WHITE PAPER

The Role of Third-Party Tools for Office 365™ Compliance

An Osterman Research White Paper

Published June 2015

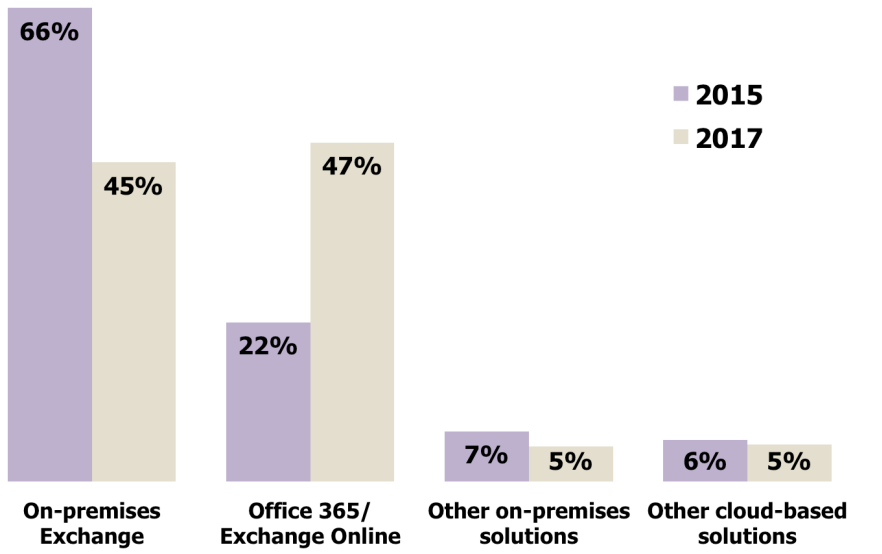
mimecast
unified email management

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

Microsoft Office 365 is a robust cloud-based offering that includes email, telephony, instant messaging, online storage, file-sharing, social media and other services delivered through a variety of subscription packages for organizations of all sizes. Office 365 is arguably the most successful of the various business-grade, cloud-based communications and collaboration services currently available. Figure 1 shows considerable current deployment of Office 365, with adoption expected to more than double by mid-2017.

Figure 1
Users of Various Email Platforms, 2015 and 2017



Source: Osterman Research, Inc.

THE CRITICAL ROLE OF COMPLIANCE

Compliance-related issues – whether driven by statutory regulations or legal precedent – are a critical consideration for organizational initiatives aimed at managing electronic communications and collaboration systems. Organizations must:

- Retain email and other communications for specific periods of time.
- Prevent business records from being modified after they are archived.
- Ensure that this content is protected from data breaches of various types.
- Ensure that this content is protected from user actions on mobile devices.
- Ensure that content is encrypted during both transmission and in storage.
- Ensure that they can produce required information quickly and accurately.
- Have the ability to conduct systematic supervision to reduce risk.

In short, organizations must be able to manage information in such a way that regulatory and legal obligations are satisfied and corporate risk is minimized, and they must do so within the confines of their budget restrictions.

Despite the growing dominance of Office 365 as a communications and collaboration service, as well as the useful features and functions it offers, it has significant limitations with respect to compliance. As with any cloud-based offering, these limitations will necessitate the use of third-party compliance capabilities in order for organizations to fully satisfy their regulatory and legal compliance obligations. This

white paper explores the limitations in Office 365, and points to third-party offerings that enable organizations to meet their compliance obligations.

ABOUT THIS WHITE PAPER

The need for this white paper is highlighted by a key finding from the survey conducted for it: only 25% of those surveyed consider themselves "fairly" or "very" knowledgeable about the compliance capabilities built into Exchange Online and the other elements of Office 365. Consequently, this white paper focuses on the need for compliance with the growing variety of industry-specific regulations and legal obligations that organizations face, as well as specific compliance issues that will be of concern to corporate decision makers in evaluating the use of Office 365. Also offered is an overview of Mimecast, the sponsor of this white paper, and their compliance-related offerings.

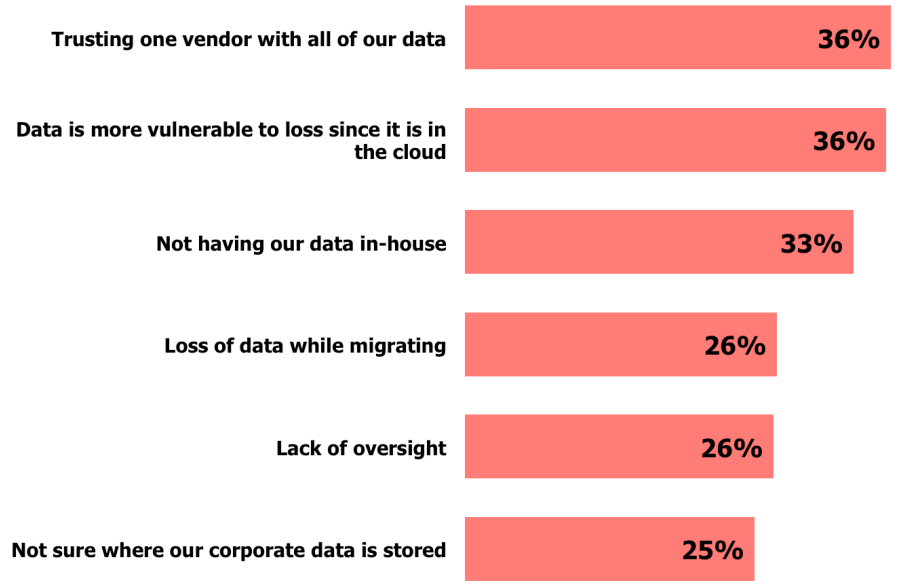
COMPLIANCE OBLIGATIONS ABOUND

Organizations around the world operate within the constraints of regulations and various other compliance obligations specific to industries, countries, regions, and legal jurisdictions. We will examine the concept of compliance obligations, note some of the significant regulations in place today, and look at both the complexity and ideal of complying with regulations.

