request or a regulatory audit during the migration? That's a distinct possibility, especially for larger organizations, and so a plan to do so must be part of the migration effort.
- **Develop a solid backup and recovery plan**
  Some solutions, such as Office 365, do not offer the more traditional concept of backing up servers and data at a point in time so that administrators can enable recovery or roll-back under disaster scenarios, the ability to recover individual files, or data over longer periods than is available by default. Many third-party vendors offer backup and recovery services that are much better, adding an essential level for the management of corporate data.
- **Develop a continuity plan**
  Cloud services like Office 365 are usually quite reliable and suffer few system-wide outages, but they do have fairly frequent localized outages. These render

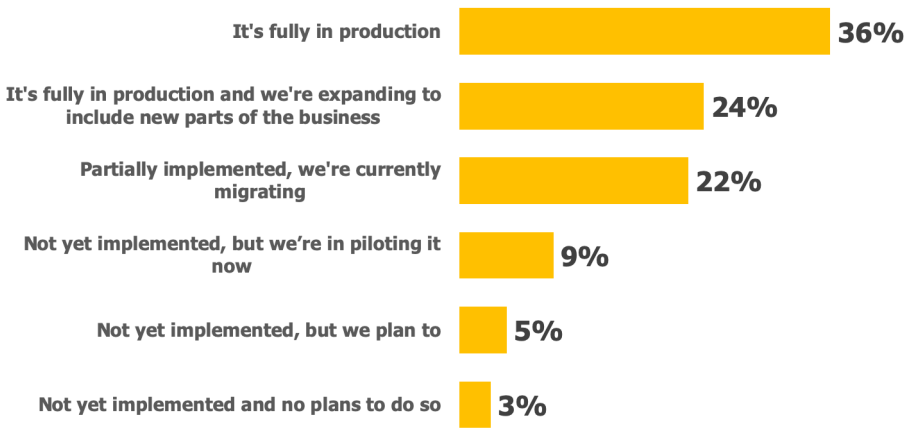
Those with heavy compliance mandates need a solid approach to ensure their organization isn't opened to the legal risks and financial fallout that can accompany a poorly executed migration.

staff members unable to do their work, and so a continuity plan should be established, supported by the appropriate technologies to ensure that employees can keep working during outages.

MIGRATING TO EXCHANGE ONLINE

This white paper discusses migration in a way that is applicable to any communication, collaboration or archiving solution, but discusses migration to Office 365 in particular because such a large proportion of migrations involve a move to Office 365. As shown in Figure Q6, the vast majority of mid-size and large organizations in North America have either migrated some or all of their users to Office 365, they are in the process of doing so, or they are planning to do so.

Figure Q6
Current Status of Implementation for Office 365



Source: Osterman Research, Inc.

A migration to Exchange Online can be an involved process, requiring a set of coordinated activities over several weeks or months (or longer, depending on the size of the organization and the volume of mailboxes and data to migrate). Staff members will need to:

- **Verify the connectivity to Exchange**
  It's essential to verify connectivity from Exchange Online to the on-premises infrastructure. For migrations from on-premises Exchange (a very common scenario) Microsoft offers a tool to ensure that connectivity is enabled and configured properly.

- **Run a pilot of the migration**
  Staff members should test the efficacy of the preferred migration option by first migrating test accounts and mailboxes, followed by a small number of actual user mailboxes. Once some of these actual mailboxes have been migrated to Exchange Online successfully, it is good to stop for a couple of weeks to see if any issues come up. If that's the case, it's easier to resolve any issues for a small number of mailboxes instead of trying to rein in the issues across a much larger number of them. Third-party backup tools can assist with a pilot migration.

- **Select the appropriate migration option**
  IT staff should select the migration option that makes most sense for their organization. These options include Cutover Migration (for smaller organizations that want to migrate all at once to Exchange Online), IMAP migration (for moving only messaging data from IMAP servers to Exchange Online), or a hybrid approach that enables coexistence between on-premises Exchange and

A migration to Exchange Online can be an involved process, requiring a set of coordinated activities over several weeks or months.

Exchange Online. This can be for the duration of just the migration itself, or as a long-term strategy to optimize between the two approaches of providing Exchange services to organizations.

- **Sync Active Directory and assign licenses properly**
  Organizations that are opting for a hybrid approach need to synchronize Active Directory with Azure Active Directory because it creates the users in Office 365. Once they have been created, Office 365 licenses can be assigned. It's helpful to implement third-party backup capabilities prior to moving data.

