Deloitte.

globalRELAY

Common approaches to email management

Presented at the annual conference of the Archives Association of British Columbia, Victoria, B.C.

Agenda

1 Introduction and Objectives

2 Terms and Definitions

3 Typical Drivers

4 Suggested Considerations

5 Comparison of Approaches

6 Summary

7 Conclusion

Objectives and Definitions

Introductions and Objectives

What we hope you'll take away from this presentation.

1 Enable more informed conversations about email archiving approaches

2 Provoke further discussion about how we manage records of electronic communications

Terms and Definitions

What we mean by “archive”, “archiving”, and related terms in the context of electronic communications management.

Archive (n.)

A secure physical or digital container used for long-term storage, preservation, management, and retrieval of trustworthy and usable information.

Archive (v.)

The process of transferring a digital or physical object to an archive. In digital environments, archiving requires taking a copy of the digital object and its metadata.

Journaling

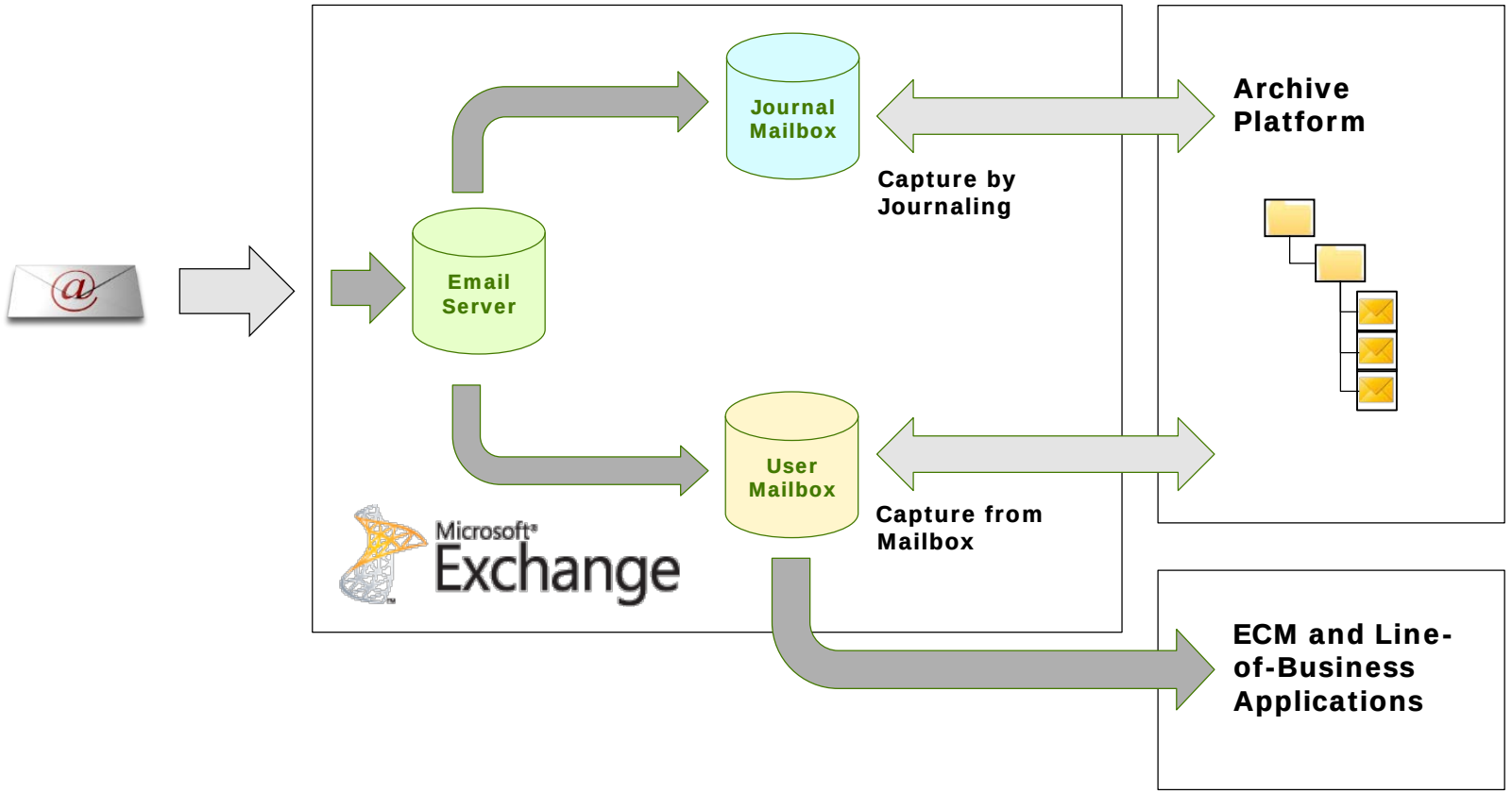
The process of capturing information about an electronic message while it is in transit (recording an incoming or outgoing email message (including metadata, main body and attachments) independently of the sender or recipient’s email server’s capture process.

