Email Management

By John Annunziello,
CRM, CDIA+, ermm

IIMC Records Management Technical Bulletin Series • 2012

Records Management Technical Bulletins

This publication, one of sixteen bulletins in the *2012 Local Government Records Management Technical Publication Series*, is a joint effort of the Municipal Clerks Education Foundation (MCEF), the International Institute of Municipal Clerks (IIMC), and the National Association of Government Archives and Records Administrators (NAGARA). Funding for this project was made available, in part, by a grant from the National Historical Publications and Records Commission.

The Municipal Clerks Education Foundation (MCEF), established in 1984, is a tax-exempt, nonprofit foundation under Section 501 (C)(3) created to raise funds for its partner, the International Institute of Municipal Clerks. IIMC uses these funds to promote, train and educate Municipal Clerks, making them proficient in the services they provide for the citizens of their community. MCEF is a diverse team of volunteers who are passionately committed to helping IIMC pursue its educational objectives.

The International Institute of Municipal Clerks (IIMC) is devoted to advancing the professionalization of the Office of Municipal Clerk and improving the efficiency of municipal government. The IIMC provides its members with educational, conference, reference, research, and informational services designed to keep them informed of changes in the professional community.

The National Association of Government Archives and Records Administrators (NAGARA) is a professional association dedicated to the improvement of federal, state, and local government records and information management programs and the professional development of government records administrators and archivists.

The National Historical Publications and Records Commission (NHPRC), a statutory body affiliated with the National Archives and Records Administration (NARA), supports a wide range of activities to preserve, publish, and encourage the use of documentary sources, created in every medium ranging from quill pen to computer, relating to the history of the United States.

Preface

Like every organization, local governments create and maintain large quantities of records. Many of these records not only are of great value to the local government, but also are of concern and essential to the citizens of the community. Federal and state-mandated program requirements, changes in growth and development patterns, expanded service needs, the use of computers and other technologies for creating and using information, and the proliferation of copies in various formats, have all contributed to this enormous accumulation of records. Each publication is intended to make available to local governments the basic principles, policies, and guidelines that should be followed in establishing a sound records management program and in carrying out sound records management practices.

The series is intended for local officials, with limited resources, who lack formal records management or archival training but who have custodial responsibility for records. These local governments include townships, villages, cities, counties, school districts, and other local political subdivisions and special-purpose districts. Each of the following publications in the series includes a bibliography that refers to other reading for more detailed information and guidance.

Overview:

Starting a Records Management Program, The Daily Management of Records and Information, Making Your Records Management Program Successful, Managing Records on Limited Resources, Funding Your Records Management Project

Creation, Collection and Storage:

Identifying and Locating Your Records, Establishing Records Retention, The Selection and Development of Local Government Records Storage Facilities, Developing a Records Storage System

Preservation, Promotion, Use and Access:

Archives for Local Governments, Protecting Records, Using and Storing Microfilm

Care, Management, and Preservation of Electronic Records:

E-Mail Management, Selecting and Using Document Imaging Systems, Managing Electronic Records, Preparing for E-Discovery

Copies of these bulletins are available on the IIMC and NAGARA websites.
IIMC at www.iimc.com • www.nagara.org

Acknowledgements

Meet the Author: John Annunziello, CRM, CDIA+, ermm

John has been in the records management (RM) area for the past 24 years. With training in Photography and Marketing, like many people, John was thrust into the world of RM and his journey began. With additional courses at the University of Toronto and attending many ARMA events and conferences, John learned how to build his RM program at the Toronto and Region Conservation Authority (TRCA). Similar to a municipal entity, the Authority encouraged John's development in the area of records management.

Like many organizations, TRCA struggled with the management of email. Accordingly, committee's were formed, courses attended and an email program was developed. This bulletin highlights the findings, the challenges and the successes of this program. The email program has filled a huge gap in the information management area at TRCA. Previously email management was hit and miss. Now all emails, whether transitory or official records, are managed effectively with classification and retention applied.

In the past 10 years, John achieved his Certified Records Manager (CRM) and Certified Document Imaging Architect (CDIA+) certifications along with a certificate in electronic records management (ermm). He has spoken at local and international conferences and continues to share his expertise with email and records management around the world. Today, John has taken an early retirement from TRCA, but continues to act in a consulting capacity.

Acknowledgements continued

Editor: Dr. Julian L. Mims III, CRM, CA

Julian Mims is a career archivist, records manager and educator. He directed the local records program at the South Carolina Archives from its inception. He was in charge of the Long Island office of the New York State Archives and Records Administration (NYSARA). As a Vice President and Award of Merit winner of ARMA International, he helped to found a record ten ARMA chapters. Dr. Mims is the author of the International City/County Managers Association (ICMA) best-seller, *Records Management: A Practical Guide for Counties and Cities*, and was editor of ICMA's *Electronic Records Management*. Earning a doctorate from the University of South Carolina in 2001, he has taught at six colleges and universities.

Special thanks to the support team:

Dale Barstow Project Co-Director and MCEF President, Municipal Code Corp., *Tallahassee, FL*

Paul R. Bergeron, MMC, CA Project Co-Director and NAGARA Liaison,
Office of the City Clerk, *Nashua, NH*

Marian Karr, MMC MCEF Treasurer, Office of the City Clerk, *Iowa City, IA*

Chris Shalby IIMC Executive Director and IIMC Liaison, *Rancho Cucamonga, CA*

Table of Contents

1. Introduction

Email has changed how organizations do business. It has often surpassed telephone use as the main tool for dialogue between two individuals or a group of users. Electronically stored information (ESI) doubles every three years[1]; many municipal offices have a dramatic need to manage their email systems. Email may have become the number one problem in managing ESI material.

Email mismanagement grows geometrically for Records and Information Management (RIM) professionals. No standards specifically address local government email. The Association of Records Managers and Administrators (ARMA) has simple guidelines. Yet many RIM professionals throw up their hands over the complexity of management issues surrounding emails. There is no single solution; costs appear prohibitive.