CONCERNS ABOUT COMPLIANCE

Decision makers are concerned about a variety of compliance-related issues, but also more general issues related to moving their data to the cloud and giving a third party control over critical data resources, as shown in Figure 2.

Figure 2
Concerns About Office 365 and/or the Migration to Other Cloud Services
% Responding *Concerned* or *Extremely Concerned*



Source: Osterman Research, Inc.

THE CONCEPT OF REGULATIONS AND COMPLIANCE REQUIREMENTS

In principle, the concept of compliance obligations, whether based on specific regulations or legal requirements, is simple: an external body of some kind – with a mandate and the authority to do so – imposes requirements that must be met by an organization, otherwise a range of penalties can be imposed. The regulations are often defined as actions that need to be taken (for example, store all email messages for three years), or actions that *should not* be taken (for example, do not delete important email messages), along with an evidence trail to demonstrate that the rules were followed. Compliance, then, is the ability to prove beyond reasonable doubt that an organization has met the conditions of the imposed requirements. The production of evidence to demonstrate compliance requires structured processes, internal procedures, and technology-based systems.

KEY ISSUES TO CONSIDER

Organizations of all kinds and sizes face compliance obligations. With respect to electronic communications and the data they generate, a set of general and common requirements are imposed across many industries, countries, and regions. Broadly speaking:

- Electronic communications should be captured, stored in a secured location, and be unchangeable once captured. Email is the predominant form of electronic communication in business and organizational life today, but obligations generally extend to other forms of electronic communication, such as instant messaging chats, files, content in collaboration systems (e.g., SharePoint) and social media content. Organizations using paper forms of communication need to capture such records as well.

- The captured communications must be retained for a certain length of time, normally on the order of three to seven years, but sometimes much longer. The records must not be deleted during this period, nor changed, nor should anyone have the ability to change them.

- If required, organizations must be able to produce authentic copies of all communications that meet certain criteria. This requires good search tools that can identify relevant communications, and create a collection for further review.

- All copies of communications must be as originally communicated. Tampering with captured messages is not permitted.

- Once the retention period for communications has been reached – for example seven years – those messages can be validly deleted. However, if messages that have reached their expiration date are being held for a current or potential investigation, deletion must not occur until the legal hold has been lifted.

- Unauthorized access to systems and data should not occur. A method of controlling access to systems and data is necessary, and encryption of data may be necessary.

PENALTIES FOR NON-COMPLIANCE

Failure to follow regulatory requirements may result in a penalty of some kind – usually scaled up or down depending on severity, frequency. The penalty is often financial in nature, but may also consist of new restrictions on action, liability for executives, and publicity that can adversely affect an organization's stock price or reputation.

COMPLIANCE REQUIRES SYSTEMS AND PROCEDURES

No single action, act, activity, or system will ensure compliance with regulations. A complex set of factors should be put into practice, and followed rigorously at all times. This can include:

- **Effective Systems**
  Electronic information systems are normally required for compliance. These must be able to identify relevant communications and messages to capture, and provide a way to store and protect captured records for a specific period of time.

- **Company Policies**
  These should clearly state what must be retained under compliance regulations for the organization, as well as what does not need to be retained. If there are specific actions that employees need to take in order to achieve compliance, the policy should state these. For example, an employee may have to work in a particular system, or assign required metadata to communications or messages so they are appropriately classified. Company policies could also spell out the consequences to the individual and organization of non-compliance.

- **Employee Training**
  For building an appropriate awareness of the compliance requirements, each employee could meet, and develop competence in performing required actions in order to stay in compliance with the regulations.

These three factors can work in concert to keep the organization and its employees in compliance with regulations and legal obligations.

THE KEY REGULATIONS

In the United States, the primary regulations that impose requirements on organizations are as follows:

- **For Financial Services Organizations**
  The Securities and Exchange Commission (SEC), Financial Industry Regulatory Authority (FINRA), PATRIOT Act, and Gramm-Leach Bliley Act (GLBA) – among many others – impose particular requirements on financial services organizations. FINRA, for example, sets prescriptive requirements on the capture, monitoring, and archiving of broker/trader communications, and demands a supervisory review process. The PATRIOT Act requires an identity trail for customers opening new accounts. GLBA imposes rules on privacy of financial information about customers, and sets standards on how to protect this information.

- **For Healthcare Organizations**
  The Health Insurance Portability and Accountability Act of 1996 (HIPAA) sets prescriptive requirements on protecting health information that is "individually identifiable." There are technology, policy, and procedural requirements to safeguard such information when stored and transmitted.

- **For Organizations that Serve the US Federal Government**
  The Federal Acquisitions Regulations (FAR) require that contractors to the US federal government retain all records, both hard copy and electronic, for between two and four years. This covers organizations providing both goods and services.