- **Migrate active user mailboxes**
  At this point, IT staff can migrate active user mailboxes in light of available bandwidth and the data throttling that Microsoft applies to migration activities. Many organizations will migrate just a couple of hundred mailboxes to migrate each night to stay within these limits. Once each mailbox has been migrated, Exchange settings should be updated so that Outlook will automatically discover the new, cloud-based mailbox.

- **Consider how to manage unused mailboxes**
  It's common to have unused mailboxes on the Exchange Server that still contain important information, but for which users have long since left the company. Exchange Online uses inactive mailboxes to support this situation. If a mailbox needs to be moved for legal or compliance reasons, a user account can be created for each mailbox: attach the two, leave the account to sync to Azure AD, assign an Exchange Online license, migrate the unused mailbox to Exchange Online, place the mailbox on legal hold, and then delete the user account. The user account will be deleted, the license freed up for future use, and the mailbox data held until the hold is removed.

MIGRATING PST FILES

Organizations that maintain PST files will need to determine what information should be migrated into Exchange Online. This requires an analysis of content inside of these files to identify data that might be subject to compliance requirements, a task in which legal and compliance teams will need to be involved.cThird-party vendors offer tools that greatly streamline and simply the processing, analysis, and migration of the right data into Exchange Online or an archive.

MIGRATING TO ONEDRIVE FOR BUSINESS

OneDrive for Business is the Office 365 venue for files and documents, and it provides users with a cloud storage solution that can synchronize to various devices, while at the same time giving IT administrative oversight of these files. While there are numerous file sync and share solutions in use across most enterprises, OneDrive should seriously be considered because it offers the dual benefit of robust file sync and share with IT management of data, something lacking in many solutions currently in use. File shares, data on corporate desktop and laptop computers, and other devices need to be migrated from their current locations into OneDrive for Business or another new location within Office 365.

Migrating Archives

Migration projects often the movement and conversion of data between computers, applications, storage devices and/or formats. There are many reasons that trigger the need for an archive migration, including a move to the cloud, a need to improve litigation support capabilities, a data center move or consolidation, an upgrade to a more efficient archive and storage technology, archive obsolescence, and several other reasons.

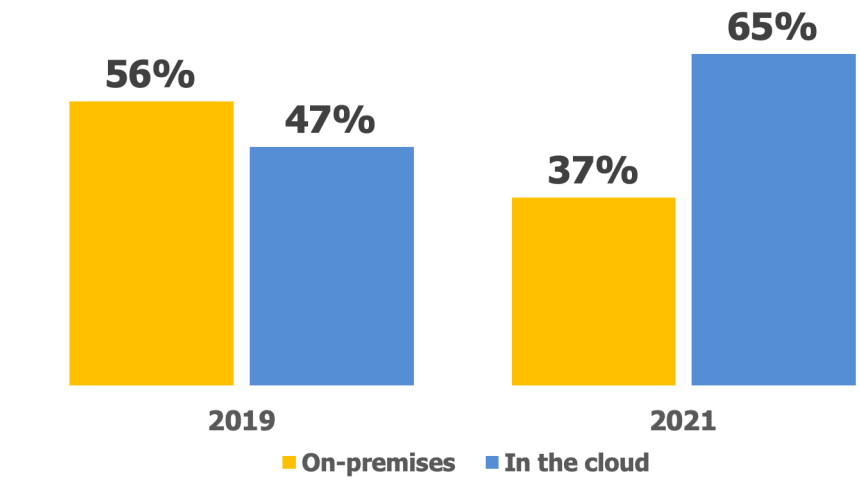
The process of migrating a long-standing repository, such as a legacy email archive is not an enviable one, since there are numerous places for things to go wrong and

Third-party vendors offer tools that greatly streamline and simply the processing, analysis, and migration of the right data into Exchange Online or an archive.

corrupt, delete or otherwise render unusable years' worth of critical corporate data. Consequently, the appropriate effort and time should be devoted to fully evaluating, culling, and cleaning up archived data before the migration. This includes defensibly deleting content that is no longer needed.

While most archived content today is on-premises, our research shows that content is decidedly shifting to the cloud, and so archive migration is a top-of-mind issue for many decision makers. As shown in Figure Q22-23, 47 percent of archived content is stored in the cloud today, but this is expected to increase to 65 percent over just the next two years.

Figure Q22-23
Percentage of Content Archived On-Premises and in the Cloud
2019 and 2021



Source: Osterman Research, Inc.

While most archived content today is on-premises, our research shows that content is decidedly shifting to the cloud.