Discovery

The process of retrieving and providing access to information in response to formal access to information request, litigation, investigation, or audit.

Types of automated message archiving

This graphic shows how journaling and “capture from mailbox” approaches differ architecturally.



Drivers, Considerations and Approaches

Typical Drivers

What may lead organizations to implement email management technology and processes.

Email contains information of value to individuals and organizations. Simply leaving it in an email system is frequently insufficient to meet business needs.

- **User Access:** Users want access to their email long after their mailbox has run out of space. Many firms have banned the creation and use of PST files.
- **Business IP:** As much as 85% of an organization's IP may be in email. This data needs to be preserved and leveraged by other systems or in workflows (for example FOI).
- **Regulation:** Legislation or regulation requires an organization to retain some or all email. Compliance requires centralized control and management of the email, to facilitate discovery and reporting.
- **Policy:** Similar to Regulation except policy is defined by the organization to meet a business need (for example, retain all email from senior management because of high risk of litigation).
- **Costs:** Typically, the type of storage required for active mailboxes is expensive, and splitting mailbox content into multiple storage tiers is difficult owing to mailbox system architecture.

Common Approaches

We will be discussing several types of technology and process approaches we see organizations take to manage email.

1. Journaling
2. Capture from Mailbox
3. Risk-Based
4. Manual Transfer to ECM System
5. “Transparent” Three-Zone Model

Suggested Considerations

What organizations may want to consider when assessing email management approaches.

 **Protection of privacy**	 **UX for standard users**	 **UX for discovery and compliance users**	 **Recordkeeping enablement**	 **Implementation and infrastructure**
The organization's ability to protect the personally identifiable information (PII) of internal and external stakeholders from unlawful disclosure and use.	*The ability of mailbox owners to find, organize, and use email messages and attachments as part of their regular work activities.*	*The ability of legal and regulatory compliance teams to find, organize, and use email messages and attachments as part of discovery, audit, and investigation activities.*	*The organization's ability to retain, protect, and provide authorized access to its personnel members' business email in conformance to operational and legal requirements, and to dispose of the email when it is no longer needed. Includes managing disposition holds.*	*The organization's ability to implement and maintain the email management technology in support of operational and legal needs.*

Approach 1: Journaling

How it works:

- Captures all email subject to journaling rules at the same time it is sent or received
- Routes journaled content into an archive
- No direct impact on the retention of email in the user mailbox
- Does not significantly affect user experience associated with day-to-day use of email, since journaling is done transparently

Applicable situations and environments:

- Financial services environments with “keep everything” mandates
- Scenarios where discovery is likely and risk of non-compliance is high

Considerations:

 **Protection of privacy**	 **UX for standard users**	 **UX for discovery and compliance users**	 **Recordkeeping enablement**	 **Implementation and infrastructure**
Only approved users have access to the archive and their access to data can be restricted as required (e.g. only to data within a specific legal case). The ability to export data from the archive can be similarly restricted.	Users continue to do all email activity in their mail client. Optionally, users can be provided with access to only their own data in the archive and do manual classification in the archive. Users search or browse folders for their data in a manner similar to how they navigate in their mail client.	Depends on the archive. More sophisticated search tools than in email clients. Many tools have early case assessment tools and supervision workflows integrated with the solution.	Records classification can be integrated with the standard user’s mailbox. Retention schedules can be automatically applied at the time of data capture. Retention periods can be altered during the data lifecycle, and manual and automated deletion is supported. Journalled data can be transferred out.	On-premise and SaaS archive are available. Journaling is very reliable and there is little opportunity for anything to “break”. Reconciliation systems can validate 100% delivery of messages. Data is archived in near real-time. Small “ask” for standard users.

Approach 2: Capture from Mailbox

How it works:

- Captures everything from the user mailbox automatically, subject to archiving rules (often age-based)
- Enables optimization of storage and emails system performance, but increases risk due to user control of mailbox (archived content may not be comprehensive)
- Mailbox owners use stubs or plugins to access archived content

Applicable situations and environments:

- Scenarios where optimization of storage and e-mail system performance is the primary driver
- Low risk / low regulation environments

Considerations:

Protection of privacy	UX for standard users	UX for discovery and compliance users	Recordkeeping enablement	Implementation and infrastructure
Only approved users have access to the archive and their access to data can be restricted as required (e.g. only to data within a specific legal case). The ability to export data from the archive can be similarly restricted.	The email client remains the user interface. No need for users to access the archive. Plug-ins or folder structures may be added to facilitate classification of messages and their attachments.	Depends on the archive. More sophisticated search tools than in email clients. Many tools have early case assessment tools and supervision workflows integrated with the solution.	Records classification can be integrated with the standard user's mailbox. Retention schedules can be automatically applied at the time of data capture. Deleting data from the archive can also delete it from standard users' mailboxes. Archived data can be transferred out.	Mailbox integration is typically part of the archive infrastructure. Implementation and maintenance can be complex. The mailbox and archive are typically synchronized once or twice a day. Small "ask" for standard users.