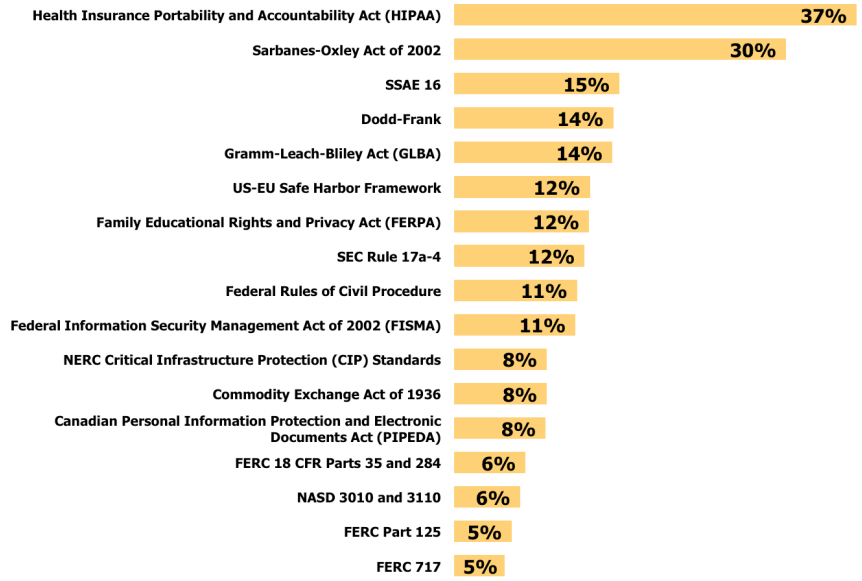
- **For State and Local Governments, and Public Sector Agencies**
  The Freedom of Information Act (FOIA) gives citizens the right to request access to records held by any federal agency. The current administration has directed agencies to work in a spirit of cooperation with requesters under FOIA. While agencies can respond to FOIA requests in the order in which they are received, there are situations where expedited processing is required. Most states and municipalities have similar open-records laws.

- **For Publicly Traded Organizations**
  Sarbanes-Oxley (SOX) requires that the financial records of publicly traded companies must be retained for up to seven years, and be available for review by the SEC at any stage.

- **For Designated High-Risk Organizations**
  Chemical manufacturing and energy distribution facilities, along with transportation operations, are designated as high-risk operations under the Homeland Security Act. Such organizations have security and recordkeeping requirements to which they must adhere.

Outside of the United States, different countries, regions, and economic blocs have their own set of regulations, such as the EU Data Protection Directive for data privacy in the European Union, and similar regulations for financial services organizations (FCA) in the United Kingdom. As shown in Figure 3, there are many compliance obligations that are an important or critical consideration for organizations that have deployed or may deploy Office 365.

Figure 3
Regulations Impacting Current and Prospective Office 365 Organizations
% Responding an *Important* or *Critical Consideration*



Source: Osterman Research, Inc.

THE COMPLEXITY OF REGULATIONS AND COMPLIANCE

In practice, regulatory and legal compliance is a complex beast. There are many individual regulations and compliance requirements for all organizations, and an awareness of these is essential to avoid the penalties noted above. Unfortunately, there is no single overarching regulation for all organizations, nor any single compliance action that will deliver everything that is necessary. The complexity is such that:

- Regulations differ by country, industry, and business function. For organizations operating across multiple countries or across multiple industries, defining an internal compliance approach is therefore fraught with complexity. It is a challenging task to reconcile the differing requirements and decide on the best way forward.

- Regulations can also be in conflict and inconsistent, so that what must be retained for one regulation does not need to be retained for another. Alternatively, while the duration of retention for one regulation is seven years, another may require only three.

- Regulatory compliance is also a dynamic field, where new regulations are introduced to right certain wrongs, or regulations are revised to consolidate past attempts and bring them up-to-date.

Organizations will require compliance professionals to ensure they are operating in alignment with current requirements and best practices.

THE COMPLIANCE IDEAL

In light of the complexity of regulatory compliance, most organizations aspire to demonstrate the following three characteristics:

- Retain only what is necessary to retain, for as long as necessary, and no longer. This means capturing communications at the right trigger point, classifying them for retention, and storing each form of communication in a tamper-proof repository for as long as needed. When records can be deleted, it should be done swiftly with a carefully prescribed plan for "defensible deletion". Employees know what they should and should not do to remain in compliance, and should follow the policies, procedures, and system requirements correctly.

- Quickly identify suspect or non-compliant communications, messages, and records and be able to demonstrate appropriate actions taken to address these. This may be in a proactive sense to minimize downstream harm, or in response to a request for information from an external body.

- Manage content with as little risk as possible. Use systems, policies, and training to minimize the compliance risks in an organization, such as inaccurate identification of content to retain, systematic failures to delete appropriate content, and insufficient care by employees in following policies.

MOBILITY IS AN INCREASINGLY IMPORTANT ISSUE

Mobility – which includes the "Bring Your Own" phenomenon with regard to devices, applications and cloud services – is a critical issue for compliance. Underscoring the growing severity of the problem are some of the key findings from the survey conducted for this white paper:

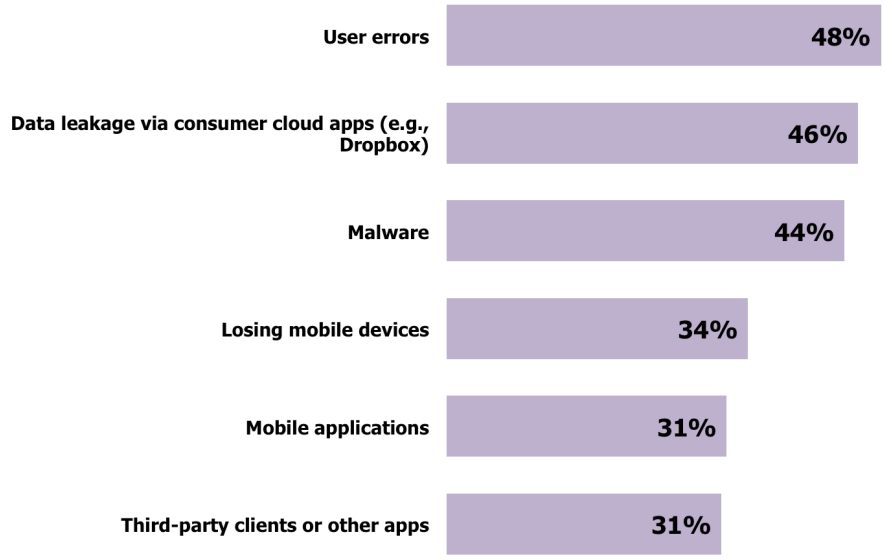
- Today, 62% of employees are enabled for mobile email, but this is expected to be 75% by mid-2017.

