eDiscovery and Information Governance in Office 365
ARMA Chicago – April 12, 2016

John P. Collins, JD | DTI | Director, Information Governance Solutions & Office 365 Consulting
Contact Information

• **John P. Collins, JD**
  – Director, Information Governance & Office 365 Consulting
  – Phone: (312) 262-9509
  – Email: john.collins@dtiglobal.com

Director, Information Governance Solutions and Office 365 Consulting Services. John works with corporations on a wide range of eDiscovery readiness, information security, RIM, and Office 365 consulting engagements. DTI has developed the nation’s first consulting practice focused specifically on eDiscovery and Information Governance in the most widely used cloud business application, Office 365. John oversees the team which assesses, implements, and manages eDiscovery and IG processes in Office 365.
Agenda

- Why a briefing on Information Governance and E-Discovery in Office 365?
- What is Office 365 and how does it work?
- What types of data may be found in Office 365?
- eDiscovery features in Office 365
- Information Governance features in Office 365
- Learning about and keeping up with Office 365
Why a briefing on Information Governance and E-Discovery in Office 365?
Why a briefing on Information Governance and E-Discovery in Office 365?

• 84% growth in # of seats year-over-year

• 1 in every 4 Microsoft enterprise customers uses Office 365

• Office 365 is Microsoft’s fastest growing commercial product ever

• Office 365 recently eclipsed Salesforce.com as the most widely used cloud-based business application

• “Commercial cloud revenue grew 88% (up 96% in constant currency) driven by Office 365, Azure and Dynamics CRM Online and is now on an annualized revenue run rate of over $8 billion” from Microsoft Press Release
Why a briefing on Information Governance and E-Discovery in Office 365?

- The data being moved to Office 365 is:
  - Among the most highly targeted and sought in discovery
  - And is largely “unstructured” (requiring governance and structure in order to be managed effectively)
Why are organizations of all types and sizes moving to Office 365?

• Cost
  – Dollars per user for email, SharePoint, IM, collaboration, etc.

• Easier to deploy and manage
  – Less infrastructure to integrate and manage

• Focus on more strategic engagement
  – Email and file storage/sharing considered commodity services

• Built to be deployed on multiple devices and available 24/7
  – Mobile and cloud first! Microsoft's mantra
Dynamics introduced by moving to Office 365

• New content types
  – NEW! Planner
  – Sway
  – SharePoint specific content
  – Voice mail preview

• New storage locations
  – OneDrive for Business
  – Yammer
  – Office 365 Groups

• Change
  – Persistent, continuous, and at high velocity

• Lower bar to deployment
  – Heavy IT integration and configuration is handled by Microsoft
  – Easier to deploy and consume features such as Instant Messaging, collaboration, Information Rights Management, etc.
What is Office 365?
What is Office 365?

• **Suite of Services/Products**
  - E-mail, Instant Messaging, Collaboration, File Storage
  - Office (Word, Excel, PowerPoint, Access, etc.), Exchange, SharePoint, Skype for Business

• **Cloud**
  - Quintessential example of cloud computing
  - Hardware, storage, backup and disaster recovery are handled by Microsoft

• **Software as a Service (SaaS)**
  - Individuals, companies, organizations subscribe to the service for a fixed monthly or annual fee

• **Brand**
  - Microsoft is labeling products and services as “Office 365” or part of Office 365 (Project for Office 365, Dynamics CRM, etc.)
The five fundamental components of Office 365

1. Yammer
   - Collaboration (Team Site)
   - Posts/Updates
   - File upload
   - Announcements
   - Polls, Praise
   - Groups
   - Like, unlike, share

2. Skype for Business
   - Instant Messaging
   - "Presence"
   - Skype to Skype (VoIP) calls (audio and/or video)
   - Online meetings

3. SharePoint
   - Collaboration (Team Site)
   - Intranet/Portal
   - Blog, Wiki
   - File Storage (OneDrive for Business, Video Portal, etc.)
   - Application development
   - Enterprise Content Management (ECM)
   - Public web site

4. Exchange
   - E-mail
   - Unified Messaging (voice mail)
   - Contacts
   - Shared Calendar
   - Tasks
   - Notes
   - Journal
   - Exchange Public Folders

Social media for "the enterprise"
How does Office 365 work?
How does Office 365 Work?

