

# The Art of Destruction

## An Overlooked Key to Records Management and e-Discovery

By Dr. Johannes C. Scholtes, President and CEO, ZyLAB North America LLC

Although storing 250 gigabytes of data can cost less than \$250, hiring an external firm to process and review this data for e-discovery can cost up to \$1 million. The impact of these costs is particularly noticeable to in-house legal teams and support staff who are often at the front lines of any e-discovery activities occurring within their organizations. Even though advanced information access technologies are available to help minimize these costs, many legal professionals do not yet have these tools in place, and for those who do, they are still confronted with the primary challenge to effectively managing e-discovery costs: the continued addiction throughout organizations to keeping and storing *too much electronic data*.

To put this problem in perspective, think about how much data your organization currently stores. Then, project that amount through the revised definition of Moore's Law, which predicts that computing and storage capacity will continue to double every 18 months—probably for the next two decades. Storage costs themselves are so low that constantly bumping up capacity can seem like the obvious, no-brainer solution to “managing” data. However, you will soon find out that your legal e-discovery costs can also comply to Moore's law: they will also double every 18 months.

To neutralize e-discovery cost and risk issues, organizations must classify documents with a proper filing plan and implement data retention and destruction policies. Regulatory authorities have established clear guidelines (i.e. Federal Rules of Civil Procedure) about what data must be kept and for how long. Only in rare cases do all email messages, for example, have to be stored. Often, no practical or legal requirements exist for retaining large chunks of organizational data, especially when one considers that data is often duplicated throughout an organization.

Unfortunately, many people are pack rats at their jobs, collecting and storing every email they send and receive as if the entire company would crumble without a solid foundation of ever-growing data repositories on which to rest. But data retention isn't synonymous with knowledge management, and knowledge management is what is supposed to be the goal of any

kind of implicit or explicit data retention activity. For “data” to become “knowledge,” data must be structured and organized, and an understanding must be in place about the impact of that data.

### The Need for Email Destruction

Email is where the high costs and risks of e-discovery are concentrated. People keep their emails because it is easy, but these email archives (PSTs) rapidly swell to gigabytes of information. Problems fester because the information in these PST folders is often completely unstructured. For example, potentially sensitive HRM-related emails (such as performance reviews or confidential financial or medical information) are frequently in the same collection (i.e. Sent Mail) as other, unrelated messages. This common situation is

***“You will soon find out that your legal e-discovery costs can also comply to Moore's law: they will also double every 18 months.”***

problematic on two fronts: non-relevant emails are kept, and confidential emails that can be classified as “privileged” in a legal discovery are not stored in separate folders.

In order to implement and execute a filing plan for your organization, you must classify every type of document you have, establish retention rules for each type, and enforce these rules.

All of which seems logical and straightforward. However, although most organizations have some type of document retention policies in place for physical documents, almost 95% of organizations do not apply



**Dr. Johannes C. Scholtes**

Dr. Johannes C. Scholtes is the president and CEO of ZyLAB North America LLC and is in charge of ZyLAB's global operations. Since Scholtes took over the leadership in 2002, ZyLAB has enjoyed double-digit expansion as well as consistent annual growth in

profitability. Before joining ZyLAB in 1989, Scholtes was an officer in the intelligence department of the Royal Dutch Navy. Scholtes holds an M.S. degree in Computer Science from Delft University of Technology (NL) and a Ph.D. in Computational Linguistics from the University of Amsterdam (NL).

records management policies to electronically stored information (ESI). Hence, a real need exists to apply the “art” of destruction, as well as of structure and transfer, to all ESI throughout an organization.

This process is easier than it seems. Granted, a big challenge with ESI records management systems is that users often don't like them and don't use them. Email archiving, for example, is often postponed “until tomorrow,” which then becomes the first day of the end of the records management initiative. The only solution in these situations, then, is to make archiving emails as easy as possible, which only works if there's a (semi)-automated system in the email environment (such as in MS Outlook). However, the effectiveness of this plan is only as good as the filing plan that supports it.

### Developing a Filing Plan

Effective records management must follow a logical sequential order. Many organizations that buy an electronic records management system have no idea what document collections exist in their organization, especially in terms of essential archives that may only reside on someone's personal hard disk. To compound the issue, opinions often differ about what collections should even exist in their organizations. Therefore, the first step is to define a list of essential archives. Start by looking at your organization's departments and their recognized information flows.

Departments and their relevant archives could include, for example: sales (contracts, customer contact files, quotes); management (board minutes and notes, legal agreements, quality control); finance (accounts payable, accounting, correspondence files with various external contact); and on down the departmental lists.