- One in five organizations has experienced data loss, malware infiltration or related problems through mobile devices during the past 24 months.

- Fifty-nine percent of those surveyed expect their mobile-related security and compliance problems either to remain unchanged or to get worse under Office 365.

The variety of mobile- and compliance-related concerns uncovered in the survey are shown in Figure 4.

Figure 4
Concerns About Various Mobile and Compliance-Related issues
% Responding *Concerned* or *Extremely Concerned*



Source: Osterman Research, Inc.

Mobile compliance is today managed through a variety of methods. For example, our survey found that 52% of organizations have implemented Mobile Device Management device controls, 34% have implemented app or data containerization, and 33% have limited the device models that can be used in their organizations. These have varying levels of effectiveness. More importantly though, one in six organizations has no mobile compliance controls in place.

COMPLIANCE CAPABILITIES IN OFFICE 365

In the section above we explored the field of regulatory and legal compliance at a high-level. In the section that follows, we assess the compliance capabilities in Microsoft Office 365, and evaluate their suitability.

MICROSOFT'S APPROACH TO COMPLIANCE IN OFFICE 365

Microsoft has invested and continues to invest a significant amount of financial resources and effort to build compliance capabilities into Office 365. The intent of these investments is to ensure its customers have adequate systemic capabilities to meet their compliance obligations. In evaluating Microsoft's approach to compliance in Office 365, we can make five statements:

- **The compliance responsibility is an organizational mandate**
  In the Office 365 documentation, Microsoft makes it clear that the responsibility for compliance rests with each organization. Microsoft is also keenly aware that compliance capabilities in Office 365 represent only one aspect of the compliance task. Organizational policy and employee training are equally essential.

- **Microsoft is addressing compliance issues**
  Broadly speaking, common compliance requirements are driving an agenda around archiving, encryption, eDiscovery, audit reporting, and legal holds, among other needs. Microsoft offers a range of current capabilities in these areas, and is evolving its capabilities to increase coverage.

- **The compliance capabilities in Office 365 are aimed at being "good enough"**
  With a platform aimed at hundreds of millions of users, Microsoft's compliance capabilities may not meet every need, nor address the requirements of every organization. The aim is to have sufficient systemic capabilities to address broad and general-purpose compliance requirements, in line with certain assumptions about the organization and its IT environment.

- **Office 365 compliance deals *only* with content in Office 365**
  The compliance capabilities in Office 365 address only content stored in the Office 365 environment and, even then, only parts of the content stored there. For example, Office 365 offers archiving capabilities for Exchange Online, but nothing similar for SharePoint or Yammer content. Content stored outside of Office 365 isn't addressed at all. With many organizations running hybrid environments for communications and collaboration, as well as using non-Microsoft services and needing to deal with content in legacy systems, relying on the compliance capabilities in Office 365 may not be suitable.

  The importance of using third party solutions that can fully address hybrid environments is underscored by a key finding from the research conducted for this white paper: among organizations that currently have less than 100% deployment of Exchange Online, 54% are planning on having a permanent hybrid environment of Exchange Online and on-premises email.

- **Office 365 supports basic compliance requirements**
  Although Office 365 addresses broad and general requirements, there are shortcomings in the systemic capabilities available. Office 365 only supports organizations with basic compliance requirements; those with more stringent requirements may find the compliance capabilities in Office 365 to be inadequate.

Let's look at the specific capabilities for compliance in Office 365, and examine the areas of its offerings that may require external compliance support.

AN ARGUMENT AGAINST TIGHTLY LINKED SYSTEMS

Microsoft has attempted to design a single, integrated system that fully handles the conflicting requirements of short-term, day-to-day communication by organizations and employees, combined with the long-term, multi-year compliance mandates under which those organizations operate. Where the first values new features, flashy upgrades, and speed-to-market, the second is dependent on stability, multi-year consistency, and nothing ever going wrong. The latter is both in conflict with the first, and is also something for which Microsoft is not known. Take Exchange 2010 and Exchange 2013 (and the Exchange Online variants of both), for example. Microsoft introduced one way of implementing legal holds in Exchange 2010, and a different set of approaches in Exchange 2013. On the SharePoint front, Microsoft's approach to records management has changed significantly from SharePoint 2007 to 2010 to 2013 (a seven-year period), and while those changes have been good and helpful on one level, it may not necessarily inspire confidence in Microsoft's ability to offer a compliance system in 2015 that will still be valid, robust, and reliable in 2022.

The tightly linked design between communication and compliance also leads to some severe implications. For example, an organization can archive content from Lync Online into Exchange Online Archiving, but that requires the user's mailbox to be on legal hold (we discuss legal holds in more detail later in this paper). Also, in order to access BCC addressee information for individuals, as well as expanded distribution list information, a sender's mailbox must be on legal hold. As a third example, the only way to achieve storage immutability is to have mailboxes on legal hold at all times. Essentially, this means that all mailboxes must be on pre-emptive legal hold at all times, and that no mailboxes can ever be deleted in case access to BCC information is required under a real legal hold request. No content can ever be deleted – even that which should be deleted due to it falling outside of regulatory mandates.

