WHITE PAPER

Best Practices for eDiscovery and Regulatory Compliance in Office 365®

An Osterman Research White Paper

Published September 2016

Sponsored by

ARCHIVE360
POINT. CLICK. MIGRATE. STORE.

OSTERMANRESEARCH

Osterman Research, Inc.
P.O. Box 1058 • Black Diamond, Washington • 98010-1058 • USA
Tel: +1 206 683 5683 • Fax: +1 253 458 0934 • info@ostermanresearch.com
www.ostermanresearch.com • @mosterman

EXECUTIVE SUMMARY

eDiscovery and compliance are essential activities for any organization, regardless of its size, the industry that it serves or the jurisdictions in which it operates. To be sure, “heavily” regulated organizations – such as those in the financial services, healthcare, life sciences, energy and certain other markets – face higher levels of compliance obligation than their less heavily regulated counterparts. However, every organization must factor eDiscovery and compliance into its communications and collaboration strategy.

KEY TAKEAWAYS

- Microsoft Office 365® provides a successful and popular set of communications and collaboration capabilities, and its use will continue to grow at a rapid pace. Although Microsoft has been offering hosted/cloud-based offerings for more than 15 years, Office 365 is the most successful iteration of the company’s cloud-based communications and collaboration offerings to date.

- eDiscovery and compliance obligations are becoming more onerous and more complex over time. However, these are essential capabilities that decision makers must consider in the context of their communications, collaboration, file-sharing, storage and other strategies.

- These complications are being driven by a number of factors, including the rapid proliferation of electronic information, the increasing number of data types that must be retained for legal and regulatory purposes, the increasing amount of data that employees manage independently of IT, and increased government oversight into corporate activities.

- Increasing regulation, oversight and court actions create an ever more complex minefield of Discovery and regulatory requirements, a situation that will become only more difficult over time. A failure to adequately address these issues will increase corporate risk.

- Microsoft has done a good job at building eDiscovery and compliance capabilities into Office 365 and should be commended for doing so. However, there are a number of limitations and deficiencies in Office 365 from an eDiscovery and compliance context that decision makers should consider as they evaluate Microsoft’s offerings. Even more so in environments that operate both Microsoft and non-Microsoft solutions.

eDiscovery and compliance obligations are becoming more onerous and more complex over time.

ABOUT THIS WHITE PAPER

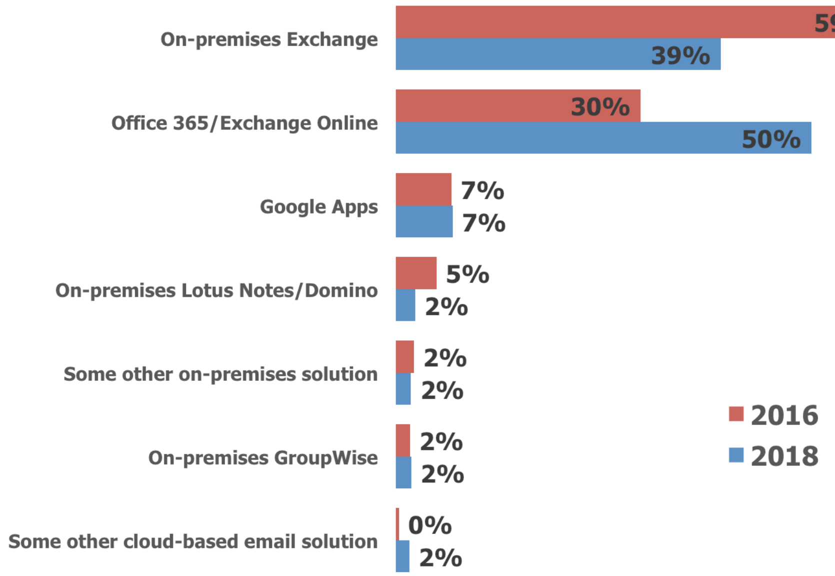
A survey was conducted for this white paper and some of the results from it are included herein. However, all of the results will be published in a separate survey report shortly after the publication of this white paper.

This white paper and survey was sponsored by Archive360. Information on the company, as well as their relevant solutions, is provided at the end of this paper.

INCREASING USE OF OFFICE 365

Microsoft Office 365 – the company’s third major iteration of its hosted/cloud-based email and collaboration offerings – is the most successful of its solutions to date. The company has been (and we anticipate will continue to be) successful in converting its base of on-premises users of Exchange and other solutions to Office 365. As shown in Figure 1, the survey conducted for this report demonstrates that growth of Office 365 will be rapid over the next 24 months as on-premises users of Exchange and other platforms migrate to the cloud.

Figure 1
Deployment of Various On-Premises and Cloud-Based Solutions
2016 and 2018



Source: Osterman Research, Inc.

THE CRITICAL IMPORTANCE OF eDISCOVERY

WHAT ARE DISCOVERY AND eDISCOVERY?

The process of discovery can be viewed in a couple of ways:

- As a relatively strict set of requirements focused on searching for content that may be relevant for use as evidence in a trial or in pre-litigation activities. Viewed in this way, discovery can include any sort of document or other information that might be useful to prove a plaintiff's or defendant's case in a civil action.