ISO 15489 and ISO 23081 are both international records management standards. ISO 15489 defines records as "information created, received, and maintained as evidence and information by an organization or person, in pursuance of legal obligations or in the transaction of business." Certainly this includes emails. Many local government offices have adopted this standard because it highlights the fundamental principles of a sound records management program. However, neither standard specifically addresses the exact requirements of an email management program. Accordingly, the organization may have to interpret the standard. Email management is not easy. This technical bulletin attempts to lay a framework of experience and correct decision-making upon the management of emails.

2. History

Electronic mail, also known as email, has been used for over 40 years. In 1971, Ray Tomlinson, introduced a system where two users were able to converse electronically within the same network.

The first message, with the letters QWERTYUIOP, was sent between two computers sitting side by side.

Ray Tomlinson worked as a computer engineer for Bolt, Beranek and Newman (BBN), the company hired by the United States Defense Department to build the first internet in 1968. The @ sign, so commonly used today, was originally designed to distinguish between computers and users.

Later, email grew to include conversation across different networks; log-on controlled transmittal/receipt. Today, the billion dollar email industry is a common means of business communication.

3. Email Etiquette

3a) When You Shouldn't Use Email

Email has become one of the most popular means of understanding within the business world. It is inexpensive, global communication.

Via email, information can be easily tracked or comments reviewed. Unlike conversation, however, it has no tone. Raised eyebrows cannot be seen in an email.

In many cases, a phone call would be a better means of communication: both individuals can quickly ask questions, or seek further clarification. Arguably, phone calls are more personable. For example, users can be bolder on the phone, as against email, which does not allow eye-to-eye contact between individuals.

The usefulness of face-to-face meeting should not be ignored; sometimes in-your-face can be good. Imagine being informed of job change by email. Is this not a cowardly way of performing business? Performance appraisals, even matters of heated interest, may best be handled in person. How much are these things worth to you: body language, to be

read, intonation, to be heard and facial expressions, to be seen. The hear no evil/see no evil/speak no evil crowd did not have your local government skills, right?

Conversely, you can review email and "tone down" hostility to the individual. With conversation, you may say something that you regret. If discussion becomes heated, you may store the email as a draft, review it the next day, and send it when you have "cooled down." Sometimes individuals have sent emails in a heated moment and later regretted sending them. Remember: conversation can be interpreted or forgotton. However, email can be ominously permanent. Email may constitute stop-action that can haunt you in court! When a certain company hired a records manager, they recruited a lawyer - - for management learned the hard way that you can be nailed with your own records. See the bulletin on E-discovery.

3b) Email Netiquette

- Writing may be misconstrued or misunderstood. Poor communication due to poor writing skills may come across the wrong way.
- Write as if you were writing to a business executive or the governing body of your local government. Would your mother be happy with the way you are writing and what you are saying?
- Your email could easily be forwarded to others. What would the consequences be, if that happened?
- Keep it short. Emails should never extend beyond one screen on a computer. Use attachments for reports.
- Bold letters or all caps come across as shouting in an email. Do not overuse the exclamation point. Similarly, letters that are totally lower case may appear unprofessional or uncaring.
- If you receive an email and the recipient expects a quick response, advise them that you received it and the response will be shortcoming. The recipient, after all, may be in a meeting or out of the office. If you must have a quick response, call. Don't assume that they are avoiding you.
- Your salutation (name, title, organization name, email address, phone) should be at the bottom, perhaps as a "footer," in your email. It is very disturbing to receive an email and remain unsure who sent it.

4. Email Management Problems

An AIIM report titled "Email Management, The Good, the Bad and the Ugly"[2], reports the results of a survey that went to over 1100 individuals.

The survey found:

- Respondents spent more than an hour and a half per day processing email, one in five spent three or more hours a day
- Over half of e-mailers had hand-held phone access: Blackberries or Smart Phones, for example. Two thirds processed work-related emails out of office hours with 28% confessing to doing so "after work, on weekends and during vacations".
- "Sheer overload" was reported as the biggest problem with email as a business tool, followed closely by "Finding and recovering past emails" and "Keeping track of action".
- Over half of the respondents were "not confident" or only "slightly confident" that emails related to documenting commitments /obligations made by staff were recorded, complete and retrievable.

Sheer volume increase of emails in organizations has created problems. Typical are bandwidth issues, increased costs in data back-up / storage costs and slower retrieval times. Statistics from the Radicati Group[3] showed an increased need to manage emails in a typical environment:

- Growth in the number of email messages
  Average 160/day
- Growth in volume of messages per user
  Over 21MB/day
- Growth in the size of email messages
  Attachments are becoming larger
- Growth in cost of email messages
  $5,000 per user per year
- Regulatory compliance to retain emails

Presumably, these numbers and costs will esca-

late. As each year passes, complexity of the issues surrounding management of emails continues. The time to start managing emails is now before it gets totally out of control.

5. Business Drivers

With today's litigious society, organizations are at risk. Legal compliance is a major driver for taking better control of emails. However, other drivers need to be taken into account:

- Efficiency improvements – speed in retrieval
- Financial return, against reduced storage space
- New legal discovery costs
- Increased staff time to manage key tasks

Stephen Maddex, lawyer and associate for Lang Michener LLP, Ottawa, Canada, suggests that before email, businesses "maintained" massive databases of paper files. Against litigation, desired documents were nonetheless easier to find since at least it was organized[4]. Today's email, however, constitutes a "massive, disorganized haystack".

Organizations have records in disarray. Understandably, problems have resulted.

6. Starting from Scratch

6a) Where Do You Start?

All projects need sponsorship; "Executive Champion" is key. Dr. Mark Langemo's book, "*Winning Strategies for Successful Management Programs*"[5], suggests that this support plus a sound business case equals success. Do you wish to initiate a project without management support and a plan?