SENDING LARGE FILES

Office 365 has a 150-megabyte limit on message size, assuming that the message does not leave the Microsoft Office 365 data centers. If it does, the effective message size drops to 112 megabytes to allow for the transcoding overhead required for sending messages externally. These are significant size limits, and represent a significant increase on the historical size limit of 25 megabytes. However, for users that need to send larger files, Office 365's inability to seamlessly handle large file transmissions may cause employees resort to alternative, consumer-grade file sharing and transmission services. These workarounds can create compliance problems for organizations in several ways:

- The message may contain sensitive information that should be encrypted, but isn't.
- The message will not be captured for archival, classification, and retention in the corporate content management system or archive.
- The message will not be scanned for policy violations.

For individuals using Outlook for Mac, the message size limit is only 35 MB, a significant decrease on using Outlook for Windows or Outlook Web Access.

BASIC CAPABILITIES IN EXCHANGE ONLINE ARCHIVING

Microsoft offers an archiving solution for Exchange Online. It provides automated archiving, retention, and deletion by having an administrator define a default archiving policy for the user's mailbox, plus more granular archiving or deletion policies for specific folders (such as the Inbox). However, a user can overwrite any administrator-defined and automatically applied policy with his/her own policy setting on a message-by-message basis or automatically via inbox rules. These personal policy settings always override the administrator-defined policy settings, meaning that employees can easily opt-out of the archiving and retention requirements. They can, for example, delete messages that should be retained. The only way to prevent the deletion of messages that should be retained is to put a user on legal hold in perpetuity, which quickly escalates to having the entire organization on legal hold to prevent inappropriate message deletion.

NO ARCHIVING FOR SHAREPOINT ONLINE, FILES OR YAMMER

Exchange Online Archiving is just that: an archiving service for Exchange.

Financial services firms are required to capture, archive, and retain social media content. The inability of Office 365 to archive its own Yammer service pushes financial services firms immediately out of compliance. For all other firms for which archiving of content in SharePoint team sites, Lync meetings and messaging threads, and Yammer conversations is required, what is available with Office 365 may not be sufficient.

Lync Online is a special case from an archiving perspective. If users are placed on legal hold, their Lync Online conversations can be archived into Exchange Online Archiving. For organizations where this condition is too severe, they may l be out of compliance with their obligations.

WEAK SUPPORT FOR IMMUTABLE STORAGE

Office 365 offers no immutable storage capability, the standard for which is WORM (write once, read many) storage. Immutability is a requirement to demonstrate original authenticity of captured messages and records, and financial services firms covered under SEC 17a3-4, for example, are required to use immutable storage and need to store a duplicate copy separate from the original. Microsoft does offer a workaround to its lack of true immutable storage capabilities in Office 365 – but this is only accomplished by placing all users on legal hold in perpetuity. Microsoft's

approach does not, however, provide a way of storing a duplicate copy separate from the original.

ELASTIC DATA RESIDENCY

Microsoft operates a global network of data centers for Office 365, and claims the right to store data in any data center. Microsoft will not explicitly state where a customer's data is being stored within its data centers, and reserves the right, without notification, to shift data at will between its data centers. For organizations operating under strict data sovereignty requirements, these elastic residency conditions will be unsuitable. Non-US customers, for example, could find that their data is being stored in a US-based data center, and therefore subject to data access under the PATRIOT Act, by the IRS, or by other US government agencies.

Data sovereignty is of particular concern across the European Union, and therefore Microsoft has self-certified with the requirements of the EU Data Protection Directive. For customers that want more assurance than self-certification, Microsoft is willing to sign a more binding agreement.

BASIC LITIGATION HOLD CAPABILITIES

Legal hold is a method of preventing stored information from being deleted even if it reaches its expiration date, and is used whenever an active legal investigation is reasonably possible or already underway to explore past actions. The capabilities for legal hold in Office 365 are as follows:

- There are two general approaches to legal hold: Litigation Hold (from Exchange 2010 and Exchange Online based on 2010) and In-Place Hold (from Exchange 2013 and Exchange Online based on 2013). Litigation Hold is a mailbox property that is turned on or off, and supports an unlimited number of mailboxes. In-Place Hold has three variants for a more granular-based approach to legal hold – a blanket hold until further notice, a time-based variant with an expiration date, and a query-based variant for a granular hold. In-Place Hold can support only 10,000 mailboxes on any given hold. If more than 10,000 mailboxes have to be covered by a legal hold, multiple and separate In-Place Holds will be required. Microsoft also recommends against using multiple In-Place Holds on a given mailbox; the recommendation is one or none, although Office 365 can support it, but with consequential performance impacts.

- As noted above, there are at least three situations in Office 365 under which a legal hold must be in place. The practical implication of these situations is that all employee mailboxes must be under legal hold at all times.

- Information about BCC recipients, or message recipients who are members in a distribution list, are only available to search after a mailbox has been placed on legal hold. If the sender's mailbox is not placed on legal hold, this information is hidden and inaccessible, and will therefore not be reflected in an eDiscovery search.

- Legal hold capabilities are available only with the Enterprise E3 and E4 plans, which are the most expensive Office 365 plans on offer. In light of the inherent weaknesses in the legal hold capabilities in Office 365, as well as the higher price for an E3 or E4 plan, a strong argument can be made for using a third-party service to achieve better capabilities at a lower price point.
- Yammer conversations are not covered by legal hold.

BASIC SEARCH PROCESSES

The search process for eDiscovery in Office 365 offers limited capabilities. Here are five examples:

- Office 365 does not index all key file types. It offers support for Microsoft Office file and document types, and other commonly used file types. However, for the

file types that are not searched by default, there is no possibility of installing additional filters to provide this capability, as can be accomplished when using Exchange on-premises. File types that are not searched are either excluded by the search process entirely, or included in search results just in case something relevant is inside. So, for example, this may result in the inclusion of certain file types during an eDiscovery search because they might contain relevant data, but the content of the files will not be indexed and will have to be searched manually.

