ZyLAB®
eDiscovery & Information Management

The Art Of Destruction

ZyLAB White Paper

Johannes C. Scholtes, Ph.D.
Chief Strategy Officer, ZyLAB

Contents

Summary 3

The Art Of Destruction 4

- An overlooked key to records management and e-discovery 4
- Understanding the need for destruction 5
- Developing a filing plan 5
- Rolling out a records management system 6
- Training and Enforcing your RMA Solution 7

Different approaches for different data 8

- Tackling the e-mail problem 8
- Collecting from and cleaning file shares 9
- Cleaning up Microsoft SharePoint repositories 9
- Audio records management 9
- Archiving and cleaning other databases 10
- Archiving and cleaning from the cloud and remote storages 10

Conclusion 11

About ZyLAB 12

Summary

Keeping data is tempting and storing of data is cheap. But in case of an e-discovery or edisclosure, hiring an external firm to process and review this data can be paramount. Proper records management and destruction policies can dramatically increase business efficiency, minimize legal risk and reduce cost in case of litigation.

In this whitepaper we will illustrate the need for destruction and show how to develop a filing plan and how to roll out a records management system. We address the issue that different data like email, audio files or data on file shares, Microsoft (MS) SharePoint remote storages or in the cloud requires a different approach.

The Art Of Destruction

An overlooked key to records management and e-discovery

Although storing 250GB 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 that 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, if situations arise in which particular information must be found and retrieved within repositories, storage-first solutions compromise organizations' ability to control processing costs, work efficiently and minimize legal risk.

"The principles of Moore's Law infer that the cost of e-discovery can double every 18 months if data is not effectively controlled"

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 e-mails, 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 hoarders in their jobs, collecting and storing every e-mail 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.

Understanding the need for destruction

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 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.

"For data to become knowledge, data must be structured and organized"

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. E-mail 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 e-mails as easy as possible, which only works if there's a (semi)-automated system in the e-mail 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 e-mail), 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 a records management system

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 e-mails, electronic and paper documents, MS SharePoint projects, (on-site and remote) database content, multi-media files, social media content, and other relevant 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 e-mails, 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 HRM or are documents you receive from parties with whom you signed a nondisclosure agreement.
- After the RMA system gets rolling, data retention must be enforced by the responsible officers.

Training and Enforcing your RMA Solution

Users need to be trained on how to file relevant e-mails, paper documents, faxes and other 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 discovery 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.

Different approaches for different data

Tackling the e-mail problem

E-mail is where the high costs and risks of e-discovery are concentrated. People keep their e-mails because it is easy, but these e-mail archives (PSTs) rapidly swell to GBs of information. Problems fester because the information in these PST folders is often completely unstructured. For example, potentially sensitive HRM-related e-mails (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 problematic on two fronts: non-relevant e-mails are kept, and confidential e-mails that can be classified as "privileged" in a legal discovery are not stored in separate folders.

"Exchange Server mailboxes and PST repositories are not designed to be used as document archives"

Exchange server mailboxes and PST repositories are not designed for, and should not be used as, document archives. All relevant e-mails and documents must be archived in assigned repositories.

Some tips to consider:

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

The e-mail archiving method can proceed as follows:

- Create a copy of the filing plan in every user's mailbox. Users can then drag and drop relevant e-mails into these folders and create subfolders where needed.
- 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.

Collecting from and cleaning file shares

Collecting from file shares is not as hard as it may seem, as long as the right software is in place. With many of these tools retention policies can be executed and early case assessment can be implemented. It is important to be sure one can full-text index all data (also incrementally) and to be sure that whatever data manipulation action one performs is audited.

Cleaning up Microsoft SharePoint repositories

More difficult than the old unstructured file servers, is MS-SharePoint that has replaced many traditional file shares in several organizations. Nowadays we are creating large unstructured data collections in MS SharePoint, which is harder to access than the old file shares.

In case of an e-Discovery, SharePoint presents significant challenges for IT departments. When using MS-SharePoint organizations need to ensure they can:

- Archive projects and documents based on various policies (closed, size, age, people involved, set retention or expiration date, activity) into a open sustainable file format (such as XML and native files).
- Do this with or without stubbing (replacing an object with a pointer to another low-cost storage location, so less expansive memory is occupied on the MS-SharePoint server).
- Implement real-time archiving of files and projects.
- Optionally, include all (hidden) meta-information in your archiving.
- Allow Federated search to your archives from within MS-SharePoint.