In my organization, I championed the Director of Finance and Business Services who also managed risk, as well as records and information technology (IT) within our organization. If you don't have such a champion, nurture a relationship with someone in senior management who sees the need for email management. A brief presentation at the executive level may yield a senior leader who understands and appreciates what needs to be changed.

In the municipal realm, the Mayor, the Chief Administrative Officer (CAO) or the Chief Information Officer (CIO) would all make excellent choices as champions for the email project. These individuals have "pull" within the organization, others tend to listen and follow what they say. As project coordinator, pull together the needed information to get one of these individuals "on board" to help drive this project.

6b) Email Strategic Planning Group

Once the executive champion has been determined, an email strategic planning group should be established. For greater support from staff, the executive sponsor should request participation from users for this committee. Include the records manager, Information Services Director, legal counsel, Human Resources management, auditor and senior level management from all major departments within the organization. The executive champion, together with the project coordinator or email administrator, should include within the agenda the necessary steps to develop an effective email system. (See email deployment checklist at the back of this report)

The project coordinator should perceive what would work within their organization. Do some homework, determine a broad course of action and present those thoughts to the email strategic planning group. Determine whether the course of action is valid, provide comment and refine the project scope. A brief presentation on the different solutions and why the project coordinator chose the one solution will be a good starting point for the group. The group should refine the course of action presented, talk to other users on the proposed action, identify problems within the current system, and work with users to bring forward a total solution. Involving users will ensure buy-in when the project is piloted and then launched.

6c) Change Management

Managing change is perhaps the most important component of bringing any new system into an organization. Users become very accustomed to doing things the "same old way". Inevitably some kick back from users will result throughout the organization. Therefore, a change strategy will need to manage effectively differences that the organization will encounter.

Information Management Journal article, "Harnessing the Winds of Change"[6] by Ganesh Vednere states that Records and Information professionals should develop controls to manage updates to policies and procedures. He identifies the following traits for system changes, such as implementing new email systems.

1. Understand the changes that need to be made.
2. Conduct a detailed evaluation of the impact of those changes on the day-to-day management of records.
3. Assess the changes that may be required to the record inventories, retention periods, records management system, line-of-business processes, procedures, and business applications.
4. Revise training and communications to address policy changes. Employees can either take the updated training immediately or in the next round of training certifications.
5. For major policy changes, take a slow-and-steady approach to implementing this. Rolling out all the changes at once is not optimal, as user acceptance is important.
6. Provide business units with ample time to understand and incorporate the updates.
7. Establish a time-line by when each business unit will comply.
8. Develop training, supporting documentation, "cheat sheets or simple instructions," communication plans, "lunch time brown bag sessions," and "what this means to me" materials for employees.

A good change management regimen cannot over-communicate its message. Identify and emphasize the benefits of each change.

Mr. Vednere suggests that system changes go on all the time. Highly plausibly, a Records and Information Management professional or email system coordinator can keep up to date with all changes to any system. Vednere recommends scheduling these changes on a semi-annual or annual basis.

The change management component should not be taken lightly. Some larger municipalities may have change management professionals on staff. If so, bring them into the process very early. Make them part of email strategic planning.

Managing change is key to the program acceptance of this program, you may want to give serious thought to hire a consultant with experience in email and change management. Look for someone in your organization with strong project management skills or Project Management (PMP) status to keep the program on track. Someone so accredited will be valuable to the email strategic planning group.

7. Classifying Emails

7a) Email as Records

Many organizations make the mistake of treating all emails the same. That would be akin to saying that apples and oranges are the same, since they are both fruit. Distinguishing different types of emails is a key starting point in developing any email system. Applying set rules to each document is a good records management practice. **Emails should be categorized according to the content within the email**. The fact that it is an email, received from a certain individual, does not determine whether an email is a record or not.

Within the Records and Information Management (RIM) profession, there is no consensus on some of the subtle differences between a record and a non-record. Some individuals call a non-record a document. Others believe that documents can remain as documents, or later become records. As a RIM professional for over 20 years, I also struggled with this concept. This report will follow the terminology that important information is either transitory or official record.

Emails are categorized as:

- Spam
- Transitory records
- Official records

7b) Spam

Our email boxes are filled with this material daily. Spam, or junk mail, is material often unrequested or unnecessary, forwarded to advise us, for example, of new products, white papers or invitations to accept online meetings. It is often health related….."bigger or smaller body parts" or ideas such as, "'how to loose weight" or where to buy "cheap" pharmaceutical products. It may be "what are you doing for lunch?" memos. Often it has little or no value.

Spammers collect e-mail addresses from chat rooms, websites, customer lists, newsgroups, and viruses which harvest users' address books, to sell. Via "e-mail appending" or "e-pending" spammers use known information about their target (such as a postal address) to search for the target's e-mail address. Much spam is sent to invalid e-mail addresses. Spam averages 78% of all e-mail sent[7].

Fraudsters enter personal information on fake websites with e-mail forged to appear to originate from a bank or other organizations such as PayPal. This is known as phishing. Spear-phishing is targeted phishing, using known information about the recipient, it may look like it came from your employer. A rule of thumb is, if you don't know the sender, or if there is no description title, don't open the email.

Use the email blocker in your email system. Setup rules to determine what should or shouldn't be received so the trash basket/firewall can work. This will decrease future spam messages.

Spam emails may have an "unsubscribe" link located at the bottom of the email. Initially, this appears to be a good idea, but spammers sometimes use this as a means to validate a current email address. Most of these links are valid. Your Information Service/Information Technology group will guide.