- Search requests in In-Place eDiscovery are queued and processed in batches. This can lead to a substantial amount of wait time, and if the original search request was specified incorrectly, the search will need to be repeated until right. Some regulations demand search results within a specified time period: for example, SEC guidance for the Investment Advisers Act of 1940 states that "…you should be able to promptly (generally within 24 hours) produce required electronic records that may be requested by the SEC staff, including email.[1]" Having to wait for a search to complete while operating under the stress of an impending deadline can be unpleasant.

- Only messages that have been retained by end users are included in the search scope, unless legal hold is turned on in perpetuity, thereby preventing the deletion of any messages and other mailbox items. If legal hold has not been enabled, the search result set will almost definitely be incomplete, and compliance officers would have no way of knowing.

- eDiscovery searches are one-time affairs that produce a set of messages and items for review. Items identified through a given search may be different to the items identified through a subsequent search, due to changes in the search index. Without re-running the eDiscovery search to locate newly created items, the review items will quickly become outdated. Running an eDiscovery search and gathering up new evidence is a manual process.

- Compliance officers cannot preview search results in the search preview pane. Results must be copied to a discovery mailbox in order to review the content.

The search request constructs in eDiscovery also cannot be saved and run again, and must be re-specified each time the search is run.

LIMITED eDISCOVERY WORKFLOW CAPABILITIES

eDiscovery workflow encompasses the range of tasks from searching for possible content covered by a legal request, to collecting and preserving such evidence, and processing it further to see which messages should be made available to opposing counsel. Systems supporting strong eDiscovery workflow enable organizations to minimize their costs during eDiscovery activities. Office 365 has some limitations in the eDiscovery area, including:

- eDiscovery processes in Office 365 are generally aimed at the left side of the EDRM model, while processing of activities on the right side of the model are generally accomplished using more purpose-built applications. Microsoft's acquisition of Equivio may address these "right-side" issues in the future.
  Only two eDiscovery searches can be run concurrently in Office 365. Any further searches will fail immediately; they will not queue.

- Microsoft recommends against having more than one In-Place Legal Hold on a given mailbox at any one time, although Office 365 can handle up to five concurrently (with consequential impacts on performance). However, even five is unacceptable in a litigious environment where many Global 1000 organizations have 500 open legal holds at any one time, and some have up to 15,000 that

[1] https://www.sec.gov/divisions/investment/advoverview.htm

they must manage. Each of these legal holds needs to be dealt with separately.

- An eDiscovery search is likely to produce different results each time it is executed. In Office 365, the search query cannot be saved for repeated execution, and there is no ability to trim the result set before exporting them for early case assessment. This makes searching and culling evidence less efficient, and more complex and costly.

- Search results can be saved into an eDiscovery mailbox, which can be exported to a .PST file. However, there are no collaborative review capabilities in a .PST file, which makes it difficult for multiple people to review the collected evidence.

NO SUPERVISORY REVIEW

Office 365 does not offer any native Supervisory Review capabilities, which is one of FINRA's requirements for its member financial services firms. In essence, a supervisor is required to systematically review messages sent by his/her employees on a regular basis, to ensure that reps are communicating in compliance. This requirement extends to all correspondence and internal communications through various channels, including Facebook, LinkedIn, and Yammer.

LIMITED USAGE/ADOPTION REPORTING

Office 365 offers only basic reports on users and the licenses assigned to them. By using PowerShell, an administrator can see which users have assigned licenses, but this only displays license assignment, not whether the license is being actively used. This makes it difficult to report on usage and adoption over time.

NO FINE-GRAINED AUDIT REPORTING

Office 365 offers two basic audit reports: a list of people who have accessed an Exchange mailbox for which they are not the owner (the Non-Mailbox Owner Report) and a report of actions undertaken by administrators on mailboxes and Exchange. Administrator actions that are tracked include the creation, removal, and modification of mailboxes, and the granting and removal of access permissions for mailboxes. The creation of Exchange Transport Rules is also tracked. Anything more granular than this is not available.

Finally, Exchange Online purges its audit reports every 90 days. This gives a very limited window of reporting on past actions.

ONLY SHORT-TERM STORAGE OF AUDIT LOGS

The mailbox owner and administrator access audit reports in Exchange Online are purged every 90 days, which is very short-term storage. Some regulations require audit logs to be stored for seven years, which is not done in Office 365. Our research found that only 62% of those surveyed consider the 90-day limit to be sufficient – among organizations that find this limit to be unsatisfactory, 24% want retention of six months and 38% require one year retention of logs.

LIMITED CONTROLLED DELEGATION CAPABILTIES

Office 365 supports five levels of administrator in the Business and Enterprise plans, including Global (the all powerful role), Billing (for making purchases and managing subscriptions), and Service (for service requests) roles. However, these roles are enabled for individuals across the entire organization, and cannot be limited to specific geographies or business units. In some organizations this lack of granularity will be perfectly fine; in many others it will gift far too much power to people.

RELIANCE ON CONSUMER MOBILE CLIENTS

In order to support a wide range of mobile devices, Office 365 utilizes a number of different approaches to extend mobility to these emerging devices. For Office 365 email, the Exchange ActiveSync protocol provides access to essentially any mobile client. SharePoint documents can be accessed or synced to devices in a number of

different ways. Unfortunately, this means many users access their email or sensitive content from a variety of consumer mobile apps.

Moreover, openness comes at a cost. While Microsoft does offer some controls over clients, most of these rely on the honesty policy. When Office 365 applies a policy it relies on the client to apply the policy. Clients can and do confirm that they are complying with policies when they are not. For example, Acompli (later acquired by Microsoft and rebranded as Outlook for iOS and Android) has misreported device configurations and bypassed Office 365 controls for mobile device types and versions.