**Backend infrastructure resides in Microsoft’s data centers**

**Backup and disaster recovery controlled by Microsoft**

*Image of Office 365 Datacenters*

Highly specialized hardware configured specifically for Office 365
How does Office 365 Work?

Unlike many SaaS applications, Office 365 has a robust locally installed "client" software component: Office.
What types of data may be found in Office 365?
What types of data may be found in Office 365? Exchange

• Similar to on-prem Exchange
• Additional considerations:
  – Site mailboxes (tied to SharePoint site)
  – Exchange Public Folders
What types of data may be found in Office 365? Skype for Business

• Skype meetings can be recorded

• Instant Messages (chats)
• Voice and video call logs
• Web meeting recordings
What types of data may be found in Office 365? SharePoint

- SharePoint is a platform, not just a single application
- It can serve multiple purposes and do many things...
SharePoint’s “roles”

• **Collaboration**
  – Team Sites: collaboration between one or more internal users

• **Extranet**
  – Collaboration between internal AND external users

• **Intranet**

• **Public web site**

• **Application Development**
  – Create wide variety of applications to support business processes

• **Enterprise Content Management (ECM)**
  – Document and records management; web and digital asset management

• **File storage and sharing (OneDrive for Business)**
  – Replace file shares and “MY DOCUMENTS”

• **Document storage (glorified file shares)**
What types of data may be found in Office 365? SharePoint

- **Files that can be uploaded into SharePoint include, but are not limited to:**
  - Word
  - PowerPoint
  - Excel
  - PDF
  - Open Office
  - CAD, CAM, etc.
  - Video
  - Audio
  - Image
  - CSV
  - Almost every type of file can be uploaded into SharePoint…

- **Files and web pages that can be created via SharePoint include but are not limited to:**
  - Standard web pages with links, images, document libraries, etc.
  - Sway
  - Blog
  - Wiki
  - Survey
  - Announcements
  - List items

- **Files and content that can’t be uploaded into SharePoint:**
  - .ashx
  - .asmx
  - .json
  - .soap
  - .svc
  - .xamlx
eDiscovery features in Office 365
In a nutshell: eDiscovery Features in Office 365

• “Standard” eDiscovery
  1. Search across one or more mailboxes and SharePoint sites
  2. Preserve Exchange/Outlook, SharePoint, and Skype for Business content
  3. “Preview” preserved content
  4. Collect and export Exchange/Outlook, SharePoint, and Skype for Business content
“Advanced” eDiscovery (Equivio Zoom)
- Near-duplicate detection
- Thread analysis
- Predictive coding ("relevance")
- Themes and Search

Defensibly reduce the volume of ESI sent outside the organization’s four walls
Enabling Defensible Legal Hold: Recoverable Items Folder

- Users do not have access to the recoverable items folder
- eDiscovery search and hold does have access
Enabling Defensible Legal Hold: Preservation Hold Library

- A “preservation hold library” is created the first time a SharePoint site is put under hold.
- Users can continue to work on content without disruption.
- Content on hold—including web pages, documents, lists, and other items—are preserved as needed (if user edits an item it prompts preservation).
- Users don’t see the preservation hold library.
- To preserve all versions of content in a site, versioning must be enabled.
What ESI in Office 365 is subject to the built-in eDiscovery tools?

- **Yes**
  - Skype for Business
    - Instant Messaging chats
    - Voice and video call logs
  - SharePoint
    - Files of all types (Word, PowerPoint, Excel, PDF, Visio, CAD, audio, video, “Sway,” and more)
    - Sites, web pages (blog, wiki, discussions, and more)
    - “App” content (calendar, survey, newsfeed, announcements)
  - Exchange
    - E-mail & attachments
      - Contacts
      - Calendar
      - Tasks
      - Notes
      - Journal

- **No**
  - Exchange Public Folders
  - Outlook Web App “Groups” (rolling out)

New!

- Yammer
  - Meeting content, recorded meetings

- Planner
What DOESN’T Office 365 eDiscovery do?