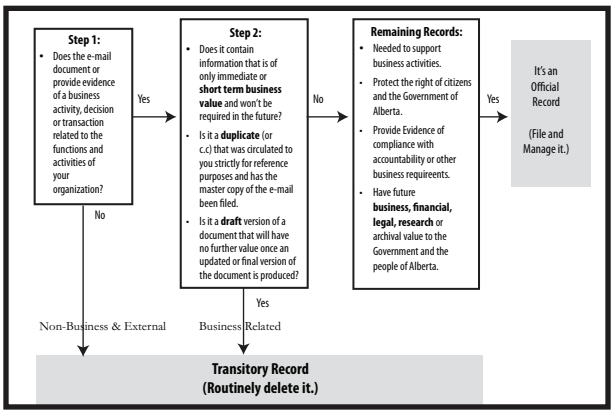
7c) Transitory Records

Transitory emails are those emails which are received and have short term value to the organization. They are not considered spam, yet as time goes on, their value quickly diminishes. The retention period tends to be fairly short and, without retention rules in an organization they are often destroyed after a set period of time, without consent from the owner.

Here are some examples of transitory records:

- Preliminary drafts of letters, reports or memos which are not significant stages in the preparation of a final document, and do not record official decisions
- Multiple copies of project or committee materials, such as minutes or agendas, sent to various committee members
- Publications such as administrative manuals, newsletters or periodicals
- Unsolicited advertising, such as flyers and brochures
- Personal messages, notification of upcoming events, or memos of minor administrative details

The province of Alberta, Canada,[8] has kindly provided this chart for their users to determine the steps in determining the difference between transitory and official records. It is a tool you may want to consider as it correctly distinguishes the difference between official records and transitory records



Note that this chart is provided as an example, and is not authority for retention/disposition.

7d) Official Records

Official records have great value to the organization and accordingly, warrant greater care. These records should be stored according to the organization's classification systems which contain records series or hierarchy of the file structure. As well, retention values should be assigned to them, per the records retention schedule. They should follow the information life cycle structure. Typically, before disposition, they are signed off for destruction by the business owner.

Some official records are considered vital records. They should be managed for easy retrieval or reconstruction, to allow business to continue despite disaster. Certain emails are vital. Typical vital records are accounts receivable/payable, insurance material, payroll, patents, deeds, and certain agreements.

8. Possible Email Solutions

Email problems have a host of solutions.

Email should feature these positive factors:

- Ease of use
- Lower cost
- Reduced volume on e-mail server
- Greater accessibility for discovery purposes or Freedom of Information (FOI) requests

Email management should fit your organization.

8a) Paper Email Records

The easiest way to manage emails may be to print them out and store them within a paper records folder. This creates a single media format, located altogether. Color-coded, alpha-numeric labels on folders in such a system allows an organization to easily locate files and distinguish misfiles.

Advantages

- A long shelf life, if stored properly
- The email record is physically seen and easily read
- Often preferred by the baby boomer generation who find reading a computer screen laborious

Disadvantages

- Easily lost or removed from folder and placed elsewhere
- Difficult to locate content, if part of a large folder
- Old technology
- Metadata (data about data) will be lost as computer systems record information which is not printed out on the paper copy. This could be vital to the context of the email.

The world encourages green technology, paper use means cutting down trees. Electronic documents are more easily stored and managed.

8b) Store Emails in Existing Email System

Organizations have allowed users to store emails within their email system via Lotus Notes or Outlook. While this leverages existing systems it is often left up to the user to manage this space. Users are often given a set amount of storage space, also known as a "quota," to store their emails. When the quota limit is achieved "excessive file storage" warnings are received from the systems administrator. The only option at that point is to delete emails.

Quotas are based upon the material found in the "in" or "sent" basket, as well as any emails which have been placed in "folders". Further, material found in the "trash bin" may

counts towards the quota limit. System administrators can allow for "auto deletion" for material placed in the "trash", however, it is often left up to the user to perform this function. Accidental deletion of email and subsequent retrieval may be accomplished by the user without assistance from the Information System/Information Technology department.

Advantages

- Easy for users to understand
- Users can structure their own folders
- Set quotas allow for better system performance

Disadvantages

- Email records may be deleted without following corporate retention guidelines
- Quotas can be easily increased, leading to system overload and additional bandwidth usage
- Poor records management practice

In *The ePolicy Handbook*, *Designing and Implementing Effective E-mail, Internet and Software Policies*, Nancy Flynn writes that "An empty mailbox is a safe mailbox."[9] Clean out overstuffed employee mailboxes with a combination of education and automation. Flynn cites five points to force employees to empty their mailboxes:

- Reach out to your employees. Explain the organization's e-risks and issue email deletion guidelines. Tell employees not to hold onto old email messages. Discourage employees from storing email on their hard drives as an alternative to their mailboxes.
- Explain to employees how the manual delete folder works. Many users do not realize that messages can, ominously, sit in the delete or trash folder forever, unless they take the necessary steps to empty it.
- Take advantage of new sophisticated management software. Assign limited email space on your email file server. Reduce the size of mailboxes, as users will eventually run out of storage room.
- Install software that allows your email systems administrator to empty users' trash folder every 30 days.
- Be alert to the fact that users may find a "work around" to store their excessive emails. Stress the fact that in litigation, all areas such as employee hard drives are subject to e-discovery.

Disenchanted employees can be a risk: email may reflect this tone. There may be adverse effects in the litigation process.

Records retention schedules should apply to all emails, ensuring that emails which are records are not inadvertently destroyed. See Chapter 9 for further information.

8c) Store Emails to an Archival Mail Tool/Server

Within the past ten years, archiving tools and software proliferated. The ARMA and the AIIM website noted over 50 companies that provided archiving solutions or email consulting services. Many companies provided software to manage archives alone; many content management systems (CMS) included this as part of their records management suite. As an add-on component to a CMS, this may be an excellent, cost effective solution to assist in email management.

In an internet search, an email management software company proclaimed: "With thousands of customers, "X" is used by administrators to maintain an archive of all corporate email correspondence, significantly reduce the demands on the Exchange server, manage and reduce the company's dependency on PST files and also meet a growing number of regulations on compliance, e-Discovery and other legislation." This is typical of many archiving systems.