In many ways, when a user accesses Office 365 data from a mobile device they are outsourcing their compliance to Apple, Google, or whatever startup developed an app appealing to end users. As many of these apps fail to respect compliance controls they can result in organizations falling out of compliance.

For example any of the following may take place:

- A message that may contain sensitive information that should be encrypted may be stored unencrypted by a mobile client.
- Users may intentionally or inadvertently open sensitive information in a mobile app that may leak the information.
- Users may intentionally or inadvertently communicate information through an unapproved mobile app, bypassing compliance controls entirely.
- Users may take sensitive information stored in SharePoint or other compliant systems and leak them to an unapproved cloud service (e.g., Dropbox) outside of compliance controls.
- Users may cut and paste information from mobile clients to other mobile apps, thereby exposing information that must be held private.
- A mobile device may be lost and the information exposed to unauthorized parties.
- Users may intentionally or inadvertently share data between compliant communications channels, such as email and channels outside of enterprise control like SMS, third party messaging or chat apps or other third party communication apps, bypassing compliance controls.

For these reasons, the growing fleet of mobile devices in many organizations represent a substantial challenge to maintaining compliance with Office 365.

EXPOSURE OF CREDENTIALS

Mobile devices also create compliance risk because of the exposure of Office 365 credentials. Most mobile devices store Office 365 credentials in an insecure way. The Apple iOS keychain may, for example, store Office 365 passwords, authentication tokens, certificates or private keys. By cracking the device password, often merely a four digit PIN, unauthorized users can gain access to Office 365 accounts. The compliance implications of such exposure are clear: not only does it potentially mean sensitive information might leak, but it may also mean a nefarious party can spoof a authorized user and use this access to bypass compliance controls.

PERFORMANCE

Another important consideration is the performance of Office 365 and the speed with which data can be migrated. For example, searches in Office 365 can take several hours to complete across a large organization. There are also export- and import-related related challenges because of the throttling in Office 365. For example, IMAP migration is throttled to 10-14 Gb per hour, while client uploading from an Outlook

.PST file is throttled to just 500 Mb per hour[2]. For eDiscovery and related types of activities, export throttling may present a challenge when exporting several terabytes of data. Exporting large chunks of data will be necessary in Office 365 because early case assessment capabilities are somewhat limited.

THIRD PARTY TOOLS FOR COMPLIANCE IN OFFICE 365

A number of vendors offer third-party tools to significantly increase the compliance capabilities in Office 365. Let's look at the broad categories of capabilities available from third-party vendors.

- **A Compliance System Built for Compliance and eDiscovery**
  Establishing a compliance management system that is separate from the day-to-day messaging and communications environment gives organizations a number of significant benefits. It is built for the special requirements of compliance, not a compromised approach to building a single environment to handle fundamentally conflicting design requirements. It also provides risk mitigation for organizations that decide to shift from Office 365 to another system. It can more appropriately handle the archiving, legal hold, and policy-based mandates in a compliance environment.

- **Compliance Beyond Office 365 Data**
  Organizations have data in historical and other current systems that must be managed according to compliance requirements, such as previous messaging systems, social media properties, and even Yammer. Unless an organization is willing to run multiple compliance management systems in parallel – which leads to significant complexity, increased cost, and increased risk of falling outside of compliance mandates – a single cohesive, integrated compliance system that can incorporate Office 365 data alongside other equally valid data sources is a more strategic investment for organizations.

- **Containerized Mobility Solutions**
  Organizations can ensure compliance is maintained on mobile devices by separating and protecting business data and apps on the device. This can be performed through the use of a container solution. Container solutions should encrypt all data in use, in storage as well as in transit. They also should restrict data leakage to unsecured apps, limit copy/paste and movement to unauthorized cloud storage solutions. In addition, they should encrypt credentials and configuration. For example, instead of leaving credentials for Office 365 unencrypted in the device OS, they should use a Kerberos Constrained Delegation capability so that apps requiring credentials are granted a Kerberos ticket to behind the firewall applications with a secure system acting as the Identity Provider. The container should also enable secure, app-to-app communications to protect enterprise data from the threats of mobile apps. The ideal solution provides consistent control of Office 365 messages and content across all mobile devices rather than relying on the specific mobile manufacturer.

- **Sending Large Files**
  Users that need to send large files should be able to do so within the compliance parameters in Office 365, and should not resort to consumer-grade services. Third-party services offer the ability for transparent distribution of large files directly within Office 365, while still being subject to the organization's compliance policies. Large file transfers are handled through a separate secure service, as opposed to using Exchange for delivery.

[2] https://technet.microsoft.com/en-us/library/dn592150(v=exchg.150).aspx

- **Policy-Driven Message Encryption**
  The ability to establish policies that trigger which messages are subject to encryption, and automatically apply the required encryption level without requiring manual intervention by users. Advanced encryption services also provide the ability to revoke encrypted messages that have been sent to the wrong person, something that is not possible in Office 365.

- **Real Policy-Based Email Archiving**
  Policy-based archiving and retention of email without the ability for users to simply override the policy settings at will. Separating the day-to-day transactional communication through email and the compliance repository helps with compliance management. Journaling of communications from Exchange to a separate archive is a well-established approach to the creation of a compliance repository.

- **Reporting on Multiple Sharing and Collaboration Technologies via a Single Pane of Glass**
  Office 365 is one of the many technologies used to share information and collaborate. As organizations invest in multiple sharing and collaboration technologies, one concern may be the explosion of dedicated – and sometimes limited – interfaces provided by the various offerings. One additional benefit of third party products is that they typically have a broader perspective and cover multiple vendor offerings in a more robust, single console. This is especially important for non-technical users, such as security and compliance officers, who need to interact with these systems to gain insight and provide oversight into their operations.