Audio records management

The nature of data changes from textual data to multimedia visual and audio data. Audio data exists on traditional fixed-line phone systems, VOIP, mobile and specialist platforms like Skype or MSN Live.

But sound, pictures, phone, video and other multimedia information cannot be searched easily, if at all. Strong audio-search solutions are needed. In order to combat market abuse, insider dealing and market manipulation, the Federal Security Agency now requires organizations that handle client orders to record and maintain records of transactions conducted over telephone lines. These records must be “readily accessible” should the relevant authorities require them. FRCP regulations in the U.S. now allow “sound recordings” to be considered for inclusion in the list of discoverable items that may be requested as part of case preparation and evidence gathering. The wider implications of Sarbanes-Oxley and SEC regulations also influence the frequency with which audio files are called upon as a source of evidence.

Archiving and cleaning other databases

Within an organization, there are also many repositories containing structured information such as financial records, logistical transactions, CRM, HRM, ERP, production and other important information. Companies have to include these repositories in their data map, as this data also needs to be managed as part of the overall filing plan. Since most such systems have proprietary, the best approach is often to archive relevant data in an open format such as XML, or to use specialized software to collect information from these repositories to assist records managers with the identification, transfer and retention of such information.

Archiving and cleaning from the cloud and remote storages

The location of data moves from being within the firewall to being everywhere and nowhere; on home computers, mobile devices, cell phones and of course in the cloud. Companies need to have well defined service level agreements with their cloud, SaaS or outsourcing partners to make sure that they have access to their corporate data when they need it and that it is actually destroyed or transferred when required.

Organizations should update their data retention policy to include:

- SharePoint, blogs, social media
- Unified messaging, voice files, video
- ADP and other financial service providers
- Salesforce and other CRM systems
- FedEx, UPS and other shipping
- BaseCamp, Google docs and other collaboration tools

It is also very important to know which protocols the provider has in place for collection in terms of speed and quality. What can be expected from the cloud provider? What to include into the Service Level Agreements (SLA's)?

Conclusion

An organization needs to consider the whole EDRM model not just one end of the spectrum. ZyLAB is the only supplier with heritage experience in dealing across the EDRM model from left to right. This is making us ideally placed to partner with you if you are at the interim stages of developing your Information Management and e-Discovery strategies.