- Viewed in a broader context, however, discovery is the ability to search for content not only within the confines of court-ordered discovery activities, but also all of the efforts focused on finding information that could somehow be relevant for any litigation- or compliance-related activity, such as senior managers performing informal early case assessments or mid-level managers searching for potentially damaging content in their employees' email or social media posts.

"eDiscovery", then, is just the extension of well-established discovery processes to any Electronically Stored Information (ESI) that an organization possesses – email messages, social media posts, voicemails, presentations, word processing files, spreadsheets, CRM data and all other relevant communication or information that could be useful in a legal action. eDiscovery can extend to any platform on which ESI is stored: desktop computers, laptops, servers, smartphones, tablets, backup tapes, and even employees' home computers and other personally owned devices.

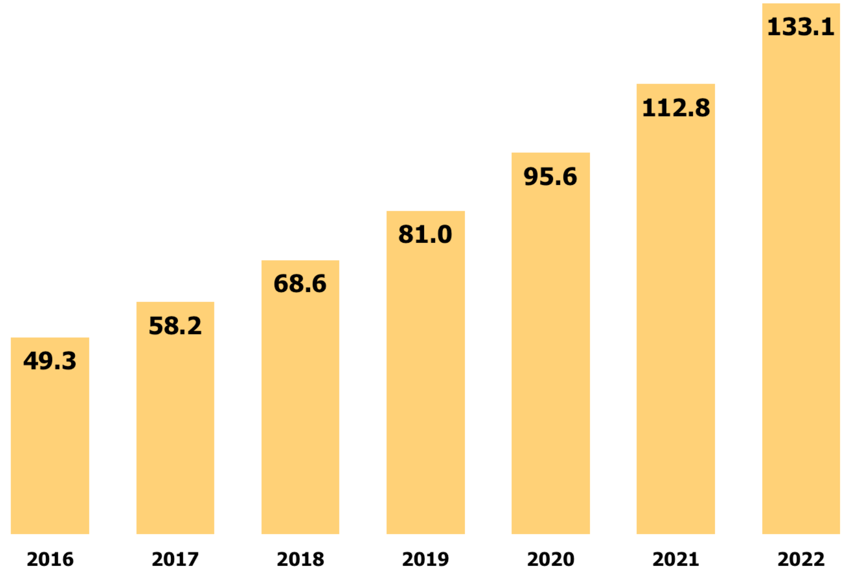
Being able to find, secure and produce information when requested by a court or regulator is an essential responsibility present in one form or another in every industrialized country.

Being able to find, secure and produce information when requested by a court or regulator is an essential responsibility present in one form or another in every industrialized country. It is also a responsibility that, if taken lightly, can cost an organization dearly in the form of fines, sanctions, penalties, lost business, or higher legal costs. At its heart, an effective and compliant eDiscovery or compliance process is highly dependent on a well-managed information governance capability. Costs and risks of eDiscovery and compliance skyrocket when an organization does not have control of their enterprise data and therefore cannot find all requested information for a legal action within the timeframe allowed by the court. Costs are also negatively impacted by finding too much data (over-collection) or not finding all relevant information (under-collection).

ELECTRONIC DATA IS INCREASING RAPIDLY

It should be a surprise to no one that ESI is accumulating rapidly. For example, an Osterman Research survey conducted during March 2016 found that organizations store a mean of 49.3 gigabytes of just email data per user (a particularly interesting data volume given that Office 365 offers 50 gigabytes of email per user[i]), and that total messaging-related storage during the previous 12 months had increased a mean of 18 percent. Based on even this relatively modest rate of growth, 49.3 gigabytes in 2016 will increase to 133 gigabytes over just six years, as shown in Figure 2.

Figure 2
Storage Growth Based on an Increase of 18 Percent per Year
2016-2022



Source: Osterman Research, Inc.

The vast majority of data accumulating within the typical enterprise is of the unstructured variety, usually controlled and "managed" by individual employees.

The vast majority of data accumulating within the typical enterprise is of the unstructured variety, usually controlled and "managed" by individual employees. Much of this unstructured data is considered "dark data" because it is invisible and not easily accessible by the company. Instead of being stored on managed electronic content management (ECM) systems, this data is normally stored on employee workstations, removable media, enterprise file shares, or even outside the organization's control on employee-managed personal clouds. Dark data poses a growing cost and liability to the organization because it is still considered an organizational asset and within its scope of responsibility, and is a major concern in the context of compliance, eDiscovery and data leaks.

While email is often one of the primary sources of discoverable information, other data types are becoming increasingly important to consider in the context of eDiscovery and compliance. This includes electronic files, social media posts, wikis, blogs, SMS/text messages, SharePoint and other data repositories, databases, CRM data and a growing number of other data types.

KEY OBLIGATIONS TO CONSIDER

Every organization faces some level of eDiscovery and compliance obligations. A set of general and common requirements are imposed across many industries, countries, and regions:

- ESI should be captured, stored securely, and be unchangeable once it has been captured. Email is the primary form of electronic communication in business and organizational life today, but obligations generally extend to other forms of relevant electronic communication, such as instant messaging chats, files, content in collaboration systems (e.g., SharePoint) and social media posts. Organizations using paper forms of communication need to capture and preserve these kinds of records as well.

- Archived communications must be retained for various lengths 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 modified, nor should anyone have the ability to tamper with them.