While all systems are different, the following features are available on many systems:

Advantages

- Maximize storage space using ZIP compression
- Email can be encrypted to ensure security measures are met
- Find email using complex search criteria
- Connect to the organization's records retention schedule

Disadvantages

- Email records are not stored according to content values
- Some systems cannot be integrated with existing technology

Thanks to the 2008 amendments to the U.S. Federal Rules of Civil Procedure (FRCP), businesses in non-regulatory situations however realize the risk of mis-managing their email archives since legal discovery experts typically search here first.

8d) Content Management System (CMS)

This scenario is advantageous only if the organization previously invested in a content management system. If the organization anticipates managing electronic records as a whole, a purchase may be warranted. Many content management systems now manage, or add, emails as part of their suite.

Purchasing software to manage emails, then purchasing a CMS would not be frugal and may cause problems. Ensure that systems can "talk" or integrate with each other. Typically, users are requiring an "all in one" system where information is accessed through one portal.

Advantages:

- Good RIM practices
- E-mails take on retention of assigned folder
- Fully text searchable
- Excellent for discovery process, since searching is quickly and easily performed
- Investment in CMS leveraged since systems have email components

Disadvantages

- Users have to back-track their emails and store in a Content Management System
- Labor intensive
- Users won't deal with old emails
- Additional costs for storage in Content Management System

Content Management System in place, email systems administrators often set small quotas for the email system to encourage users to store content within the CMS. Backlog may result, the user now has a smaller mail box and yet has a considerable amount of transitory and outdated material stored. The user may perform considerable cleanup to meet quota guidelines. When this happened within my organization, there was a great backlash from the users. Ensure that you provide considerable time to perform this duty.

Most software on today's market allows for "drag and drop" into a Content Management System (CMS), ensuring ease of use for the user. Of course, this means using two windows: the email system and CMS open at the same time. Some Content Management Systems, working in harmony with the email system, do not allow email and attachment to be stored as one document. Prior to purchasing a CMS, ask the vendor if this is the case. You may want to be able to store them separately.

Recently launched into email systems such as Outlook or Notes, is the availability to connect these email systems to the Content Management System. In a demo, the Content Management software opened within the email window and actually appeared to be a part of the email system. To store an email, simply "drag and drop" it. Of course when dropped into a folder, the retention elements become assigned to the email. Because of easy use, transparent records management is becoming more popular.

8e) Big Bucket Approach

This is a fairly new approach to managing records. Municipalities merge and the records from both entities combine. Organizations have hundreds or thousands of categories to manage. Your organization may need the "Big Bucket" approach.

Rather than an unmanageable amount of record series, a predetermined amount of "buckets" are assembled wherein like retentions are grouped, and the users may have a dozen different "buckets" to store their emails. This makes it easier for the user, and is becoming more popular as organizations struggle for email solutions. Of course, the big bucket approach not only can apply to email but to all records.

Advantages

- Easy for users to understand
- Users determine in which bucket to put records
- Records have retention assigned
- Timesaver

Disadvantages

- Poor records classification
- Often results in longer retention periods
- Event driven retention (i.e. disposition occurs 7 years after employee leaves) is not possible since preset terms are assigned to buckets

The smaller the number of "buckets", the greater the chance of keeping the records beyond their legal and organizational requirements. For example, you may have a bucket with a retention period of seven to ten years. If the retention period is actually seven years, as many financial records are, those records will be retained three years longer than required.

8f) Quota Settings

An absence of quota standards can be a problem. More emails slow the system and make them more difficult to locate. Quotas predetermine storage space allotted to each user. In some organizations, a call to the Information Services/Information Technology group will result in increased space, or increased quotas for storage of emails. This practice, however, is not recommended since email can easily grow out of control.

Many organizations allow increased quotas for senior staff only. This is not recommended because of the message it sends to all staff…that senior management is more important than all other staff.

Advantages

- Reduced email storage space
- Better management of email accounts
- Forces users to manage accounts

Disadvantages

- More user intervention
- Chances of deleting e-records increased
- Investment in Content Management System not leveraged since folder structure determines retention and is not normally part of the quota
- No records classification
- Email records not linked to organizational records

8g) Rule Based Tools

This software allows the administrator the "look and feel" of an email management system. Its tools such as "crawlers" search for duplicates or stores similar emails in one folder. Rules established by the administrator determine the scope of the system.

Advantages

- Less user intervention
- Identifies duplicate emails
- Manages all emails, past and present
- Leverages investment in Content Management System
- Records are complete and classified
- Leverages existing (IBM, Microsoft) investment
- Technology can also manage shared drives

Disadvantages

- System effectiveness depends on how rules are created and applied
- More work for records staff
- Most expensive solution

8h) Store Emails in the Cloud

The latest trend in managing emails is to store them as a service in the internet also known as the "cloud," (sometimes called cloud computing). There are different ways to store data in the cloud:

1. Private organization (a single organization)
2. Public cloud (full multi-tenant)
3. Hybrid cloud (any combo of others)
4. Community cloud (a single organization, plus other closely aligned organizations)

Each of these has its own distinct advantages;

and each is listed from the most to the least expensive. Deciding whether to move your email records to the cloud depends on the risk factor, especially the risk tolerance within your organization.

Advantages

- Low, predictable costs
- Managed as a service, with unlimited space
- Web based, accessible by all
- Robust feature sets are available
- Rapid deployment
- No in-house Information Technology (IT) support

Disadvantages

- Security – outside the company's firewall
- Loss of management control
- Ownership
- Customer service relations with the internet provider need to be established

The service level agreement (SLA), a requirement for cloud based services, should be reviewed with comments from legal, finance, records, IT, and major users.

