

Email Management Case Study

Kapil Lohia

ARMA Survey on Information Management Prepared or Not?

- > Majority of RIM professionals feel unprepared
 - **when it comes to email management – 72%**
 - for eDiscovery - 68 %

- > The study also reveals a cause for their lack of preparedness:
 - **62% do not have an email archiving system**
 - 75 % do not have a system that manages their content consistently over the enterprise

- > Inconsistency in the application and enforcement of policy is still lacking.
 - Only 38% reported they manage records according to their retention schedule
 - **Only 41% manage their email according to their retention policy**
 - Only 20% manage their electronic documents according to the schedule

Agenda

- > Why do we manage email?
- > What does email archiving provide?
- > What does email records management provide?
- > What's the solution?

Growth of the Digital Universe

- > Information silos and storage continue to grow
- > Osterman Research- “The Importance of Viewing Email Holistically – 2008”
 - Email use is increasing at roughly 20% per year and email message stores are growing at an average of 35% per year
- > Forrester – “Data Data Everywhere 2007”
 - The volume of the world's data doubles approximately every three years.
 - Growing at 30% a year, we'll reach zettabyte sizes by 2010 — that's a number with 21 zeros!
 - Approximately 80% of the world's data is unstructured

Regulations and Compliance

> Wisconsin Specific:

- Public Records Law - Wis. Stat. § 19.31-19.39
- Open Meetings Law - Wis. Stat. § 19.81-19.98
- Case Law and Attorney General Opinions

> The Freedom of Information Act

> Federal Rules of Civil Procedure

> *Sarbanes-Oxley Act of 2002*

> *US Securities and Exchange Commission (SEC)*

> *National Association of Securities Dealers (NASD)*

> Many more...

When Litigation Strikes

- > It is required that information be reserved, or placed on hold
 - What is relevant?
 - What is expected?
 - How do you find everything?
 - How long will it take?
 - How much will it cost?



Open Records Requests and Discovery

- > Open records requests, litigation, audits, and investigations
- > All relevant information must be produced, regardless of its potential to embarrass or damage
- > Requests/Discovery orders can severely impact IT and incur high costs
- > Few organizations have appropriate “hold” mechanisms that freeze processing of records in anticipation of litigation

Understanding the Email Challenge

An Email Server Is *NOT* A Repository

“With message volumes continuing to skyrocket, and as much as **70% of corporate intellectual property stored within or accessible via email**, enterprise messaging is truly ‘mission-critical.’ Yet firms have not realized that **email servers should not be *corporate intelligence repositories* or be expected to migrate the risks of inappropriate communications or unauthorized distribution of corporate assets.**”

-Enterprise Strategy Group

Backup Systems Are *NOT* Archives

“Traditional backup solutions offer temporary preservation of emails in case of a disaster. They are ***not* designed to store messages** for long periods of time for regulatory purposes or offer users access to their emails. ...they are **very hard to search**...they are a **poor choice** for companies that want to comply with regulations or offer users easy access to their messages.”

-The Radicati Group, Inc.

Traditional Back Up Solutions Fall Short

> Back Up Tapes

- Traditional way to store/restore messages
- Cost-prohibitive and time-consuming process.
 - *Radicati*: Manual tape restoration costs \$2,000 to \$5,000 per tape, resulting in total charges in typical litigation cases exceeding \$200,000 per case.
- Response times for Audit / Discovery requests typically unacceptable
- Recycling policies (ie Overwriting) do not meet records and compliance requirements

> Large Pharma

- eDiscovery Case: Plaintiff sought email messages from only a few of the defendant's employees
- Rather than incur the costs of isolating these emails from back up tapes, estimated to be between \$1.1 million and \$1.7 million, defendant settled with the plaintiff.

Understanding the Email Challenge

Email should NOT be retained forever

“Retaining everything forever is unwise and costly, as is deleting it after 30 days. An all-or-nothing approach will not work and enterprises must have a good understanding of the legal and technical issues involved.”

- Gartner Group

Every email should NOT be retained

“Firms need a way to archive only those emails that are business records, for just as long as necessary, and to be able to produce just the relevant records as part of a legal discovery or internal investigation.”

