Why today’s Email Archiving Technology alone is a losing proposition and what you can do about it.

This paper is designed to provide invaluable planning information to you along with Best Practice Advice built upon significant experience gained by ReSoft International in assisting its clients in implementing Email Archiving solutions.

Outside of certain regulated industries, some 70% of companies today are not Email-Compliance-Ready and do not necessarily see the benefit of being so. Unless regulations or previous litigation episodes are forcing action to be taken, the need and associated dollars to act are driven by a new and, most likely unanticipated, event. Response to this event is, inevitably, a reactive and chaotic approach.

Email Archiving is not the End Game.
Many of those organizations that are today focusing on Email archiving see it as a panacea of protection. But Archiving can only ever be a defensive position and is only really the tip of the iceberg. By the time the incident gets to a legal discovery request, for which you are implementing email archiving to respond to, in many respects you have already lost the battle - in cost, in time, in use of resources. So there is a choice of making discovery responses a routine activity or an unplanned, chaotic episode

What can be done pro-actively to mitigate this? We argue the following steps should be considered in addition to implementing an Email Archiving Solution:
- define consistent, defendable Acceptable-Use policies
- implement a measurable process for Distribution AND user Understanding of Acceptable-Use policies
- implement a Document Classification process to allow users to determine what does/doesn’t get kept as a business record – capturing email from the journal is expensive in process, storage, licensing, administration & makes extraction slower and more expensive management - no-one really wants to do it!
- Legal discovery is inevitable. Plan for it by setting achievable service-level goals for retrieval & analysis of respondent email.

Remember, there is always a risk of malicious intent by the employee. However, if this is planned, the employee will always find a way to get round any existing recording mechanism you have - a phone call, USB Drive, ftp upload etc.

What the Legal Profession is saying.
The Sedona Conference (www.thesesedonaconference.org) is an independent charitable, 501(c)(3) research and educational institute dedicated to the advancement of law and policy in the areas of antitrust law, complex litigation and intellectual property rights. It exists to allow leading jurists, lawyers, experts, academics and others, at the cutting edge of issues in the area of antitrust law, complex litigation, and intellectual property rights, to come together - in conferences and mini-think tanks (Working Groups) - and engage in true dialogue, not debate, all in an effort to move the law forward in a reasoned and just way.

Putting it all together:
The Email-Information-Governance-Lifecycle
Preparation Questions for Defining an Email Archiving/Retention/Analysis Policy

The Sedona Conference Working Group on Best Practices for Electronic Document Retention & Production has issued the following guidelines:

1. An organization should have reasonable policies and procedures for managing its information and records.
2. An organization’s information and records management policies and procedures should be realistic, practical and tailored to the circumstances of the organization.
3. An organization need not retain all electronic information ever generated or received.
4. An organization adopting an information and records management policy should also develop procedures that address the creation, identification, retention, retrieval and ultimate disposition or destruction of information and records.
5. An organization’s policies and procedures must mandate the suspension of ordinary destruction practices and procedures as necessary to comply with preservation obligations related to actual or reasonably anticipated litigation, government investigation or audit.

Building a Workable System for you.
With this in mind, the rest of this paper focuses on the areas to consider when implementing an email archiving and retention solution to protect the organization. We cannot define the retention rules that you need to use but we can provide a checklist of the areas that our other customers have looked at.

a). Defining User Acceptable-Use Behavior to prevent future infractions
   • How often will you distribute your Email Acceptable-Use Policy?
   • What commitment do you require from your users that they have read and understood the policy and consequences for infraction?
   • What level of confidence do you have that your-now-educated employees will fulfill their obligations of the Acceptable-Use Policy?
   • What plan of response will you have to any infractions?
   • How will you demonstrate you are monitoring & measuring user compliance, understanding and possible infractions of the policy?