To manage risk, examine the cloud provider's

level of data security. Minimally, ascertain:

- Is the cloud provider contractually obligated to protect the customer's data at the same level as the customer's own internal policies?
- Who has access to customer data, and what are their backgrounds?
- Where is the provider's data center physically located, and what safeguards exist to prevent data centers from unauthorized access (for example, 24/7 security personnel)?
- Does the provider promise to maintain user data in a specific jurisdiction and/or to avoid certain jurisdictions?
- What are the provider's migration policies regarding moving data internally or to alternate providers? (ensure that no data is lost or falls into the wrong hands.)
- Does the provider conduct regular backup and recovery tests?
- Does the provider's security policies comply with all applicable regulatory rules?
- Is the provider willing to undergo on-demand or periodic audits and security certifications?
- Is the provider required to investigate illegal or inappropriate activity?
- Is the provider required to disclose any new vulnerabilities that may affect the confidentiality of customer data, or the integrity and availability of their services?
- In the event of lost or compromised data, is the data backed up, and can it be easily reconstituted from the backups?
- What are the provider's policies on data handling/management and access control? Do adequate controls exist to prevent impermissible copying or removal of customer data by the provider, or by unauthorized employees of the company?
- What happens to data when it is deleted?
- What happens to cloud hardware (for example, trailers of servers) when the hardware is replaced?

Any of the above should be reviewed. Should each stipulation be in writing: reviewed, approved and filed with your organization?

According to Gartner Inc., cloud computing is worth billions of dollars.[10] "Worldwide cloud services revenue was forecast to reach $68.3 billion in 2010. By 2014, the industry is poised for strong growth with revenues expected to climb to $148.8 billion. "

Although this may be the future, email adminis-

trators need to look beyond attractive cost savings. Administrators should also be concerned with:

- Performance
- Availability of information
- Data security
- Interoperability with other systems
- Legal responsibilities

9. Email Retention

Many organizations give users the option of deleting their emails with little or no consequences as to whether they are record-related or not. Transitory records are often deleted by the user, while emails which are record-related are retained and disposed of according to the records retention schedule.

While working on an ARMA presentation on email management, I contacted local municipal offices to determine how they manage their emails. One of the largest municipalities had a policy to keep all emails that were received. After time, emails were forwarded to an archival server which stored them indefinitely. They had a retention schedule to manage paper records and dispose of them when the retention period expired, yet this did not apply to email records. Saving all emails received or sent should only apply to certain regulated industries, such as banking or investment firms where this practice is mandated[11]. Email and other records should all be treated with the same rules.

Retention of emails equals the risk which the organization is willing to take. Keeping emails for too long can be just as damaging as not keeping them long enough. Many states, provinces or countries have records retention periods for managing all records. Software can help administrators ascertain, and apply, legal requirements for records retention.

Putting policies in place, documenting them and following them is the correct way to manage email retention. If email policies are questioned in court, be sure you can prove that your organization follows a systematic approach to managing email. You should be protected, by the consistent, all-inclusive nature of such standard procedures.

Companies such as Microsoft and Enron have found that incorrect management of old email has hurt tremendously in court-awarded costs. Enron no longer exists, due to penalties. To guard your organization, retain emails for as short a period as possible. The longer you keep emails, the greater the cost and risk to your organization.

To mitigate the risk of keeping emails for too long, organizations need to be reminded that although the email has been destroyed on the email server, it still exists in a backup tape. Backup tapes, if not overwritten or replaced on a consistent basis, mean you are keeping all email forever. In e-Discovery, all existing information on active systems, as well as data found on backup tapes, can be requested. Develop a policy for tape retention and follow it.

10. Email Policy

Part of reducing risk to an organization is to establish an email policy which outlines the expectations of the organization. A policy must be established then followed. The policy itself should be fairly simplistic.

A policy that cannot be readily followed, especially due to complexity, is poor management.

Here are some guidelines which should be followed:

- The email strategic planning group should help to set the guidelines.
- Include users from all departments to assist in the acceptance of the guidelines and represent overall company beliefs.
- Policy should be approved by senior management, legal council and the governing body.
- Communicate the policy to new staff. Refresh via yearly reminders. Be sensitive to trouble areas.
- Establish clear guidelines regarding the opening of documents. As a document is opened, it is vulnerable to virus. Ensure that virus software is current and operational.
- Enforce security precautions: passwords that are not shared, computer access restricted to users only, unusual behavior investigated.
- Require users sign-off: reading, understanding

and acceptance of the policy.

- Advise staff on the inherent legal and organizational risks of poor email management.
- Develop and maintain mandatory training for all users.
- Establish penalties for poor email compliance. Connect job description and performance appraisal with an understanding of email management.
- Review the policy, on a yearly basis, to address issues or changes to the email system.

A major concern in developing a policy is to ensure that there are audits performed to ensure compliance. Too often, a policy is known only to those who have been involved in the project and not communicated to the whole organization. Knowledge is critical for all employees, especially those who are new.

Audits should be significant, but fun. The "email police" at your desk should be notable, but non-threatening. If email management is fun, it may be welcomed. Some organizations provide gift cards for users who have gone "beyond the call of duty" in managing email. Others provide certificates of achievement for similar excellent governance practices. Most users like to be recognized for outstanding performance in all areas.

After you have drafted your email policy, ensure that legal council reviews it for accuracy and completeness. An experienced lawyer will be familiar with any state or provincial laws that may impact your organization's risk strategies or e-policies.

11. Training

Emphasize the benefits of the email program, as you provide a better understanding of the system.

Training should reach all new users in the organization, to include:

- Review of written email policies
- Expectations in the use of email, example: privacy
- Best practices in writing and sending emails
- Email etiquette
- Risk factors, example: reduce litigation
- Sign-off of understanding and acceptance of policy

There are many different ways to perform training. A PowerPoint presentation often is the tool. However, using low-cost digital or video cameras, together with editing software, an ingenious email administrator can assemble a semi-professional presentation. If you have a marketing department, use their services. Similarly, if you are not comfortable writing the script, ask Human Resources or training department to assist. The better the presentation, the greater the impact upon the user. Levity added to the presentation increases the level of trainee acceptance because the exercise may become a fun adventure.