Archive migration can be challenging, difficult and risky. If an organization decides to move its email archives from their current location, either on-premises or in the cloud, maintaining chain-of-custody is essential. This means migrating the data within the archives in such a way that data integrity is not compromised, since this could lead to legal and regulatory repercussions. Given that archives typically contain many years' worth of data, they can represent a much larger amount of data than the email in current day-to-day Exchange mailboxes, and so losing chain-of-custody or otherwise compromising the integrity of this data can have bigger ramifications. Managing the migration of this data volume has to be incorporated into the overall plan so as to avoid migration delays.

While the migration is underway, IT staff must be aware of mailbox size limits in Exchange Online and ensure that the archived data is migrated to the user's archive, not their mailbox. Moreover, IT staff must be careful with managing stubs to avoid broken links, they must manage journal data appropriately, and they must manage data on legal hold properly.

CONSOLIDATING ARCHIVES

Some organizations will have multiple, incompatible legacy archives that might including an email archive, a file system archive and a content management solution. Having multiple archives increases costs, increases legal hold and eDiscovery risk, and it reduces overall productivity. Consolidation of archives into a single, higher performance archive can produce a positive return on investment (ROI) based on having a single repository of content to search and, in the case of on-premises archiving solutions, fewer hardware and software support costs.

Archive consolidation also occurs following corporate mergers or acquisitions. When companies with existing archives are merged with another with the same or different archiving solutions, consolidating the disparate archives into a single platform provides better ROI and more efficient regulatory compliance and eDiscovery because there are fewer resources to search.

UPGRADING TO A BETTER ARCHIVING SOLUTION

Over time, archiving solutions become outdated for various reasons. Legacy archiving systems are often a barrier to benefiting from new archiving capabilities, particularly those available in the cloud:

- **Migrating to improve scalability**
  The importance of scalability is often underestimated. Many customers of legacy archiving solutions have found out too late that their archiving vendor's promise of unlimited scalability and performance has fallen short. In many instances, these scalability shortcomings have come about as the volume of data has increased faster than expected, thereby increasing the amount of content archived; or they were faced with a particularly large eDiscovery requirement and found that searches were taking far too long to complete. These situations can place the organization at risk and dramatically increase costs. The only option is to move to a higher performance archive that has room to grow.

- **Migrating to improve search performance**
  Many legacy archiving solutions rely on inadequate indexing and search technology. As archived data sets become larger, search response times become much slower. Consequently, the only sure way to address the problem is to upgrade to a higher performance archiving solution. An integral part of this upgrade process is the migration of the existing archive data set in such a way that takes advantage of the new system capabilities with the existing archived data set.

- **Migrating to a cloud-based archive**
  Archiving in the cloud is a viable alternative to on-premises archiving solutions. A cloud archive can offer an optimized storage solution for long-term retention in conjunction with other cloud managed services, such as more advanced access security and more efficient litigation support services. The cost savings of cloud archiving versus on-premises archiving can be significant when the up-front costs of hardware, software, additional experienced IT staff, and annual support are taken into consideration. Because of these differentiators, many organizations are moving their archiving requirements to the cloud, either for new content only or for migration of existing archives.

- **Migrating to archive new data types**
  Since the early days of archiving that were focused just on email, many new data types have been introduced that also should be archived, such as text messages, social media posts, collaboration system content, voice content and the like. Many of these newer content types can be cross-connected and benefit from systematic grouping, much like being able to automatically construct an email conversation thread in the past. Obviously, older archiving solutions were not able to address different and unknown data formats and normally were targeted at one specific platform, such as email. Organizations are moving to more format-inclusive archiving systems and so are considering the migration of older archives into the new solutions to enable more expansive information capabilities.

Archiving in the cloud is a viable alternative to on-premises archiving solutions.

Other Considerations

RETIRING APPLICATIONS

Applications that are obsolete or unused, but yet remain active in an organization's infrastructure, can be a significant resource drain when including hardware and annual hardware support costs, annual software support contracts, and the additional staffing needed to service the applications. This situation is even more challenging when the underlying technology, such as Windows XP and previous versions of Exchange, reach end-of-life.

When considering retiring an application, the existing data generated by the application must be properly managed, particularly in the context of the legal and regulatory support requirements. If any data in the application repository continues to within the regulatory retention period or might be relevant to a legal action, then that data must be retained, migrated and secured. Once the regulatory and legal issues have been resolved, the data's business value should be considered. In many situations, much of the data might still be of value to the organization and so should be migrated to another repository for long-term retention.