- Forrester Research

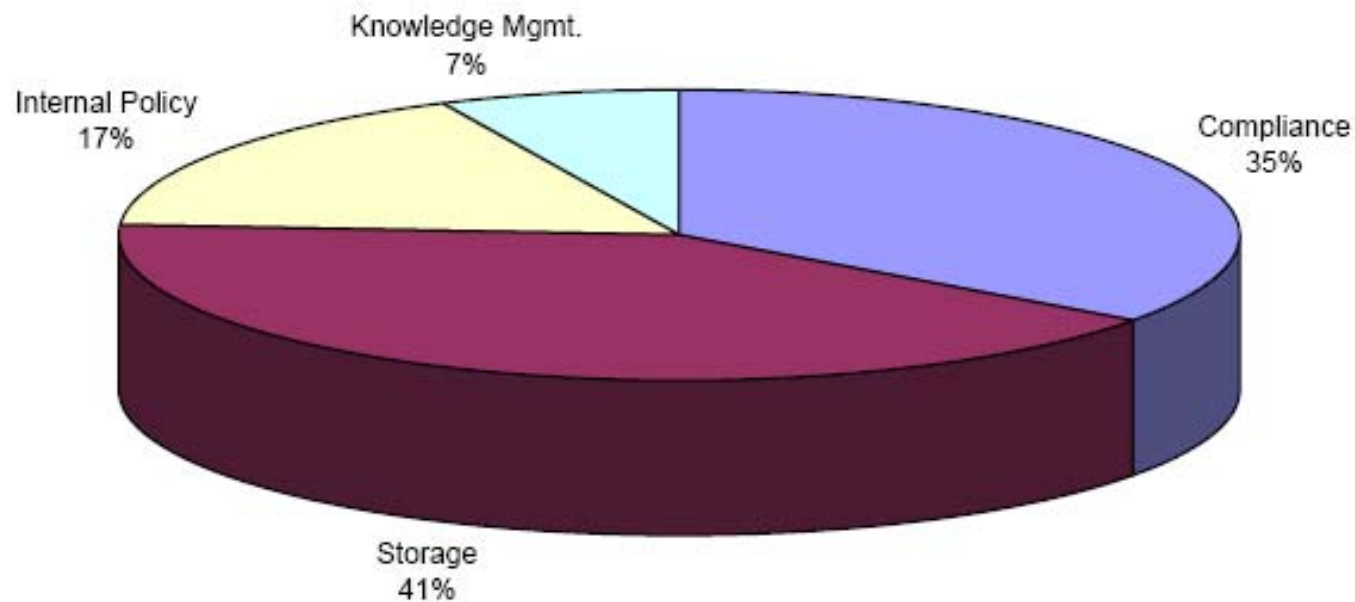
\$1

cost of storing a gigabyte of data

\$30,000

cost of discovery on a gigabyte of data

Market Trends Driving Email Archiving



The Radicati Group, October 2004

Key Email Archiving Capabilities

- > Storage: Decrease the storage requirements of the organization's email system
 - Move emails to archive (stubbing)
 - Centralize the emails to assure there is one version of each email stored.
 - De-duplicate attachments and store only one instance.
- > Capture: All incoming and outgoing traffic
- > Retention: Assign retention to mailboxes
 - Assign retention rules by date or by recipient
 - Based on volume (% full)

Archiving Solution Benefits

- > Secure and read-only archive
- > Offloads email server
- > Compression of email archives
- > Provides off-line storage (e.g. PST file) migration tools
- > Elimination of time users spend trying to keep under an email 'quota' and increased ability to find email when users need to

Additional Benefits of some Archiving Solutions

- > Enable single instance storage
- > Extended search capabilities
- > Email Discovery tools
- > Sampling and supervision as required by SEC
 - Flag email for review and block from send (i.e. inappropriate verbiage)
- > Basic Lifecycle Retention rules
 - Start archiving when the volume is 80% full, and continue until the volume is 50% full
 - Archive all files older than 30 days, except for Hidden and System files

Government's Stance on Email

> U.S. DoD 5015.2

- “[Organizations] shall treat email messages the same as any other record, and these shall be subject to all requirements of this Standard”

> NARA

- Managing electronic mail records
 - Agencies shall manage records created or received on electronic mail systems in accordance with the provisions of this chapter pertaining to adequacy of documentation, recordkeeping requirements, agency records management responsibilities, and records disposition (36 CFR parts 1220, 1222, and 1228)
- Revised Final Rule 36 CFR Part 1234 :
 - Provides flexibility for the management and disposition of short-term temporary email, by allowing agencies to manage these records within the email system (180 days).
 - However - Federal agencies have an ongoing obligation to take reasonable steps to freeze the disposition of any and all records as specified in court orders or other legal process, which email systems do not offer.