Training should apprise users that all emails belong to the organization, who purchased the software and hardware. Further, advise that emails may be monitored. Avoid a "Big Brother" appearance by asserting that you are not spying on them, but simply trying to reduce risk within the organization.

12. Generally Accepted Recordkeeping Principles

GARP® ARMA INTERNATIONAL — Generally Accepted Recordkeeping Principles®

ARMA International launched GARP® to provide guidelines in managing records and information in the normal course of business. These guidelines enable organizations to create, organize, maintain and use records such as emails, so that they are managed more effectively.

These principles are comprehensive in scope, but general in nature. They are not addressed to a specific situation, industry, country or organization, but are intended to set forth the characteristics of an effective recordkeeping program, allowing flexibility based on the demographics of the organization.

Whether your organization includes staff records management professionals or not, the following principles apply to all records within an organization, which includes transitory or official emails records:

- **Principle of Accountability**

An organization shall assign a senior executive who will oversee a recordkeeping program and delegate program responsibility to appropriate individuals, adopt policies and procedures to guide personnel, and ensure program auditability.

- **Principle of Integrity**

A recordkeeping program shall be constructed so the records and information generated or managed by or for the organization have a reasonable and suitable guarantee of authenticity and reliability.

- **Principle of Protection**

A recordkeeping program shall be constructed to ensure a reasonable level of protection to records and information that are private, confidential, privileged, secret, or essential to business continuity.

- **Principle of Compliance**

The recordkeeping program shall be constructed to comply with applicable laws and other binding authorities, as well as the organization's policies.

- **Principle of Availability**

An organization shall maintain records in a manner that ensures timely, efficient, and accurate retrieval of needed information.

- **Principle of Retention**

An organization shall maintain its records and information for an appropriate time, taking into account legal, regulatory, fiscal, operational, and historical requirements.

- **Principle of Disposition**

An organization shall provide secure and appropriate disposition for records that are no longer required to be maintained by applicable laws and the organization's policies.

- **Principle of Transparency**

The processes and activities of an organization's recordkeeping program shall be documented in an understandable manner, and be available to all organization personnel and appropriately-interested parties.

If your organization does not have a formal records management program, use these guidelines as a starting tool. The complete GARP® program can be found on the www.arma.org website. If you have a formal records program in place, use GARP® to measure the qualitative nature of your program, for this may advance your records or email program.

13. Risk Management

13a) Encryption of email

Encryption is a security measure to ensure that the receiver of the email is the only person or group who can open the email. A key (or password) is usually sent under separate cover, which when entered, unlocks the email.

This can be a problem for email records which have long term retention. If the record is stored encrypted, the only access is via a key. If the key is lost, so is the ability to open the email. Ensure that all encrypted emails can be opened in the future.

Local governments sometimes restrict the use and export of encryption software and related information. Organizations should be aware of any restrictions within their jurisdiction.

13b) Litigation[12]

Jurisdiction may affect risk. Canada and Europe do not tend to be as litigious as the United States. Accordingly, the risk factor is heavier there. Email may be affected by jurisdiction.

Courts consider the "trustworthiness" of the record in its admissibility in a court of law. This causes some problems for email records. Some systems allow the user to alter the email record, thus compromising the integrity of the email. A user with malicious intent could make it appear that something was written, when it really wasn't. Other systems allow messages to be altered, but the header information needs to reflect the change to the original email. Creation and adherence to a policy that is sensitive to such variances will reduce risk of litigation in government offices.

Metadata (specific information contained within the email such as date, time created, addressee, and addressor) should be a part of any worthwhile email system. In the event of litigation, legal council may not only request the body of the email, together with attachments, but also the metadata behind the email, in order to ensure the trustworthiness of the record. The Information Services/Information Technology/ Records group can assist in this area.

Lawsuits where users sued their organization over the expectation of privacy have increased. Privacy policies were generally in place, nonetheless there were lawsuits. To protect your organization, have each user sign-off that training was received, and that organizational expectations were communicated, understood and accepted. Yearly sign-off on the policy further reduces risk to the organization and refreshes the user's memory.

For further guidance on email, see the NAGARA/ IIMC bulletin on e-discovery.

13c) Legal Holds

An email system should be able to apply legal holds. Thereby, the administrator can protect the organization against un-necessary destruction of emails which could be a part of the litigation process. All emails which may be a part of litigation should be retained. A legal hold protects an email and extends its retention until the value of the email has diminished.

In many cases the legal hold process has not been administered and email records have been wrongly destroyed. This resulted in costly penalties, often millions of dollars, or in some cases, led to closure of the firm[13]. Legal holds should be administered when:

- One party is advised by the other that a lawsuit will be initiated
- One party has reason to believe, based on overtures or investigation, that the other party is considering or preparing for a lawsuit
- Your organization foresees possible consequences as a result of a certain action

Once litigation has started, courts impose a duty to preserve email records relevant to the case until the matter has been resolved. If the organization fails to preserve the records, courts may conclude destruction of email records was an attempt to circumvent justice. Such irresponsible management of records has resulted in court sanctions, such as striking out part of the case, losing the case, fines, or imprisonment[14].

13d) Email Viruses

An e-mail virus is computer code sent to you as an e-mail attachment which, if activated, will cause some unexpected, and usually, harmful effect. Adverse results may be destruction of certain files on hard disk or re-mail of the attachment to everyone in your address book. While there are other kinds of computer virus, e-mail viruses are the best known and may cause great loss of time and money. Two effective defenses against e-mail viruses for the individual user are:

(1) A policy of never opening (for example, double-clicking on) an e-mail attachment unless you know who sent it and what the attachment contains, and
(2) Installing and using anti-virus software to scan any attachment before it is opened.

Symantec Hosted Services suggests that 1 in 80 email links are malicious in nature, designed to cause great harm to your computer and network[15]. Also, web based malware loaded without user permission is used by hackers to access private information or retrieve passwords.