- When necessary, organizations must be able to produce authentic copies of all content that meets certain criteria. This requires robust search tools that can identify relevant communications, keep them organized, and make it easy for these collections to be furnished for further review.

- Once the retention period for communications has been reached, this content can be validly deleted in most cases. However, if messages that have reached their expiration date are being held for a current or potential investigation (litigation, or legal hold), deletion must not occur until the hold has been lifted. It is essential to note that items placed on legal hold will need to be retained beyond their retention period until the legal action is concluded and the legal hold has been removed. At that time they can be safely deleted if they are older than the length of the retention period.

- 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 also be necessary. Robust access controls are essential, as are specific definition of the organizational roles that will have access to the archive.

- When records can be deleted, it should occur swiftly with a carefully prescribed plan for "defensible deletion" – the practice of identifying and deleting data that is no longer needed and retention of which would increase corporate risk.

ESI should be captured, stored securely, and be unchangeable once it has been captured.

THE FEDERAL RULES OF CIVIL PROCEDURE

The Federal Rules of Civil Procedure (FRCP) are a set of rules, first established in 1938, that provide the basic ground rules for civil litigation in the United States. The rules were updated significantly in 2006, most notably to codify the concept of ESI.

The result of the 2015 changes to the FRCP will be shorter and more limited discovery periods, the requirement to be better prepared for eDiscovery quickly once the litigation process starts, and attorneys must be ready to address claims and proportionality issues in the context of eDiscovery. Key changes to the rules include the following:

- The discovery process is now more limited than it was previously in order to minimize the pain it imposes on all parties to litigation.

- Whereas the 2006 changes to the FRCP focused on the provision of ESI, the 2015 changes modify the focus to preservation of ESI. The new rule imposes "curative" measures when ESI is lost or absent, which may make an inability to produced requested information during discovery more expensive and consequential.

- Parties under the previous FRCP rules could simply object to a request for the production of information. The new rules require the objecting party to state the specific reasons for its objection and the party "must state whether any responsive materials are being withheld on the basis of that objection".

eDISCOVERY REQUIREMENTS AND COMMON MISTAKES

Decision makers can learn from court decisions about what to do – and what not to do – in the context of eDiscovery. Here are some notable lessons that decision makers should take to heart:

- **Backups can create problems for the eDiscovery process**
  Backups, either on tape or on disk, are a poor method for retaining discoverable content because accessing this content is time-consuming, expensive and may not produce all of the necessary information.

- **eDiscovery must not be overly broad**
  Although an older case, *Moulin Global Eyecare Holdings Ltd. v. KPMG* is useful to consider because the court rejected the plaintiffs' arguments for a discovery request that it considered too expansive. The court determined that allowing this type of broad access to the defendant's electronic content would be "tantamount to requiring the defendants to turn over the contents of their filing cabinets for the plaintiffs to rummage through.[ii]"

- **Not retaining ESI can lead to sanctions**
  In *Frank Gatto v. United Air Lines*, the plaintiff deleted his Facebook content, access to which had been requested by the plaintiffs. The court agreed with the defendant's motion and issued an adverse instruction, one of the worst possible situations for any party to a legal action[iii]. By archiving ESI in a compliant manner, companies can defend themselves against these types of doomsday scenarios in a set-and-forget fashion.

- **Demonstrating that appropriate material was used**
  Many recruiters use social media content in their process of evaluating candidates. However, employers cannot consider a candidate's race, religion, sexuality or certain other types of information. If an employer uses social media as part of the hiring process, it should archive the content it used about candidates to demonstrate that it did not evaluate material that could not be legally considered. A failure to do so – and an employer's inability to demonstrate its good faith evaluation of this information during eDiscovery – could result in serious consequences. Relevant regulations in this regard include the Americans with Disabilities Act, the Age Discrimination in Employment Act, the Civil Rights Act of 1964 and Executive Order. No. 11,246[iv].

Information subject to [regulatory] retention requirements should be treated with care, much like information subject to eDiscovery.

COMPLIANCE AND INDUSTRY REGULATIONS

THE CONCEPT OF REGULATIONS AND COMPLIANCE REQUIREMENTS

Most nations impose some form of regulatory obligations for records retention that direct what information must be retained and for how long. Information subject to these retention requirements should be treated with care, much like information subject to eDiscovery, because of the potential penalties and fines for not following the laws. Data subject to compliance requirements that is not managed and retained in compliance with these regulations can trigger government information requests. These can quickly transform into expensive legal proceedings, fines, and maybe even jail time.

THE KEY REGULATIONS

In the United States, the key regulations that impose requirements on organizations include the following:

- **Healthcare**
  The Health Insurance Portability and Accountability Act of 1996 (HIPAA) establishes various requirements on Protected Health Information – information about an employee's health that can be linked to his/her identity. There are various technology, policy, and procedural requirements to safeguard such information when stored and transmitted.

- **Financial Services**
  The Securities and Exchange Commission (SEC), Financial Industry Regulatory Authority (FINRA), Dodd-Frank Act, PATRIOT Act, and Gramm-Leach Bliley Act (GLBA) – as well as other requirements – impose various obligations on financial services organizations. FINRA, for example, establishes requirements on the capture, monitoring, and archiving of broker/trader communications, and demands a supervisory review process. The Dodd-Frank Act has created the Financial Stability Oversight Council and implements a variety of supervision and oversight controls on financial institutions. The PATRIOT Act specifies an identity trail for customers opening new accounts. GLBA imposes rules on the privacy of financial information about customers and sets standards on how to protect this information.