Requirements for Managing Email as Records

- > Require Authentic, trustworthy, and complete email records
 - Stored in original format
 - Restorable to original or comparable application

- > Must capture who, what, when, and where of original email messages to have legal or business value as records
 - Message metadata
 - Header information
 - Body Content
 - Attachments

Security Requirements Met by Records Management

> The Unedited Original

- Read-only
- Limited Access
- Detailed Audit Trails

> Ensure document destruction

- Based on Retention Schedule
- Disk Scrub / Shredding

Advanced Security Requirements

> Supplemental Markings

- Code words
- Caveats (e.g. Eyes Only)
- Security Markings
- Roles based Security

> Hierarchical Security

- Government Level Designations
 - Secret, Top Secret, etc.
- Upgrade / Downgrade over time
- Applied to:
 - People, Records, Documents, Containers

Additional Key Requirements

- > Search: You must be able to find the document when required.
- > Retention: Retain for as long as required and no less.
- > Destruction: Destroy the document in accordance with retention requirements.
- > Hold: You must “Lock it down” when required based on:
 - Legal Hold
 - Audit Hold
 - Department/Agency Hold

Email Records Management Compliments Email Archiving

> Archiving:

- Compression of email archives
- Stubbing
- Email capture options (Automated and manual)
- Review and Supervision
- Storage of non-records for short term storage
- De-duplication of email & attachments
- Email Discovery and hold
- Natural Language Processing and Open Lexicon for Supervision

> Records:

- Life-cycle tied to organization's retention schedule
- Email capture options (Automated and manual) tied to classification
- Email available based on security model (not just recipient and administrator)
- Corporate knowledge accessible
- Enterprise discovery and disposition hold
- Extensive Audit Trail (DoD 5015.2)

Integration is the Answer!

