

## Where Should an Organization Manage Email?

By Kris Brown - Posted Feb 1, 2006

Every organization is watching their email storage grow at an exponential rate. As email and electronic communications change the way organizations do business, IT groups have to deal with masses of emails. While IT groups are dealing with infrastructure issues, records managers are losing sleep over the information that is being lost in these email stores. C-level management is becoming aware of the growing problem, and seeking solutions. The question is "Where should our organization manage email to manage our organization's risk?"

The concept of "where" is one that doesn't necessarily jump out at the IT administrators who are trying to deal with this problem. However, this is one of the most important influencers in whether an organization will be successful in its attempt to manage the email problem.

There are four 'locations' where email can be logically managed within an organization. Each has its own advantages and disadvantages; however, only one of these will really help an organization to truly manage the records that are created in email. The four locations are:

1. At the SMTP gateway—the location where all incoming and outgoing communication via email occurs. This doesn't capture vital internal communications.
2. At the intranet email server—all the internal communication could be captured as well as all delivered and authored communications, regardless of source or destination.
3. At the email client—where most email in an organization is created or received. Leveraging an automated tool at the desktop could be an easy way to ensure that the email is captured without interaction.
4. At the individual—who sends and receives the email. With the right tools and training, the individual could capture emails, while adding valuable metadata.

Defining these locations leads to the next obvious question: How do I determine the best location? A key factor in this determination is understanding why the organization is capturing the emails in the first place. If the organization is capturing emails for compliance, governance and best practice, there is only one location for this to happen—at the individual level. This allows the organization to apply the records management rules to include:

- appropriate classification;
- appropriate retention and destruction;
- ability to retrieve the email in a timely fashion; and
- ability to scale with the size of the email stores.

The individual is the best person to correctly classify the email, in terms of the metadata that they provide to the email management, and therefore records management, platform. With a well-defined classification structure, an individual is able to ensure appropriate retention and destruction policies are applied, without having to understand the business rules that drove the development of that structure. Most importantly, only a system based on metadata search rather than document content search can truly scale to cover the evergrowing volumes of email content that needs to be managed.

All the other locations require complex artificial intelligence, via rules or other systems, to "guess" how to classify an email. They will also require ever-larger document content index engines to process the enormous email stores for searching. When information is misclassified by these automated systems, it may be kept longer than it is required to be. This, of course, means organizations are potentially increasing their liability in terms of emails not destroyed and this breeds risk, and no one needs to hear any more stories of the email that killed a career.

So where should an organization manage its email? This question's answer lies in the following rhetorical question: If it was your career on the line, would you want a system with default rules to classify the key piece of information...or the person who sent or received it?