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

- **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.

- **Federal, State and Local Governments**
  The Freedom of Information Act (FOIA) gives citizens the right to request access to records held by any federal entity other than Congress or the Judicial branch (most states and many local governments have similar provisions known as "open-records" or "sunshine" laws.) The current administration has directed federal 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.

- **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 nations, regions, and economic blocs have their own set of regulations, such as the EU Data Protection Directive for data privacy in the European Union, as well as similar regulations for financial services organizations in the United Kingdom. There are many compliance obligations that are an important or critical consideration for organizations that have deployed or may deploy Office 365, 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
Top Ten Regulations That Impact Organizations
Percentage Indicating "Important" or "Critical" Considerations

Regulation	%
Health Insurance Portability and Accountability Act (HIPAA)	38%
Sarbanes-Oxley Act of 2002	28%
Federal Information Security Management Act of 2002 (FISMA)	22%
Gramm-Leach-Bliley Act (GLBA)	21%
Federal Rules of Civil Procedure	17%
Family Educational Rights and Privacy Act (FERPA)	15%
Dodd-Frank	14%
US-EU Safe Harbor Framework	14%
SSAE 16	13%
SEC Rule 17a-4	12%

Source: Osterman Research, Inc.

REGULATIONS AND COMPLIANCE ARE COMPLEX

Regulatory and legal compliance is a complex undertaking. There are many regulations and compliance requirements for all organizations, and an awareness of these is essential to avoid the penalties that can result from non-compliance. 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 nation, industry, legal jurisdiction and business function. For organizations that operate across multiple nations or across multiple industries, defining an internal compliance approach is 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 might be seven years, another may require only three years of retention.

- Compliance with regulatory obligations 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.

Decision makers should engage compliance professionals to ensure they are operating in alignment with current requirements and best practices.

There are many regulations and compliance requirements for all organizations, and an awareness of these is essential to avoid the penalties that can result from non-compliance.

COMPLIANCE IN AN IDEAL WORLD

Because 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 information at the right trigger point, classifying this data for retention, and storing each form of data in a tamper-proof repository, in a search-ready state, for as long as necessary. When records can be deleted, it should occur swiftly with a carefully prescribed plan for "defensible deletion". Employees must 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 content**
  The organization should be able to demonstrate appropriate actions taken to address this type of content. This should 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**
  Decision makers should employ systems, policies, and training to minimize the compliance risks in an organization, such as inaccurate identification of content for retention, systematic failures to delete appropriate content, and insufficient care by employees in following corporate policies. Increasingly, analytics capabilities are being applied on top of archived content to identify information which could pose security, compliance or legal risks to the organization. These capabilities can proactively surface communications content which may put the organization at risk, and enable the company to address it before it becomes a large problem.

COMPLIANCE AND eDISCOVERY IN OFFICE 365

MICROSOFT'S APPROACH TO COMPLIANCE IN OFFICE 365

While Microsoft has taken great pains to provide compliance capabilities in Office 365 – and has done a good job at doing so – we believe there are some weaknesses with Microsoft's approach to eDiscovery in Office 365 when organizations operate a hybrid environment of Office 365 and on-premises solutions. Let's look at the evidence to support our contention.

While Microsoft has taken great pains to provide compliance capabilities in Office 365 – and has done a good job at doing so – we believe there are some weaknesses with Microsoft's approach…

INCOMPLETE CAPTURE OF CONTENT

Organizations cannot find what they have not captured, and eDiscovery requires a foundation of content completeness. Office 365 does not support the full capture of content, nor its retention if captured. For example:

- **Deleted email purged after 14 days**
  Unless the user's Exchange Online mailbox is on legal hold, email they delete from their mailbox is moved to a hidden folder and then purged 14 days later. In Exchange Online, the 14-day timeframe can be increased to a maximum of 30 days.

- **Partial capture of Skype for Business content**
  By default, conversations in Skype for Business (and Lync before that) are stored in the user's Conversation History folder in Outlook. However, this setting can be turned off by the user with a simple click. Even with it turned on, however, only text-based instant messaging interactions and file upload actions into meetings are captured; peer-to-peer file transfers, audio and visual interaction for instant messages and conferences, application sharing, and conferencing annotations are not captured. The capturing of instant messaging conversations can be forced, but only by putting the user's mailbox on legal hold.

- **Deletion of Skype for Business meeting content**
  Attachments to a Skype for Business meeting are deleted after eight hours (for ad hoc meetings) and 15 days (for one-time and recurring meetings, with the 15 days counter starting at different times for each type of meeting).

- **No capture of Yammer content**
  Content in Yammer is not captured for archiving, even though it is a core part of the Office 365 offering. With new Yammer capabilities supporting sharing and collaboration scenarios with external parties, the archive is blind to what happened, and thus eDiscovery is too. Customers do have the option of including Yammer content, but only in conjunction with a third-party ingestion service.

- **Audit reports deleted after 90 days**
  Reports of actions taken by IT administrators and people who have access to the mailbox of another user are retained for 90 days and then deleted. Office 365 cannot report on actions taken more than 90 days prior to an eDiscovery content search since the data is not stored.