b). Defining Email Retention Policies to capture potential infractions
   • For which of your users will you be capturing email?
   • How long do you need to keep it for and will it vary by context/user (eg: HR, Legal, Tax, Sarbanes, Executives etc.)?
   • Does archived mail have to be an EXACT replica of the original for Legal purposes?
   • Does the email need to be stored in a form that cannot be tampered with?
   • Do you wish to archive all types of message (not just Email, possibly Calendar, Memos, Drafts etc.)?
   • Do you need to keep copies of all email regardless of whether the user still has it in their mailbox?
   • If not, do you want the user to determine which messages should be captured and which can be purged?
   • Will you remove email from a user’s mailbox after a certain age?
   • Will you allow users to save copies of email into a Personal Archive?
   • If so, how long can the user then maintain the email in the Personal Archive?
   • What proof do you need that you have collected the right messages?
   • Do you need to set up a sampling process to audit your capture process?
   • Do you wish to put any restrictions on emails a user sends – perhaps based on words in the email, or being addressed to a competitor; if so, what action do you want to take – block delivery, warn?
Preparation Questions for Defining an Email Archiving/Retention/Analysis Policy

• Once implemented, do you want the system to start capturing from that point onwards or do you need to capture old emails that may already sit in mailboxes, Personal Archives or on backup tapes?

c). Defining Retrieval & Analysis Policies for Accessing and Analyzing the Captured Emails

• Who will be able to access the captured messages?
  o Email Administrator
  o Compliance, Legal or HR
  o User to access their own messages

• What types of search criteria will be used to query the Archive?
• What information will you require regarding discussion-threads, communication flows between users as part of the search?
• What is your target turnaround time to retrieve messages after the request has been made?
• What is your target turnaround time to have analyzed the respondent messages for compliance?

d). Technical Questions

• Do you have traveling users that need access to their Archive while disconnected?
• Do your users need to get access from webmail?
• Will you archive into a single container or into Use-specific containers?
• Where will you store archived messages, does it need to be non-tamperable, does it need to get cycled as it gets older (eg: first 90 days in mail file, next 360 on SAN, remainder on tape etc.)??
• What are your requirements for an exit strategy for the archived email (eg: migrate mail out of the archive if, say, after 5 years you find another solution)?
• Do you have or wish to have Quotas, what are they?
• What do you want to happen when the user hits their Quota?
• Do you want to warn users as they approach their quota?

What should I do now?

ReSoft International is here to help you. We are an independent integrator and reseller of best-of-breed software technologies that address Email & Instant-Messaging Security, Regulatory Compliance and Storage Relief.

1. Get Educated – ReSoft has put together a comprehensive White Paper Library addressing many of the issues you are probably facing. Some of the areas the Library covered are highlighted below. You can download any of these white papers free of charge.

RESOFT WHITE PAPER LIBRARY SAMPLE: http://www.re-soft.com/wp

2. Contact ReSoft for further discussions on how we may be able to help you. ReSoft has, for over 16 years, acted as a trusted advisor to hundreds of organizations, applying the relevant technologies and techniques from its broad set of Email & IM Security tools to reduce liability risks and save time.

This paper has set out to illustrate ReSoft’s significant coal-face experience in providing professional services and solutions that have helped many organizations to define & implement policy-based Archiving & Discovery systems across industries and organizations of all sizes. We have defined what we believe are the key questions to be asked when planning what to

“Frost & Sullivan believes that Re-Soft's main competitive advantage lies in its ability to offer a complete solution for the content security space that more specialist vendors are not able to match. This strength is likely to have a positive effect on the company's growth in the market.”

Frost & Sullivan
Preparation Questions for Defining an Email Archiving/Retention/Analysis Policy

do with PST files. These questions are part of an Archive Planning Workshop we offer to assist organizations in determining whether they need to deploy email archiving, what components would be required, and how they would be justified.

For Further Discussions, please contact:
ReSoft International LLC
PO Box 124 New Canaan CT 06840
http://www.re-soft.com  203 972 8462  info@re-soft.com