CONSOLIDATING STORAGE

Storage solutions that get older and are not as efficient as newer generation storage solutions should be replaced with higher capacity and more technically advanced storage devices, such as swapping conventional hard disk storage for solid-state storage. Storage consolidation can reduce the number of devices that must be managed, reduce support costs, and it can increase overall system performance. When beginning a storage consolidation project, migrating the existing data to the new storage solution requires a carefully planned data migration. Once the data migration is complete and verified, old storage resources can be retired or repurposed.

Using Third-Party Tools

Organizations that migrate to Office 365 and other, newer solutions should evaluate the use of third-party tools that can improve their experience. Some of these solutions include:

- **Searching for problems**
  Tools that evaluate the current environment for metadata consistency; permissions that have been incorrectly assigned; incorrect user names; users who have left the firm who still have access to corporate resources; incompatibilities with other software, and disallowed file types, names, or sizes; and other issues should be considered.

- **Tools to simply migration activities**
  Tools that streamline the process of migrating from on-premises servers to cloud-based services can be useful, such as those that provide one-hop migration from a legacy Exchange Server environment to Exchange Online, without having to upgrade to a later version of Exchange Server first. Similarly, tools that enable migration from on-premises SharePoint and other content sources to SharePoint Online or OneDrive for Business, while maintaining full metadata integrity, can save lots of headaches. Some tools support the re-arranging of content structures during the migration process, scheduling migration activities to optimize available bandwidth, and automating staff communications about pending migration activities.

- **Tools to ensure continuity**
  As noted earlier, capabilities that enable continuity during outages are an essential element for any communication or collaboration system, but they can also provide value during the migration process itself. Ensuring that users

Organizations that migrate to Office 365 and other, newer solutions should evaluate the use of third-party tools that can improve their experience.

continue to have access to their email and other data resources during a migration can improve employee productivity and mitigate at least some of the risks associated with migration problems.

- **Tools to help address compliance obligations**
  Tools to improve the compliance capabilities in Office 365 and other platforms can be useful if they strengthen the native encryption, data loss protection and archiving capabilities in these platforms. For example, the use of third-party encryption can make data more secure by encrypting data before it reaches Microsoft's data centers. In the event that a data center is breached, or if the cloud provider is subpoenaed by a government, customer data will still be protected.

Summary

Migrations from one communications or collaboration platform to another, or from one archiving solution to another, can be arduous and fraught with difficulty. They can be all the more complicated when a paradigm shift is involved, such as migrating from on-premises infrastructure to cloud-based solutions. However, with the right planning, expertise and partners, migration can be as painless as possible, helping organizations to achieve the business value they seek from moving to new and better platforms.

Sponsor of This White Paper

To better meet your company's security, data protection and compliance needs, Zix can enhance your Office 365 environment with advanced threat protection, archiving and email encryption. Zix delivers a superior experience and easy-to-use solutions that have earned the trust of more than 19,000 organizations including the nation's most influential institutions in healthcare, finance and government.

To defend your company from malware, ransomware, phishing and other email threats, ZixProtect combines a multi-layer email security approach with automated traffic analysis, machine learning and real-time threat analysts. In addition, ZixProtect's business continuity feature ensures that your organization can continue to communicate if your email experiences a disruption.

ZixArchive eases email archiving and eDiscovery with automatic email collection and storage in a secure cloud. Its automatic indexing and multiple search criteria gives you and your employees convenient and rapid access to archived emails. ZixArchive also enables you to share an email hold with outside legal counsel and auditors and revoke privileges when access is no longer needed, keeping your data within your control.

To ease email encryption for you, your employees and your recipients, leverage the industry's leading solution ZixEncrypt. Automatic transparent delivery between customers and robust delivery methods for other recipients enables easy access to encrypted email for anyone, anywhere and on any device, making the user experience exceptional and compliance simpler. Proven policies and advanced reporting provide peace of mind, while customizable branding and security capabilities make email encryption fit your unique company needs.

Leveraging our more than 15 years of hosted experience, you can have confidence that Zix email security solutions integrate seamlessly with Office 365. You also benefit from the support of the ZixData Center, a state-of-the-art facility with PCI DSS 3.2 certification, SOC2 accreditation and SOC3 certification. Staffed 24/7/365, ZixData Center has a track record of consistent 99.999% availability. In addition, Zix delivers exceptional customer support 24/7/365 no matter your questions or concerns.

www.zixcorp.com
@ZixCorp
+1 866 257 4949
sales@zixcorp.com

With reliability, experience and superior support, Zix improves email security for your Office 365 environment. To learn more about our solutions for Office 365, visit www.zixcorp.com/office365.