• Legal hold notification and workflow
  – Telling custodians they are on hold and tracking acknowledgements
  – Sending out questionnaires
  – Providing audit trail of when and who is on legal hold

• Does not identify, preserve, or collect ESI located outside of Office 365—for example:
  – Desktop, laptop, tablet computers
  – File (network) shares
  – Smartphones

• Processing
• Review
• Production
Information Governance Features in Office 365
Information Governance features in Office 365

• Retention & Disposition
  – In-Place Archive (Exchange)
  – Document deletion policies (SharePoint)
  – Information Management Policies (SharePoint)
  – Messaging Records Management (MRM) (Exchange)
  – Records Management (SharePoint Records Center) (SharePoint)
  – Site Closure Policies (SharePoint)

• Information Security
  – Data Loss Prevention (Exchange)
  – Encryption (Exchange)
  – Information Rights Management (IRM) (Exchange, SharePoint)

• Auditing (All Office 365 components)
• Mobile Device Management (MDM) (Exchange)
• Transport Rules (Exchange)

NOTE: terminology used by Microsoft for IG and eDiscovery related features is “Security and Compliance”
IG features in Office 365: Retention & Disposition
IG features in Office 365: In-Place Archive (Exchange)

- NOT the type of archiving associated with dedicated archiving tools such as Enterprise Vault, SourceOne, Legato, etc.
- Provides additional storage capacity for email
- Emails can be moved into the archive via several methods:
  - Move or copy by user
  - Inbox rules
  - Retention policy
- Key benefit is elimination of need for off-server storage (such as PST files)
• Email management framework
• Employs a “tagging” paradigm
• Tags get applied to:
  – Entire mailbox OR a folder OR an individual message/item
• Multiple tags can be created, for example:
  – 1 year (delete all items after one year)
  – 5 year (retain item or items in folder for 5 years)
  – Archive (move Inbox items to archive mailbox after 6 months)
• Policies:
  – Can aggregate tags into distinct policies (Executive Policy, VP Policy, Legal Dept. Policy, etc.)
• Legal hold suspends deletion
IG features in Office 365: Document Deletion Policies (SharePoint)

• A policy framework for SharePoint
  – Applies to site collections, sites, OneDrive for Business

• Not a records management oriented approach
  – Keep for X number of years then delete

• Multiple policies depending on need:
  – Policy for OneDrive for Business
  – Policy for internal team sites
  – Policy for extranets

• Legal hold suspends deletion
IG features in Office 365: Information Management Policies (SharePoint)

• Framework for
  – How long to retain files and content
  – Audit actions taken on files and content

• Provides various options for what happens to files and content
  – Delete
  – Start a workflow
  – Etc.

• Implementation requires planning, training, careful thought
  – Can apply policies at the site collection, site, or library level
• Out of the box, SharePoint provides a framework to implement records management

• Three possible approaches:
  – “In-Place:” leave document in current location but declare it as a record
  – “Records Center:” documents are moved into a centralized repository within SharePoint and managed as records there
  – Hybrid
• Close and/or delete SharePoint sites automatically
  – Trigger can be site creation or close date
• Make closed sites read-only
• Can create a workflow (such as an approval process) if desired
• Options available to extend period prior to deletion
IG features in Office 365: Information Security
IG features in Office 365: Data Loss Prevention (DLP)

- DLP policies contain sets of conditions which filter messages and attachments
- DLP policies employ:
  - Rules: for example, if a sequence of numbers such as 123-12-1234 appear
  - Actions: if 123-12-1234 appears, do not send the message
  - Exceptions: its ok to send the message if the sender is John Doe
- Target PII, PHI, credit card numbers, social security numbers, drivers license numbers, etc.
- Use out of the box templates, create custom rules, or import rules created by 3rd parties
IG features in Office 365: Encryption

• Multiple options available to implement a program to encrypt sensitive information in email
  
  • Office Message Encryption (OME)
    – Works with internal and external recipients
    – No special software required by recipients (don’t have to be on Office 365)
  
