



Intelligent email archiving

by Michael Murphy

WITHIN THE PUBLIC sector, email is as mission-critical as any other IT system. As a result, organizations are evaluating their overall policies and systems for managing email, and IT professionals are being called on to address the most common email management concerns, including resource management, retention management, and discovery management.

Increasingly, Canadian public sector institutions are evaluating or using email archiving software solutions to manage these issues. With these systems, IT can control the growth in email storage costs while giving end users email storage and search capabilities in a more user-friendly manner and providing legal departments a consistent system for retaining and finding emails. While these systems simplify the issues of archive storage size, archive retention period, and archive search, the issues don't disappear.

Why not? Because not all email is created equal. Some email is an asset; other email is a liability. The amount of time it should be retained depends upon the category into which the email falls. Government sectors using email archiving systems either have no automated archiving system – they archive, but keep everything for the same period of time, or they archive, but keep all data forever.

There is a better way: enter intelligent archiving.

A natural evolution of early email archiving software solutions, intelligent archiving utilizes intelligent classification and retention technologies to capture, categorize, index, and store target data to enforce policies and protect assets – all while helping to reduce storage costs and simplify management.

Intelligent archiving solutions address a fundamental challenge of email storage and discovery: data classification. Rather than treating all email the same, intelligent archiving offers intelligent classification and categorizes messages according to their relevance to specific purposes. Only when data is appropriately classified can it then be intelligently filtered, retained, and discovered.

Not only do different types of email messages have different values, different departments have different classification

Governments of all levels are custodians of massive amounts of sensitive public information. Be it health records, tax returns, driver's licences or other confidential data, it is all stored somewhere within a government's computer network, and a significant amount of this information – often important information – is found in the form of email. Archiving it appropriately for retrieval when required (i.e., legal discovery process) can be a challenge.

needs for their information. For example, highly process-driven ministries such as finance or health may require much more granular classification than would a department with more fluid interaction. Other sections may already have an enterprise content management (ECM) system in place and simply want to extend it to archived email.

Intelligent archiving accommodates these classification approaches offering user classification that allows individuals to sort messages as part of archiving, automated classification that tags messages based on rules, and integration with ECM systems that applies existing ECM policies to email messages.

User classification

Many organizations rely on their users to make difficult decisions about what email to save or delete. However, this often burdens them with too many processes and impacts their productivity. For example, the user may be tasked with using a Web interface, saving an email to a specific folder, or using an application plug-in to specify metadata.

Intelligent archiving systems offer a seamless, intelligent user-driven classification model, reducing the number of steps the user must take in classifying emails. This software monitors user email activity, identifies email that needs to be classified, and prompts the user to choose from a subset of predefined classifications only when necessary.

By providing a policy-based email capturing process, the user classification engine enables all government-critical and regulated email to be sorted as each item is created or read by the user. This helps enforce user retention policies by taking control of records where they are most vulnerable.

Automated classification

In contrast to user classification, automated classification takes decision making out of the hands of users and puts it into the circuits of the archiving system. Today's classification engines use a combination of approaches to analyze a message and determine the type of content.

For example, an automated classification engine may evaluate senders and recipients as well as the groups in which they reside to determine content type. It may also evaluate message direction since messages sent externally often merit a higher degree of scrutiny and retention. An automated engine may evaluate messages for keywords or phrases or for patterns, searching emails for sequences – like those that identify social insurance numbers, for example.

The most robust intelligent archiving systems offer a wide variety of tagging rules based on customizable or predefined conditions. Flexibility is key because rules can be established on multiple levels. Tagging rules also allow for certain actions to be taken on messages, including retention setting, exclusion, and flagging for review.

Integration with ECM

Many public sector organizations may already have an ECM system in place that categorizes and manages records across multiple content types. These systems can be integrated with intelligent email archiving systems to allow the archive to store and optimize email while enabling the ECM system to drive retention decisions that are consistent across different types of data. Once messages are in the integrated system, users can browse and search for messages managed by the system.

For external management of retention policies, objects are created in the ECM system that reference archived messages in the intelligent archiving system. These objects are then controlled by the ECM system's standard policies, which age objects through configured retention lifecycles and ultimately delete objects as they reach expiration. When a retained message is deleted with the ECM system, the integration ensures that the corresponding archived message is removed from the archive.

Putting intelligence to work

Once messages are categorized using user or automated classification or integration with ECM systems, the intelligent archiving system leverages 'intelligent filtering' to delete non-relevant email before archiving; 'intelligent retention' to determine how long to keep archived emails based upon their classification; and 'intelligent discovery' or review to tag emails with metadata to make them easier to search and discover in the future.

Public sector organizations can also augment the benefits of an intelligent archiving system with best practices for email retention including:

- Archive all email for at least the same period of time that backup tapes were retained.
- Organizations are recommended to place holds on all email that is subject to outstanding investigations to ensure it is not deleted.
- Organizations should also ask users to drag email into records folders in their email system to classify email that needs to be stored for longer than the default period; these folders should be pushed out only to users who tend to be process-oriented.
- Finally, organizations should apply a default policy using automated classifi-

cation for other groups of users and enforce an overriding policy to retain email that has been flagged as containing sensitive information.

Regardless of the direction governments take for managing email, adding intelligence to their archiving policies helps ensure the balance of storage optimization, records retention, and fast discovery while capturing the business value of email archiving implementations.

An intelligent email archiving system provides a common framework that consistently enforces content control policies across an organization – from email gate-

way security to archiving. IT professionals can proactively prevent the risk of data loss and policy violation and respond to e-discovery requests rapidly and cost-effectively. With such a streamlined and centralized approach, public sector employees can not only retrieve data quickly but have the opportunity to analyze it as well – turning data into a useful tool rather than an inactive cost centre. ☞☞

Michael Murphy is vice-president and general manager, Symantec (Canada) Corp.