THE ARCHITECTURE REQUIRES THAT ALL MAILBOXES ARE CONSTANTLY ON LEGAL HOLD

Entire user mailboxes must be placed on legal hold in order for certain types of data to be captured and archived in Office 365. For example:

- **Skype for Business and Lync**
  Instant messaging conversations from Skype for Business (or the previous generation of Lync) will be archived into the user's mailbox only if their mailbox is placed on legal hold. Instant messaging conversations are captured by default by the Skype for Business client and stored in a folder in Outlook, but this can be turned off by the user. Putting the mailbox on legal hold forces the capture.

- **Third-party data sources**
  Microsoft's recent foray into supporting the ingestion of non-Office 365 data sources for archiving and eDiscovery in Office 365 requires that the user's mailbox be set to In-Place Hold in order for archiving to work.

In addition, some information is available only in an eDiscovery search if legal hold is turned on. Specifically, BCC information for emails are stored in the sender's mailbox, which must be on hold in order for that information to be returned. The logical implication, therefore, is that in order to uncover BCC information, *all* mailboxes need to be on legal hold during an eDiscovery search, and relatedly, if a sender's mailbox is deleted before a three to seven year retention period for email data, that information will not be available.

If the legal hold mechanism – which is conceptually intended to be used to prevent the deletion of data in face of a pending or current lawsuit – is permanently required in order for basic capture and search processes to work, organizations will retain far too much data and may be unable to defensibly delete over time. That said, some industries are obligated to retain some types of information for long periods and so operate under a sort of permanent, de facto legal hold.

This means that organizations will bear the additional risk of storing what could be very large amounts of data for long periods without the ability to defensibly delete this content and thereby reduce their corporate risk. Many third-party solutions do not suffer from this limitation and should be considered not only from the perspective of reducing storage requirements, but, more importantly, from the perspective of reducing the risk of retaining too much content.

….organizations will bear the additional risk of storing what could be very large amounts of data for long periods without the ability to defensibly delete this content and thereby reduce their corporate risk.

A PROLIFERATION OF eDISCOVERY APPROACHES ACROSS MICROSOFT'S OWN PRODUCTS

Microsoft does not offer a unified approach to eDiscovery across its tools, but instead there is an ever-changing roster of capabilities that differ by product and product version. For example:

- **Exchange Server 2016**
  Organizations quick to embrace Exchange Server 2016 can search both on-premises Exchange 2016 mailboxes and public folders, as well as Office 365-based mailboxes and public folders in the same search. In-Place eDiscovery in Exchange 2016 cannot search non-Exchange content. When searching public folders, the only option is to search all public folders, and all public folders must be put on hold (there is no granularity to support only putting specific public folders on hold).

- **SharePoint Server 2013**
  The eDiscovery Center in SharePoint Server 2013 works only with SharePoint 2013 and Exchange 2013; earlier versions of Exchange Server are not supported. The eDiscovery Center can search for content in SharePoint on-premises, but for architectural reasons is unable to search SharePoint Online. A separate eDiscovery Center is required for SharePoint Server 2013 on-premises and SharePoint Online.

- **Office 365 Security & Compliance Center**
  The recently released Security & Compliance Center can search content in SharePoint Online, Exchange Online (mailboxes and public folders), OneDrive for Business, and Office 365 Groups. It does not search other Office 365 content natively – such as Yammer – and does not search any on-premises content.

For compliance and legal professionals, the problems with this approach include:

- **Multiple eDiscovery cases**
  Multiple eDiscovery searches and legal holds will need to be initiated and managed through different Microsoft products. The Office 365 Security & Compliance Center does not search on-premises content, requiring a second eDiscovery search and case to be established using the appropriate on-premises tools.

- **Competence in multiple products**
  eDiscovery is fraught with business risk – fail to find the right or all relevant data and your organization is likely to face punitive damages. Produce too much data and generally the costs of human review escalate. For legal professionals, having to learn multiple approaches to eDiscovery just to carry out an eDiscovery search, establish a case, and instantiate a legal hold adds risks about inadvertent user error.

For IT professionals, the problems include:

- **Security permissions across products**
  In order for authorized compliance professionals to manage eDiscovery searches and case work across different products, IT professionals need to manage security and permissions across different products.

- **Forced maintenance of legacy infrastructure**
  With eDiscovery cases and legal holds managed in older versions of Exchange Server or SharePoint Server, IT professionals must support these older products until all outstanding eDiscovery and legal hold situations have been resolved.

- **Significant complexity on upgrades**
  Upgrades across any or all of the various Microsoft solutions will add further complexity to the issues noted above.

In summary, relying on Microsoft for eDiscovery means that there are various product- and version-specific eDiscovery capabilities that will need to be simultaneously used, managed, and maintained over time. This creates unnecessary complexity and risk in an area already fraught with enough business risk and operating stress. The use of third-party solutions can provide remedies to many of these issues.

Microsoft frequently changes its approach to archiving and eDiscovery without providing migration options from the current approach to the new approach.