  • Secure/Multipurpose Internet Mail Extensions (S/MIME)
    – Uses certificates in a private-public key framework
    – Includes digital signature
• Encrypts files and limits programs and users who are allowed to decrypt

• Limits what users can do:
  – Email: who can access, forward, print, or copy sensitive data
  – SharePoint: limit actions users can take on files such as read-only (can't edit), copying and printing

• Can be configured to be in effect for set period of time (expiration)

• Email rules:
  – Can configure rules to apply IRM to certain messages (for example, messages containing word “confidential”)
Additional IG features in Office 365
IG features in Office 365: Mobile Device Management

- Different than Exchange Active Sync (EAS) and if EAS is enabled it is superseded by MDM
  - Requires Office 365 license
- Manage iPhones, iPads, Androids, and Windows Phones (NOTE: Blackberry has a specific service offering through Microsoft)
  - Requires Office 365 license
- Users can still access SharePoint and Outlook Web App via browser (MDM does not control)
- Selective wipe!
IG features in Office 365: Auditing

- Tracks changes made by BOTH Microsoft and subscriber
- Audit reports can be viewed and downloaded
- Audit data available for 90 days (longer in some instances—this is a moving target)

- Reports include:
  - Litigation holds & eDiscovery searches
  - Mailbox access by non-owners (delegates)
  - Admin activity (admin audit logging) in Exchange Online
  - Access to mailboxes (mailbox audit logging) in Exchange Online
  - User activity in SharePoint Online and OneDrive for Business
  - Admin activity in SharePoint Online and OneDrive for Business
  - Admin activity in Azure Active Directory (the directory service for Office 365)
  - User sign-in activity in Azure Active Directory

- 3rd party audit tools more robust (API available)
- Compliance Center reporting in deployment (provides additional reports)
Key IG and eDiscovery considerations
Learning about eDiscovery and IG in Office 365

Office 365 security and compliance

26 out of 44 rated this helpful - Rate this topic

Applies to: Office 365 Enterprise, Office 365 Midsize Business

Topic Last Modified: 2015-10-29

Microsoft Office 365 is designed to help meet your organization’s needs for content security and data usage compliance with legal, regulatory, and technical standards. Setting policies and enabling services that optimize these conditions is an important part of administering Office 365. To establish a secure and compliant Office 365 work environment that meets your organization’s requirements, you may want to learn more about the topics of security and compliance described in this topic.

The following table describes the Office 365 features that are available to help you with fulfilling your organization’s security and compliance needs.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Office 365 Compliance Center</td>
<td>You can use the Office 365 Compliance Center to manage compliance across Office 365, Exchange Online, and SharePoint Online. It can manage archive mailboxes, discovery cases, auditing reporting, and retention and deletion policies in Exchange Online and SharePoint Online. You can also assign permissions to compliance managers in your organization so they can access some or all of the compliance features in the Compliance Center.</td>
</tr>
<tr>
<td>Import PST files to Office 365</td>
<td>Use the Office 365 Import Service to import PST files to Exchange Online mailboxes or import data files to your SharePoint Online organization. For both types of files, you can upload the files over the network or copy them to a hard drive and then ship the drive to a Microsoft datacenter, where the data will be imported to Office 365.</td>
</tr>
<tr>
<td>Anti-spam and anti-malware protection in Office 365</td>
<td>Office 365 has built-in malware and spam filtering capabilities that help protect inbound and outbound email messages from malicious software and help protect you from spam. You don’t need to set up or maintain the filtering technologies, which are</td>
</tr>
</tbody>
</table>

Keeping up with Office 365

Office 365 Roadmap
The Office 365 Roadmap lists updates that are currently planned for applicable subscribers. Updates are at various stages from being in development to rolling out to customers to being generally available for applicable customers worldwide.

- Analyze Office 365 data with Equivio Zoom
- eDiscovery Case Management, Hold & Permissions
- eDiscovery Infix & Suffix Wildcards
- Office 365 Groups: Support compliance requirements
- Public Folder eDiscovery & In-Place Hold

Trusting Office 365

Office 365 Trust Center
Your people and your data are your most important assets and so, as you consider Office 365 for your productivity needs, we want to do our best to answer your top questions upfront. Trust Center is the place where we share our commitments and information on trust-related topics.