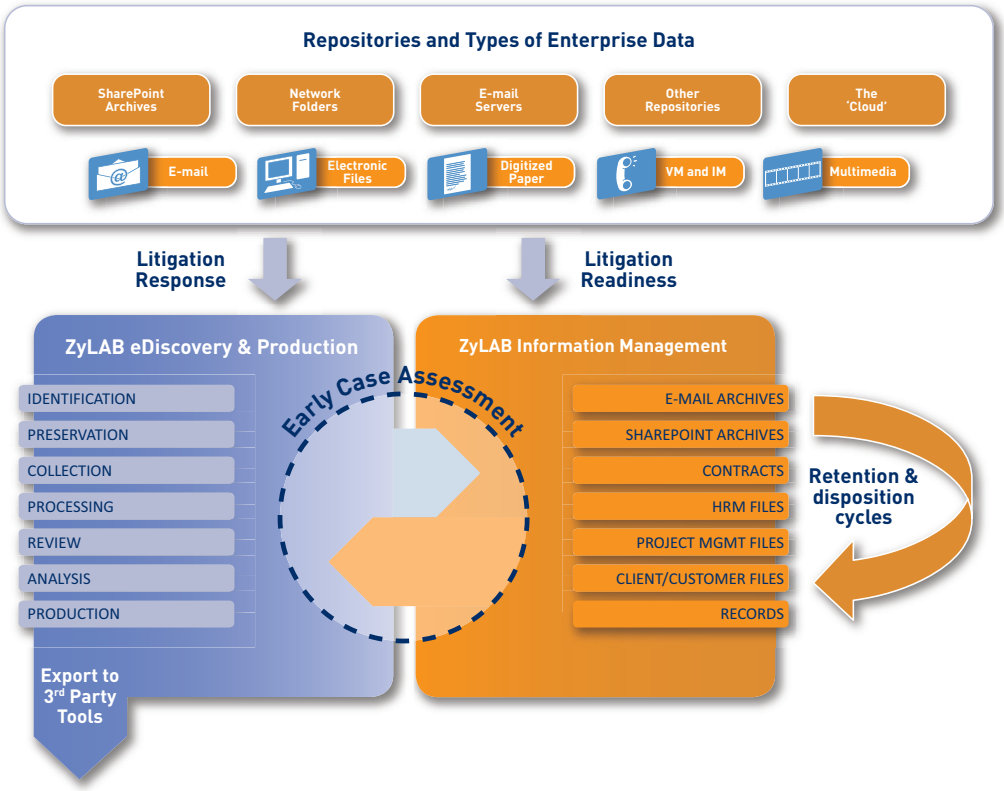

Figure 1: From Litigation Response to Litigation Readiness

ZyLAB's industry-leading, modular e-Discovery and enterprise information management technology puts you in command of boundless enterprise data in order to mitigate risk, reduce costs, investigate matters and elicit business productivity and intelligence.

ZyLAB straddles the convergence of information management and eDiscovery to keep your content assets (and liabilities) in order and to cost-effectively mine them when an investigation ensues.

About ZyLAB

ZyLAB's industry-leading, modular e-Discovery and enterprise information management solutions enable organizations to manage boundless amounts of enterprise data in any format and language, to mitigate risk, reduce costs, investigate matters and elicit business productivity and intelligence.

For nearly 30 years ZyLAB has been a dominant player in compliance and e-Discovery-related solutions, due in part to its' advanced capabilities for multi language support, searching, content analytics, document reviewing, and e-mail and records management (for both scanned and electronic documents).

While the ZyLAB eDiscovery & Production system is generally implemented to investigate a specific legal matter, it is a solid and robust foundation from which to pursue proactive, enterprise-wide objectives for information management. Those broader goals are achieved through the use of the ZyLAB Compliance & Litigation Readiness system.

The ZyLAB eDiscovery system is directly aligned with the Electronic Discovery Reference Model (EDRM) and features modules for forensic sound collection, culling, advanced e-mail conversion (Exchange and Lotus Notes) and legal review.

The company's products and services are used on an enterprise level by corporations, government agencies, courts, and law firms, as well as on specific projects for legal services, auditing, and accounting providers. ZyLAB systems are also available in a Software-as-a-Services (SaaS) model.

ZyLAB's products are extremely open and scalable, with installations managing some of the largest collections of mission-critical data in the world. The award-winning ZyLAB Information Management Platform bundles our core capabilities into a single solution that provides an optimal framework for six, specialized, all-in-one system deployments.
Currently the company has sold 1.7 million user licenses through more than 9,000 installations. All of our solutions include full installation, project management and integration services. Current customers include The White House, Amtrak and US Army OIGs, US Department of Treasury, The EPA, National Agriculture Library, and Royal Library of the Netherlands, FBI, Arkansas and Ohio state police forces, German customs police, and Danish national police, War Crimes Tribunals for Rwanda, Cambodia, and the former Yugoslavia, KPMG, PricewaterhouseCoopers, and Deloitte, Akzo Nobel, Sara Lee, Pacific Life, Siemens, Dow Automotive and Lloyds of London.

ZyLAB has received numerous industry accolades and is one of the few companies to be positioned as a Leader in Gartner's "Magic Quadrant for Information Access Technology" for 2007, 2008 and 2009. ZyLAB has received numerous industry accolades and is one of the few companies to be positioned as a Leader in Gartner's "Magic Quadrant for Information Access Technology" for 2007, 2008 and 2009. In addition, Gartner has given ZyLAB the highest rating ("Strong Positive") in its "MarketScope for E-Discovery and Litigation Support Vendors" for 2007, 2008 and 2009, as well as a "Visionary" rating in its 2011 "Magic Quadrant for E-Discovery".

ZyLAB is certified and registered as compliant with the International Standards Organization (ISO) 9001:2000. ZyLAB also lets Microsoft, Oracle and other infrastructure providers regularly certify critical components that work closely with their infrastructure. ZyLAB was certified under the US-DoD 5015.2 records management standard and ZyLAB is compliant with the European MoReq2 standard and various other regulations

Headquartered in Amsterdam, the Netherlands and McLean, Virginia, ZyLAB also serves local markets from regional offices in New York, Barcelona, Frankfurt, London, Paris, and Singapore. To learn more about ZyLAB visit www.zylab.com

www.zylab.com

ZyLAB®
eDiscovery & Information Management