- > Store emails (ARCHIVING) to address volume and storage concerns

AND

- > Manage emails (RECORDS) as records to ensure compliance at the same time

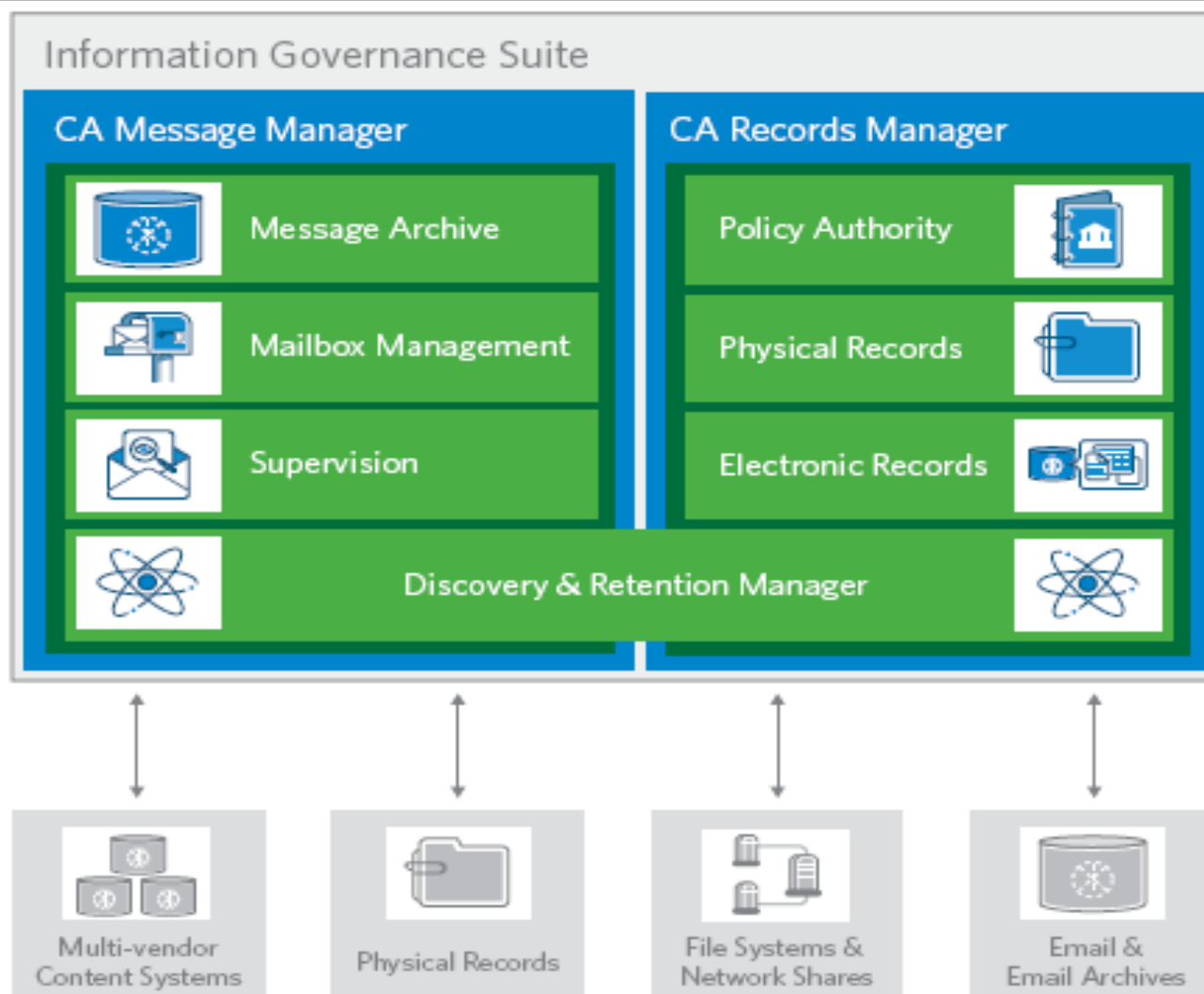
ENABLE

- > Search & retrieve all records *securely* (including email) from wherever they live (all disparate repositories)


TO

- > Ensure *compliance* through *transparency* in normal business processes.

Comprehensive Information Governance



Comprehensive Email Management

- > Email managed against corporate retention schedule
 - > Integration with Leading mail vendors: Microsoft Outlook, IBM Lotus Notes, Novell GroupWise
 - > Work in-Context via mail client or web-based interface
 - > Capture email with ease
 - Rules engine for automatic capture/ declaration against the corporate retention schedule
 - Drag and drop filing
 - Save on send to capture authenticity of email record
 - Batch filing, including .pst handling for legacy email
 - GUI interface for mobile devices to capture emails sent from Blackberry or Treo
 - > De-duplication for storage optimization
-
- Stub email in the email client for continued end user access 

Email Search and Discovery

> Single point of search and retrieval

- Email are included as corporate knowledge asset with other content based on access rights
- Metadata search (To, Cc, Bcc, Subject, sent/received date, etc)
- Full text content search

> GUI interface for mobile devices

> Discovery

- Automatic flagging of email as attorney-client privilege, confidential, responsive, etc.
- Legal holds can be placed on all content, including email, to freeze retention schedule
- Result sets can be sorted, printed in bulk, or converted to PDF, TIF, PST/NSF and exported to CD/DVD

Case Study: Large Midwest City

> Key Business Benefits:

- CA Message Manager's Archive and Discovery components dramatically reduced eDiscovery response times and costs

> Key Solutions Benefits:

- Centralized archive for 8400 City Email users
- Manage "huge" Email volumes

> ROI: Savings in discovery legal costs

- Previous request for 5yrs. of email for 4900 of their users required the entire email and server team of 8 people - 18 Months, to respond to the document request
- \$15 Million in costs associated with this request
- Similar requests now delivered in under 30 minutes

Case Study: Attorney General's Office of Midwest State

> Key Business Benefits:

- Litigation readiness and reduction in risk associated with discovery
- Management of growing volumes of email