Welcome

Built-in security
- Service-level security through defense-in-depth
- Customer controls within the service
- Security hardening and operational best practices

Privacy by design

Continuous compliance
- Proactive processes to meet your compliance needs
- Customer controls for organizational compliance
- Independently verified to meet evolving standards

Transparent operations

With Office 365, it's your data. You own it. You control it. And it is yours to take with you if you decide to leave the service. The core tenets of our approach to earning and maintaining your trust are:

Learn more about Office 365

• **Free** one-hour in-depth briefing on eDiscovery in Office 365
  – Complete walk through of native eDiscovery features and functions
  – Live demonstration
  – Q & A

• **Full and half-day Office 365 Workshops**
  – Key legal, records, and Information Governance aspects of moving to Office 365
  – Review of built-in eDiscovery and IG capabilities
  – One Drive for Business deep dive
  – Path forward: strategies and tactics for legal and RIM

• **Office 365 eDiscovery Administrator Training**
  – Full-day training
  – Office 365 fundamentals
  – eDiscovery workflows for Exchange, Skype, SharePoint
  – Hands-on labs
  – Workflows, best practices, limitations
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>What is Office 365 (it’s not just email in the cloud!) but rather an entire ecosystem of applications, tools, and content. This webinar breaks it all down.</td>
<td>Can you address some, all, or none of your eDiscovery requirements and needs using the built-in eDiscovery features of Office 365? This webinar will help organizations answer this question.</td>
<td>Office 365 provides several different approaches to the retention and disposition of data—including full records management capabilities via SharePoint. This webinar will provide an overview of the various options and approaches to managing data residing in Office 365.</td>
</tr>
<tr>
<td>• The Office 365 plans available—and why this is important</td>
<td>• Review of type of ESI available for discovery from Office 365</td>
<td>• Options for records management in SharePoint and Exchange</td>
</tr>
<tr>
<td>• The primary system components (Exchange, SharePoint, and Skype for Business)</td>
<td>• eDiscovery Center explained: where much of the eDiscovery activity takes place</td>
<td>• Security and compliance features</td>
</tr>
<tr>
<td>• Types of data and ESI likely to reside in Office 365</td>
<td>• Exchange (email) only eDiscovery</td>
<td></td>
</tr>
<tr>
<td>• Overview of the Information Governance and eDiscovery features built into the platform</td>
<td>• Office 365 Compliance Center</td>
<td>– Data loss prevention (DLP)</td>
</tr>
<tr>
<td></td>
<td>• Pros and cons of built-in eDiscovery features</td>
<td>– Mobile device management (MDM)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>– Information Rights Management (IRM)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>– Encryption</td>
</tr>
<tr>
<td></td>
<td></td>
<td>– Auditing</td>
</tr>
</tbody>
</table>

http://dtiglobal.com/news-events/events
Office 365 Consulting, Training, and Implementation

• Office 365 Readiness and Strategy
  – eDiscovery best practices and workflows
• Office 365 eDiscovery Outsourcing
  – DTI operates eDiscovery features and functions
• Office 365 Email Management and OneDrive for Business Planning
• Legal Hold Process and Planning
• Training
  – Half or full Day workshops and training for law firms and corporations

Consulting

• Records and Information Management (RIM)
  – Assessments
  – Policies and schedules
  – Program implementation
• eDiscovery and Litigation Readiness
  – Assessments
  – eDiscovery response planning and implementation
  – Process design and implementation
• ESI Data Mapping
  – Proactive process to “map-out” an organization’s IT systems and ESI sources
  – Proprietary “systems” and risk based approach

Technology Services

• Defensible disposition and deletion
  – Categorization
  – Repository/application retirement
  – Content audit
  – File share and SharePoint cleanup
• Email and archive migration
  – Archive retirement
  – Migrate email to cloud
  – PST consolidation
  – Legal hold repository
• Sensitive Data Retrieval/Remediation
  – Targeted identification of PHI, HIPAA, PCI, IP, and other sensitive and critical data types
    • Delete
    • Copy/Move
    • Audit