Approach 3: Risk-Based

How it works:

- Combination Journaling and Capture From Mailbox approach with blanket retention rules based on the associated risk
- High-risk roles subject to journaling to prevent loss of information that could be subject to discovery
- General user population has Capture From Mailbox set-up to manage mailbox size and optimize infrastructure

Applicable situations and environments:

- Highly litigious environments
- Situations where adoption is a challenge due to classification overhead

Considerations:

Protection of privacy	UX for standard users	UX for discovery and compliance users	Recordkeeping enablement	Implementation and infrastructure
Only approved users have access to the archive and their access to data can be restricted as required (e.g. only to data within a specific legal case). The ability to export data from the archive can be similarly restricted.	The email client remains the user interface. No need for users to access the archive, or to assign records classifications – blanket retention schedules are assigned.	Depends on the archive. More sophisticated search tools than in email clients. Many tools have early case assessment tools and supervision workflows integrated with the solution.	Record classification can be integrated with the standard user's mailbox. Retention schedules can be automatically applied at the time of data capture. Retention periods can be altered during the data lifecycle, and manual and automated deletion is supported. Journalled data can be transferred out.	On-premise and SaaS archive are available. Could require two different products to be deployed depending on the specific requirements. Small "ask" for standard users.

Approach 4: Manual Transfer to ECM System

How it works:

- Mailbox users move messages and attachments to a corporate ECM system from the mail client
- Mailbox users are responsible for assigning the appropriate records classification (and retention rule)
- Optimally, the ECM system is integrated with the mail client

Applicable situations and environments:

- Lower risk / lower regulation environments
- Organizations with mature RM practices for non-email content
- Case management scenarios

Considerations:

 **Protection of privacy**	 **UX for standard users**	 **UX for discovery and compliance users**	 **Recordkeeping enablement**	 **Implementation and infrastructure**
Users need to have the appropriate permissions to add data to the correct location of an ECM system. If the system is not configured correctly, they could view/access data that they should not. Read/write access (but not copy) is a configuration option.	ECM may provide a plug-in for email client. Otherwise, users will use the ECM interface for filing email correctly: could be drag and drop, pick list, or navigate a folder structure. Less disruptive if records classifications are applied in the background to user-centered folder structures.	Compliance and eDiscovery have to be done either from the email system or from within the ECM (or both). This is a problem if the ECM does not contain all email that must be kept to conform with recordkeeping policies.	The ECM or email system needs to be designated as the system of record for email, for a strong recordkeeping regime to be managed. For example, while legal holds can be applied to content in the ECM system, they may cover all in-scope email.	Records classification infrastructure is implemented as part of the ECM system, with a plug-in into the email client (or a separate web interface). Standard users will require training to learn the manual transfer and classification process.

Approach 5: “Transparent” Three-Zone Model

How it works:

- Combines automated capture from mailbox with additional manual classification to capture email with business value and formal records
- Leverages plugin integration to corporate ECM systems
- Based on “zones”: zone 1 (transitory), zone 2 (business value archive), zone 3 (formal records repository)
- Requires user interaction to identify and classify zone 3 email
- Email that users do not put in zone 3 is copied to zone 2 for a set retention period
- Causes some adoption resistance when zone 1 deletion is introduced

Applicable situations and environments:

- Highly regulated environments where user overhead is warranted
- Organizations with mature RM practices for non-email content
- Scenarios where a work email system is also used for personal communication
- Case management scenarios

Considerations:

Protection of privacy	UX for standard users	UX for discovery and compliance users	Recordkeeping enablement	Implementation and infrastructure
Users need to have the appropriate permissions to add data to the correct location of an ECM system. If the system is not configured correctly, they could view/access data that they should not. Read/write access (but not copy) is a configuration option.	Users need to decide whether email needs to be kept as a formal record (zone 3), or if it’s enough to designate it as having business value (zone 2). Assisted by user-centered folder structures in the zone 3 repository.	Compliance investigations and eDiscovery may need to be conducted in more than one zone get a full view of responsive content.	Record classification can be integrated with the standard user’s mailbox. A blanket retention period will be applied to zone 2 email. Deleting data from the zone 2 archive can also delete it from standard users mailboxes.	Mailbox integration is typically part of the archive infrastructure with the addition of “zones.” Implementation and maintenance can be complex. Small “ask” for standard users if they are already using the ECM system regularly.

Conclusion

Conclusion

Takeaways from our review of approaches.

Email management is a solution to a business problem, not an IT problem

- Business enablement and regulatory/policy compliance need to define tools, not the other way around
- The correct email management solution for your organization should be driven by how you need to use and manage the archived data, not by the cost or ease of archiving the data in the first place.
- Collaboration between business, RM, legal, compliance, IT is critical

User experience is the key differentiator

- User experience is tied to the effort required to apply the right records classification to email (as well as to find and use email again)
- What's more important: designing around classification and retention rules, or what users will actually do?

Thank you.

Stephen Lazenby
Head of Product
Global Relay
Contact: stephen.lazenby@globalrelay.net

Jill Teasley
Lead, Analytics & Information Management
Consulting | Deloitte
Contact: jteasley@deloitte.ca