After mapping out the departments and relevant archives, define the documents that must be retained in each archive (paper, electronic and email), as well as who has the appropriate access rights, the location of the archive (physical or network-based), the responsible officer and the retention and destruction rules. Responsible officers carry out and enforce the collection, structure, access and retention rules for the documents in their designated archive. The basic filing plan is in place.

## Rolling Out Records Management

Next, the filing plan needs to be put into action, which can be done manually. Fully automatic RMA systems aren't necessary as long as data has been clearly separated into archives and locations that allow for individual retention actions. For example, if all outgoing quotes from one year are stored in one directory, they can be deleted in one batch when their designated destruction data comes up.

Some additional points to consider:

- ◆ To eliminate the need for local copies, all employees should store emails, documents and records in an assigned archive as early as possible in the business process;
- ◆ Unstructured legacy archives must be organized and structured. All local, personal and backup copies of archived and non-relevant, non-archived local emails, paper and electronic files should be destroyed on a specific, realistic date;
- ◆ The most sensitive documents are confidential documents and (potentially) privileged documents that typically come from HR or are documents you receive from parties with whom you signed a nondisclosure agreement; and
- ◆ After the RMA system gets rolling, data retention must be enforced by the responsible officers.

Exchange server mailboxes and PST repositories are not designed for, and should not be used as, document archives. All relevant emails and documents must be archived in assigned repositories. Some tips to consider:

- ◆ Implement an appropriate email archiving tool;
- ◆ Set an automatic deletion date for all messages, calendar items, journals and tasks older than 90 days that still reside on your MS Exchange server in personal, shared, or functional mailboxes and in central repositories (public folders and the list server). This wholesale deletion will occur every three months; and
- ◆ Old email repositories (PST and server-based mailboxes) also need to be sorted out and cleaned up before a set date. Choose a group to help support this activity. Consider using the same group that

# RM, E-Discovery and Knowledge Management

## ZyLAB's Universal Approach

Since 1983, ZyLAB has worked alongside professionals in the auditing, legal and intelligence communities to develop the best tools for investigating and managing large sets of archived data. These award-winning technologies have been bundled into the ZylIMAGE Information Access Platform, an integrated document, content and records management solution that enables businesses, auditors and legal professionals to capture, investigate, structure and disclose information in an efficient and secure manner.

ZyLAB offers specific process functionality, relevancy modeling, and flexible content analytics, all supported by ZylIMAGE's robust search capabilities and an XML-based archiving framework that is applied for a number of specific applications:

- ◆ Email archiving
- ◆ E-discovery and e-disclosure;
- ◆ Corporate compliance and contract management;
- ◆ Case management and litigation support;
- ◆ Back-office records management for organizations facing legal risk, such as construction, outsourcing, customer service, medical or HR environments;
- ◆ Federal and local government records management; and
- ◆ Historical files.

The ZylIMAGE Information Access Platform is optimized for these applications due to its combination of search technology, security and business-focused content-management functionality. ZyLAB can quickly deploy even the most complex installations of specialist solutions and provide all the necessary training, documentation, support and maintenance.

ZyLAB also offers text-analytics technology that supports more than 200 languages and can be easily deployed to scale. The ZylIMAGE Information Access platform enables organizations to bring knowledge management in house, take the mystery out of e-discovery and stabilize comprehensive records management initiatives.

works on electronic discovery projects because performing clean-up activities provides a good training environment for e-discovery team members.

The email archiving method can proceed as follows:

1. Create a copy of the filing plan in every user's mailbox. Users can then drag and drop relevant emails into these folders and create subfolders where needed.
2. Make sure that software is in place that provides an option to automatically archive Sent messages to a designated location on a regular pre-defined basis.

## Training and Enforcing your RMA Solution

Users need to be trained on how to file relevant emails, paper documents, faxes and electronic files when they become an employee. HRM and the direct manager are responsible for conducting this training.

Although they can delegate enforcement of this policy, the responsible officer always has final responsibility. In addition, IT people must be trained on how to discover PSTs on the network and restrict the usage of memory sticks and CDs/DVDs. Any copies made must be registered.

Make sure that an authorized officer (ideally a board member) annually checks the responsible officers for execution of these procedures. RMA is useless without the proper training and enforcement to support it.

To sum up, filing plans are the drivers of effective electronic records management, and one of their critical components is their ability to instigate controlled, yet thorough, document destruction. To enhance user acceptance, consider starting with a manual system and then gradually automating relevant parts.

After a plan is in place, more advanced automatic filing systems, such as those with text analytics technology, can be used to automatically classify records into the filing system. ■