14. Summary

No thinking professional fails to manage email. Organizations need to determine the difference between transitory and official records, and store emails according to content. Applicable statues, regulations and laws, together with internal policies and procedures, determine the course of action for retention and management of emails. Electronic email system software such as Athena Archiver is available to assist administrators in creating, identifying, maintaining, protecting and disposing of emails.

This report has outlined eight different scenarios to assist in managing emails. Some systems standalone; others are meant to cooperate. For instance, a system may apply quota limits, together with storage in a content management system or an archival system. New technologies offer innovative possibilities.

The best solution may integrate your current email system. Leveraging existing technology may be more cost effective. Cooperate with the reseller of the software, or with the existing software developer, to determine if changes may provide an effective email system. It may be best to start from scratch rather than throwing good money after bad. Neither cheap, nor expensive, solutions may be the best. If funds permit, consider hiring an email or records consultant to help keep your project on track.

The amount of risk tolerance within your organization will help you choose an effective system. All email solutions may increase productiveness within your organization. Response to litigation or Freedom of Information requests will be quicker and less costly with any email system. Much of the software today is web based. This allows local users and the general public to access via the internet certain records logging on to the email server. Your goal, and reward, as the email administrator may be an optimum email system. Use the information within this report to determine the correct system for your organization.

Email Deployment Checklist

__ Document the current situation. Identify problems within your organization, talk to users.

__ Secure an executive sponsor.

__ Create an Email Strategic Planning Group (ESPG). Communicate your email records message.

__ Determine business drivers for your organization.

__ Evaluate email solutions. Share solutions with the ESPG. Develop basic requirements.

__ Build relationships with other leaders.

__ Formalize a Request for Information (RFI).

__ From the results of the RFI, determine a preliminary budget. Share requirements with senior management and the Information Technology group.

__ Receive preliminary funding.

__ Develop possible solutions with ESPG.

__ Draft a Request for Proposal (RFP) including all requirements for the email system.

__ Have ESPG evaluate draft RFP, formalize and send.

__ ESPG evaluates results, receives further clarification, and chooses solution.

__ Finalize funding.

__ Pilot solution with heavy user group. Work out bugs.

__ Develop communication and change management component.

__ Develop policy and procedures.

__ Create email manual and cheat sheets

__ Work with Records Manager to determine file structure and retention.

__ Initial, and on-going, training.

__ Rollout out email program, department by department.

__ Evaluate success, gather feedback and make necessary changes.

__ Perform yearly audits for compliance and governance purposes.

This chart is basic in nature but can be used as a guide to develop your program. All organizations are different and the necessary steps for your solution may need to be adjusted.

References:

Mary Belis, History of Email http://inventors.about.com/od/estartinventions/a/email.htm

Email spam, Wikipedia - http://en.wikipedia.org/wiki/Spam_email

Jennifer Kavur, "Email Overload" IT Business, Computer World Canada, March 23, 2010

http://ezinearticles.com/?Email-Archival---The-New-Frontier&id=4688097

Mary Flynn, The ePolicy Handbook, Designing and Implementing Effective E-mail, Internet and Software Policies, 2001, ISBN 0-8144-7091-2

#saa10: The Cloud - Opportunity or Risk for Records Managers?, Mimi Dionne www.cmswire.com/cms/enterprise-cms/saa10-the-cloud-opportunity-or-risk-for-records-managers-008314.php

Barclay T. Blair, Governance for Protecting Information in the Cloud, ARMA International's Hot Topic: Making the Jump to the Cloud?

Guideline for Managing Email, ARMA International, 2000, ISBN: 0-933887-91-4
ARMA International, Requirements for Managing Electronic Messages as Records, 2000, ISBN: 1-931786-22-4

Robert F. Williams, Lori J. Ashley, 2009 Electronic Records Management Survey, Call for Sustainable Capabilities, Cohasset Associates

What is email virus? http://searchmidmarketsecurity.techtarget.com/sDefinition/0,sid198_gci214549,00.html

Security As A Service: Managing Email Security for Today's Threat Landscape, Symantec Hosted Services half day seminar

Footnotes

[1] 2003 UC Berkeley study

[2] AIIM Market Intelligence, Industry Watch, Email Management – The good, the bad and the ugly, 2009

[3] The Radicati Group Inc study, "Business User Survey, 2008

[4] Computer World Canada, Jennifer Kavur, April 6, 2010

[5] Winning Strategies for Successful Records Management Program, Dr Mark Langemo, CRM, FAI, 2002, Information Clearing House Inc., ISBN0-929316-59-9

[6] Information Management Journal, ARMA International, "Harnessing the Winds of Change", November/December 2010, Ganesh Vednere

[7] Dan Fletcher (November 2, 2009). "A Brief History of Spam". http://www.time.com/time/business/article/0,8599,1933796,00.html. Retrieved 2010-09-23

[8] Government of Alberta, "Official and Transitory Records: i A Guide for Government of Alberta Employees' 2004, Page 12 www.rimp.gov.ab.ca/publications/pdf/OfficialTransitoryRecordsGuide.pdf

[9] The ePolicy Handbook, Designing and Implementing Effective E-mail, Internet, and Software Policies, Nancy Flynn, 2001, ISBN 0-81144-7091

[10] Gartner Research, June 2010, http://www.gartner.com/it/page.jsp?id=1389313

[11] www.mainframezone.com/it-management/storage-data-management-optimize-your-data-archiving-without-sacrificing-performance

[12] Zubulake v. UBS Warburg LLC,, 2003 U.S. Dist. LEXIS 12643 (S.D.N.Y. July 24, 2003).

[13] Arthur Andersen

[14] Pension Comm. of the Univ. of Montreal Pension Plan v. Banc of Am. Sec., LLC, No. 05 Civ. 9016, 2010 WL 184312 (S.D.N.Y. Jan. 15, 2010).

[15] Security-As-A-Service: Managing Email Security for Today's Threat Landscape, Semantic Hosted Services, half day seminar