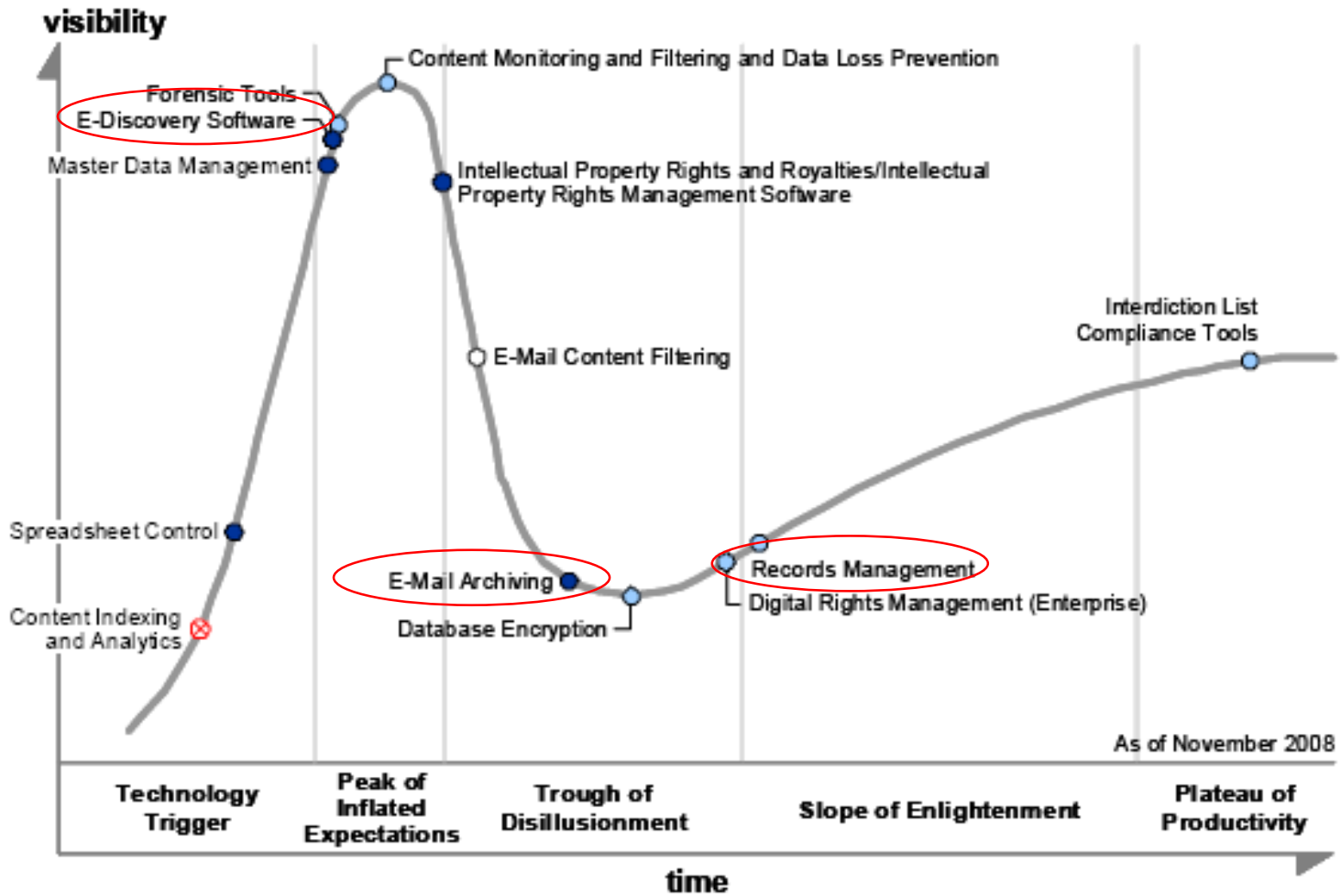
> Key Solutions Benefits:

- Retention and Discovery of Email, IM, SharePoint
- Easily administer Legal Holds
- Policy based retention
- Maintain information in place

> ROI:

- Reduced storage costs
- Savings in discovery legal costs

Figure 1. Hype Cycle for Legal and Regulatory Information Governance, 2008



Years to mainstream adoption:

- less than 2 years
- 2 to 5 years
- 5 to 10 years
- ▲ more than 10 years
- ⊗ obsolete before plateau

Source: Gartner (November 2008)

Questions & Discussion

Kapil.Lohia@ca.com

www.ca.com/IG