- **Policy-Based Archiving for SharePoint, Lync Online, and Yammer**
  Email is an important part of day-to-day communications, but it is not the only content type that needs to be archived. Organizations using SharePoint, Lync Online, Yammer, and other social media services need the ability to archive content, apply policy, and may have the same compliance capabilities – such as eDiscovery and legal hold – that are available for email. The growing importance of non-email forms of communication makes this an essential issue to resolve.

- **Support for Immutable Storage**
  Immutable storage systems, by design, prevent any modification to messages and other data once stored. It provides an authentic and unaltered record of what happened, and is required by some regulations. Office 365 offers an inadequate approach to immutable storage by requiring people to be on legal hold at all times. Third-party solutions provide true immutable storage without using legal hold.

- **Control over Data Residency**
  For organizations that have specific requirements about data residency, third-party solutions provide tighter contractual specifications for where data is actually stored. This allows organizations to know with complete certainty that their data is stored in a particular data center, city, or country (to allow for in-country co-location for redundancy and resilience).

- **Legal Hold**
  Compliance systems with advanced legal hold capabilities support the placement of multiple concurrent holds, fine grained selection of hold targets, and coverage for multiple data types. Third-party systems also use legal hold as they are intended to be used: only when an active legal case is reasonably anticipated or underway, not as an inefficient and unsustainable approach for ensuring retention, discoverability, and immutability.

- **Advanced Search Capabilities**
  Third-party archiving solutions offer the capability to get real-time search results in an eDiscovery inquiry, as well as support for more than two concurrent eDiscovery searches. More advanced search capabilities also allow for the indexing of more file

types, which is an important compliance consideration for organizations working with or receiving non-standard files.

- **Advanced Identification of Sensitive Data**
  Third party tools for Office 365 can also provide reporting on violations, classifying the most frequent incidents to highlight needed corrective action.

- **Workflow Capabilities for eDiscovery**
  Organizations handling multiple concurrent eDiscovery requests need proper workflow capabilities to assure quality, streamline effort, support multi-party review, and reduce legal costs. More advanced third-party tools provide such capabilities for organizations using Office 365.

- **Supervisory Review**
  The ability to systematically review email messages and other communications is important under the FINRA regulations. Human review complements other automated checking mechanisms to assure compliance and provide early detection of infractions.

- **Long-Term Log Retention for Compliance and Trend Reports**
  Some regulations require the retention of log, audit, and trend reports for up to seven years. Exchange Online purges its reports every 90 days. Third-party tools provide long-term retention for such reports, for example by using Microsoft Azure as the long-term repository.

- **Fine Grained Audit, Compliance, and License Reports**
  While Office 365 offers a set of basic reports for audit, compliance, and licensing purposes, many organizations need much more to optimize their use of Office 365 and complementary services. These should provide reports, dashboards, and drill-down analytics for the overall Office 365 service, as well as its individual components. Reports should also be able to be scheduled for automated delivery to specific groups and individuals, as well as being available on-demand at any time.

- **Unified Reporting on the Usage of Multiple Tools**
  Office 365 is just one of the many technologies used to share information and collaborate. As organizations invest in multiple sharing and collaboration technologies, the proliferation of dedicated interfaces for each system is a concern. Third-party products typically have a broader perspective and cover multiple vendor offerings in a more robust, single console. This is especially important for non-technical users, such as security and compliance officers who need to interact with these systems to gain insight and provide oversight into their operations.

- **Controlled Delegation Capabilities for Compliance**
  Organizations with complex organizational structures require more controlled delegation capabilities for managing the configuration of Office 365, as well as the compliance-related tasks that individuals can undertake. The default approaches in Office 365 require giving too much control for too broad a set of tasks to individuals. Third-party tools enable the delegation of compliance capabilities in Office 365 to authorized users with a more limited scope, such as specific organizational units, divisions, or countries.

- **Wizards (Not PowerShell) for Tasks**
  Many tasks in Office 365 require familiarity with and use of PowerShell to complete. Add-on products provide simple wizard-driven interfaces for achieving the same outcomes, while hiding the complexities of Office 365 from administrators.

SUMMARY

Office 365 is a robust platform that offers a number of useful capabilities. However, it can be seen to lack a variety of compliance and eDiscovery-related features and functions and require the use of third-party solutions in order to help satisfy compliance obligations. Consequently, Osterman Research recommends that organizations carefully evaluate the compliance capabilities within Office 365, determine where the deficiencies exist for their particular situations, and deploy third-party tools to address these inadequacies.

SPONSOR OF THIS WHITE PAPER

Designed specifically to augment the benefit of Microsoft Office 365 with additional layers of enhanced email security, an independent email archive and backed up by a 100% service availability SLA, email continuity. All enhance the value Microsoft Office 365 or Microsoft Exchange Online delivers to your business.

Mimecast provides a highly secure and resilient independent offsite email archive which augments Office 365 across all mid-size and enterprise E plans, and Exchange Online plans 1 and 2. The Mimecast Archive for Office 365 delivers enhanced eDiscovery and compliance archive tools as well as an end user orientated Outlook integration to provide end user security and a real time archive search functionality directly from their desktop. Mimecast's Secure Email Gateway adds enhanced security, Data Leak Prevention, Email Encryption and the unique Mimecast Large File Send service, allowing Office 365 users to send and receive files up to 2GB.

mimecast
unified email management

www.mimecast.com

@mimecast

UK/EUROPE
+44 (0) 207 847 8700
info@mimecast.com

+44 (0) 1534 752300
info@mimecast-offshore.com

NORTH AMERICA
+1 800 660 1194
+1 781 996 6340
info@waltham.mimecast.com

SOUTH AFRICA
+27 (0) 117 223 700
0861 114 063
info@mimecast.co.za

AUSTRALIA
+61 3 9017 5101
1300 307 318
info@mimecast.co.au