MICROSOFT FREQUENTLY INTRODUCES NEW eDISCOVERY APPROACHES WITH NO MIGRATION PLAN

Microsoft frequently changes its approach to archiving and eDiscovery without providing migration options from the current approach to the new approach. For example, the new Office 365 Security & Compliance Center is a significant step forward for Microsoft compared to its previous approaches in Office 365, but existing cases in the previous SharePoint Online eDiscovery Center could not be migrated since the cases are "*completely different objects, and their underlying architecture is also different*."[v]

SUPPORTS ONLY BASIC SUPERVISORY REVIEW

The new Office 365 Security & Compliance Center introduced basic supervisory review capabilities. The capabilities are basic because:

- **Only supports email**
  Supervisory Review supports only email in Exchange Online, despite the growing use of other forms of electronic communication that are subject to compliance requirements and supervision oversight. As of this writing, Supervisory Review supports only email, not Skype for Business or other Office 365 applications.

- **Add-In app for Outlook**
  Emails marked for supervisory review can be accessed only using a special add-in app for Outlook, which needs to be installed by an IT administrator using PowerShell.

- **No pre-review content analysis**
  While messages can be captured for review by a person, there are no capabilities in Office 365 to perform content analysis on captured messages in advance of human review to signal potential problems.

- **Only basic workflow for incident management**
  Incidents are managed by dragging non-compliant or questionable messages into specially marked folders within the Outlook app. There are no real workflow capabilities for addressing identified problems.

Organizations with supervisory review requirements generally need capabilities beyond what is offered in Office 365.

Deleting a user from Exchange Server on-premises will also delete their archive in Office 365.

NOT ALL CONTENT CAN BE PUT ON HOLD

Office 365 does not offer complete coverage of content from a hold perspective, even for email messages. In-Place Hold and Litigation Hold cannot be applied to emails sent using IMAP or POP clients, or to custom applications that use the SMTP protocol.[vi]

There are similar challenges with the eDiscovery Center in SharePoint on-premises. For example, in SharePoint 2013 eDiscovery Center a file on a file share whose file name is longer than 259 characters cannot be discovered, there is no mechanism for searching line-of-business applications, nor is there a native mechanism for indexing image files. In short, there is no absolute guarantee that all content relevant to a case will be discovered.

LEGAL HOLD DOES NOT GUARANTEE IMMUTABILITY

Immutability of data storage is required by most regulations (such as those from the SEC), meaning that data cannot be deleted if it is not cleared for deletion, such as when it is under legal hold or subject to retention settings. Microsoft's approach to compliance and eDiscovery does not guarantee immutability. Specifically, if a user is deleted from Active Directory, the following will happen:

- **Mailbox deleted even if under legal hold**
  In Exchange Server 2016, the user's mailbox will be marked for deletion, even if it is under legal hold, and after a certain timeframe will be expunged from the Exchange message store.[vii]

- **Office 365 archives will be deleted**
  Deleting a user from Exchange Server on-premises will also delete their archive in Office 365. This process can be reversed by contacting the Office 365 Support

Team, but this action must be done within 30 days of deleting the user, otherwise the archive mailbox is unrecoverable.

- **OneDrive for Business site deleted**
  After removing a user account, his or her OneDrive for Business site will be deleted after 30 days unless recovery action is taken. The same is true for users of SharePoint Online My Site accounts.

Exchange administrators also have super-user privileges to search for and delete email across multiple mailboxes. While this is intended for the deletion of inappropriate email, and any deletion actions are logged for 90 days, messages can still be deleted without trace under certain circumstances.

CONFUSED INCENTIVES FOR MICROSOFT

There is a need for communication and collaboration environments with innovative tools to support day-to-day interactions, but also to provide a long-term archiving and eDiscovery capabilities to support compliance requirements. These two business needs can conflict, as evidenced in the following actions:

- **SharePoint Server 2013 and Exchange Server 2013**
  The eDiscovery Center in SharePoint Server 2013 mandated the use of Exchange Server 2013 in order for searches to work across both SharePoint content and Exchange mailboxes. Support for earlier versions of Exchange Server were not supported, forcing organizations to upgrade Exchange in order to get cross-product coverage.

- **Advanced eDiscovery for 2016 Server Editions**
  Microsoft's new Advanced eDiscovery capability in Office 365, built on the Equivio Zoom technology acquired in early 2015, is supposed to be extended to support on-premises content in addition to Office 365. However, this will work only for SharePoint Server 2016 and Exchange Server 2016.

There remains a fundamental tension – and perhaps it is an irreconcilable conflict – between the desire for rapid innovation on the user front end, and support for long term archiving and eDiscovery in the background. Microsoft is proving itself on the first challenge with Office 365, but is lagging on the second.

MICROSOFT'S APPROACH LEADS TO BUSYWORK

The design of Microsoft's eDiscovery capabilities for Office 365 and on-premises servers require ongoing manual processes to work. For example:

The design of Microsoft's eDiscovery capabilities for Office 365 and on-premises servers require ongoing manual processes to work.

- **Content searches not kept up-to-date**
  Content searches for responsive content are not automatically kept up-to-date. Compliance professionals must re-run each content search to locate any new results since the last time it was run.

- **Permissions must be set in multiple places**
  Permissions related to eDiscovery and compliance have to be setup in different places across Office 365, including the Security & Compliance Center, Exchange Admin Center, and SharePoint Online.

- **No migration of content searches**
  Content Searches started in the Security & Compliance Center cannot be moved into an eDiscovery case. They must be recreated after a case has been established.

- **Interlinked upgrades for new features**
  IT administrators must manage interlinked upgrades in order to get advantage of new features. Want to use eDiscovery in SharePoint Server 2013? Upgrade to

Exchange Server 2013 as well. For SharePoint Server 2016? Ditto.

- **Multiple searches to find all responsive messages**
  One must create multiple searches to find all of the responsive messages. For example, one search must be initiated in Exchange 2016 to include IRM-protected messages that cannot be indexed, while a second search must be initiated to include messages that contain an .rpmsg attachment.

OTHER ISSUES TO CONSIDER

In addition to the issues discussed above, there are certain other problems with Microsoft's approach to archiving, eDiscovery, and regulatory compliance:

- **Microsoft sees everything as an email**
  When ingesting content from third-party communication systems and social networks – such as Facebook, LinkedIn, Twitter, and Thomson Reuters – all content is forced into the body of an email message for storage in the user's Exchange Online mailbox. While the content of the specific interaction may be captured, the native presentation and surrounding context is difficult to re-create authentically, e.g., expanding a conversation thread from a Facebook or LinkedIn post.

- **Unique names for content searches**
  In the Office 365 Security & Compliance Center, the name of a content search must be unique across the entire Office 365 organization. This includes content searches the current user cannot see, and content searches in eDiscovery cases. It is our view that could lead to the inadvertent disclosure of legally privileged information regarding current litigation. For example, if a name was disallowed for a new content search, then by implication that same name was in place for an existing search, revealing potentially sensitive information.

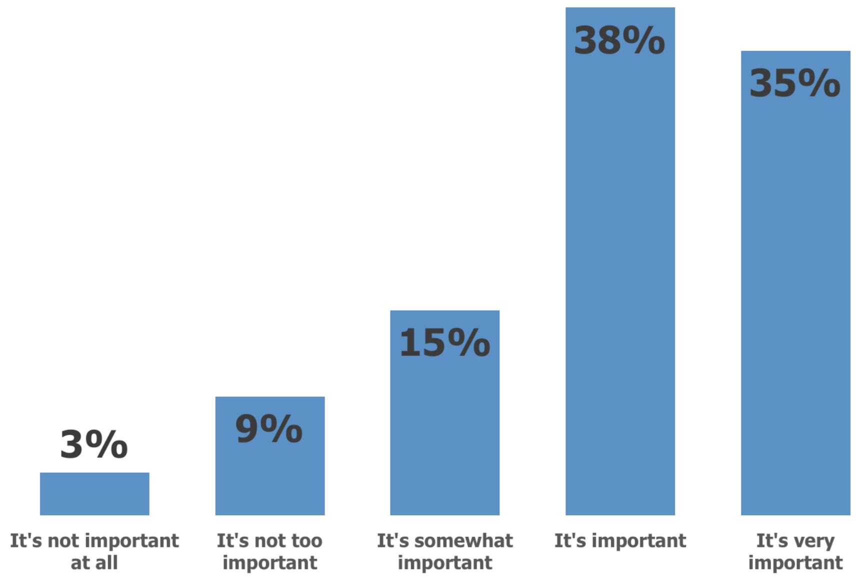
- **Add SharePoint and OneDrive for Business sites by URL**
  The Office 365 Security & Compliance center does not offer the ability to select SharePoint sites or OneDrive for Business sites by name, nor to navigate to them in a visual hierarchy. Instead, these must be entered by URL.

- **Retention tags and policies for hybrid Exchange**
  Retention tags and policies define the default duration for which a message should be retained. There is no automated way to keep retention tags and policies in sync across Exchange on-premises and Exchange Online. An administrator must manually export all current retention tags and policies from Exchange on-premises, and then import all tags and policies into Exchange Online. It's a manual process. It's all or nothing. And the destination tags and policies are overwritten by the new ones.

- **Use of a single archive for all content**
  Every organization should aspire to the use of a single, comprehensive archive for all of their content in order to minimize the complexity of eDiscovery or compliance efforts and to reduce the cost and complexity of managing archived content. The importance of having a single archive for eDiscovery and compliance was corroborated by our survey respondents, as shown in Figure 4.

Every organization should aspire to the use of a single, comprehensive archive for all of their content…

Figure 4
Importance of Having a Single Archive for eDiscovery and Compliance Purposes



Source: Osterman Research, Inc.

THIRD PARTY TOOLS FOR COMPLIANCE

While Microsoft offers a basic and somewhat flawed approach to eDiscovery and regulatory compliance in Office 365 and hybrid configurations, several third-party vendors provide fit-for-purpose capabilities that meet the modern archiving, eDiscovery and regulatory compliance requirements faced by organizations around the world. For example, third-party vendors offer capabilities to help organizations manage compliance more effectively and efficiently by:

- **Unifying eDiscovery search, legal hold and export**
  Offering archiving and eDiscovery systems and cloud services designed for multiple native data formats, multiple source systems across cloud services and on-premises servers, and multiple generations of those systems means that third-party vendors offer a unified approach for compliance professionals.

- **Respecting native data formats and preserving critical metadata**
  When ingesting data from external services such as Facebook, Twitter, and even its own Yammer service into Office 365, Microsoft forces all content into the body of an email message. Some third-party archiving and eDiscovery vendors don't force such an unnatural conversion process, as a consequence of architecting their archiving and eDiscovery capabilities to handle data formats in natural form beyond just email. Among other benefits, this enables the accurate contextual re-creation of messages and interactions from other services. A big concern with conversion is the loss of metadata which is critical in an eDiscovery scenario.

- **Offering real supervision review**
  While enabling the supervisory review of email messages is a necessary first step, it is not sufficient to meet the requirements. Supervisory review requires the ability to review more than just email, and organizations require workflow and escalation capabilities to handle violations. Supervisory review is mandatory for financial organizations as part of the FINRA rules. Failing to do proper supervision of all communications (email and social) could result in significant

Several third-party vendors provide fit-for-purpose capabilities that meet the modern archiving, eDiscovery and regulatory compliance requirements faced by organizations around the world.

fines.

- **Providing capabilities for proactive compliance management**
  Organizations need to stay ahead of potential compliance violations by getting early warning of developing situations. Third-party vendors offer real-time content analysis to identify sensitive data, privacy violations, and inappropriate patterns in communication.

- **Enforcing enterprise-wide DLP policies**
  The DLP policies in Office 365 cannot, by default, be applied to systems beyond Office 365. Third-party vendors enable an enterprise-wide approach to the use of DLP policies, by automatically applying what has been configured in Office 365 to other online and on-premises environments, including file shares and even structured databases.

- **Synthesizing actionable dashboards**
  With an ever-changing set of data in Office 365 and on-premises environments, compliance professionals need to know the current state of risk and prioritize their response across multiple competing demands. Third-party vendors can analyze content at rest and in motion within the organization's Office 365 tenant, and provide a visual dashboard to facilitate the prioritization of corrective action.

SUMMARY

While Microsoft is making forward strides with its eDiscovery capabilities, there are a number of limitations and weaknesses in its approach. Osterman Research recommends that every organization evaluate the capabilities of third-party vendors and select the right approach in light of their requirements profile. Since Office 365 is built first-and-foremost as a day-to-day communication and collaboration environment – an area that Microsoft is hotly contesting against Google, Slack, Huddle, and other new entrants – its eDiscovery and regulatory compliance capabilities are lacking in capability for most organizations. Due to conflicting design goals between day-to-day interaction and long-term retention, and the incentives within Microsoft to push hard on the roll-out of new versions of its tools, organizations should be careful about proceeding with a Microsoft-only approach to eDiscovery and compliance. Meeting compliance requirements and delivering on the demands for eDiscovery is not an area to embrace sub-optimal tools and hope for the best.

SPONSOR OF THIS WHITE PAPER

Archive360 Delivers Email Archiving Migration Solutions and the Industry's First Compliance Storage Solution Based on the Microsoft Azure Platform.

Archive360, Inc. provides next generation email archive migration software solutions and cloud-based storage for regulatory compliance, legal, and low touch or grey unstructured data. Archive360's flagship solution offering is *Archive2Anywhere™*, a data migration platform that integrates with the most popular data sources and target repositories for fast and defensible archive migrations.

The cloud-based *Archive2Azure™* is a managed compliance storage solution based on Microsoft Azure. It is delivered as part of the Archive2Anywhere™ platform and is the industry's first solution allowing for management of departed employee data and complete elimination of legacy email archives and other low touch or 'grey' data.

ARCHIVE360
POINT. CLICK. MIGRATE. STORE.

www.archive360.com

@Archive360

info@archive360.com

+1 630 358 4448

Osterman Research, Inc. does not provide legal advice. Nothing in this document constitutes legal advice, nor shall this document or any software product or other offering referenced herein serve as a substitute for the reader's compliance with any laws (including but not limited to any act, statute, regulation, rule, directive, administrative order, executive order, etc. (collectively, "Laws")) referenced in this document. If necessary, the reader should consult with competent legal counsel regarding any Laws referenced herein. Osterman Research, Inc. makes no representation or warranty regarding the completeness or accuracy of the information contained in this document.

THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND. ALL EXPRESS OR IMPLIED REPRESENTATIONS, CONDITIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE DETERMINED TO BE ILLEGAL.

REFERENCES

[i] https://technet.microsoft.com/en-us/library/exchange-online-limits.aspx#StorageLimits

[ii] http://legalref.judiciary.gov.hk/lrs/common/ju/ju_frame.jsp?DIS=71431&currpage=T

[iii] http://www.wassom.com/wp-content/uploads/2013-DNJ-Gatto-spoliation.pdf

[iv] http://archivesocial.com/blog/social-media-recruitment/

[v] Microsoft Office Support, Manage eDiscovery cases in the Office 365 Security & Compliance Center, July 2016, at https://support.office.com/en-us/article/Manage-eDiscovery-cases-in-the-Office-365-Security-Compliance-Center-edea80d6-20a7-40fb-b8c4-5e8c8395f6da.

[vi] Microsoft TechNet, Compliance and Security Features in Exchange Online Archiving, May 2016, at https://technet.microsoft.com/en-us/library/compliance-and-security-features-in-exchange-online-archiving.aspx.

[vii] Microsoft TechNet, In-Place Hold and Litigation Hold in Exchange 2016, July 2016, at https://technet.microsoft.com/en-us/library/ff637980%28v=exchg.160%29.aspx.