Moving eDiscovery into the Enterprise
by M. E. Kabay, PhD, CISSP-ISSMP
CTO, School of Graduate Studies
Norwich University, Northfield VT

I recently received an interesting essay from a public relations officer, Dave Dix, who wrote, “In the wake of Enron, Sarbanes-Oxley, and new Civil Rules of Federal Procedure in 2006 governing standards for preserving information, eDiscovery (i.e., identifying, collecting, and processing electronic legal evidence) is turning into an ever-greater expense for many mid- and large sized companies. Unstructured information is proliferating, spending is skyrocketing, heavyweight analysts such as Gartner and Forrester are weighing in. More and more enterprises are deciding to bring eDiscovery in-house, rather than have it performed by litigation support services firms. But when they do, they'll need to assemble a careful checklist of features their solution will need to have to be effective.” He then included the following essay from Ursula Talley, who is vice president of marketing for StoredIQ <http://www.storediq.com/>, a provider of “enterprise-class Intelligent Information Management solutions that enable organizations to gain visibility and control over business-critical information in order to meet compliance, governance, and legal discovery requirements.”

The remainder of today’s column is Ms Talley’s work (with minor edits). I was particularly impressed that she does not even mention her own products!

* * *

If you work for a mid- to large-sized company—say, one with more than $500M in revenue—you are probably familiar with the problems of eDiscovery. Your enterprise may routinely face five or more litigation matters each year, and you have terabytes of unstructured information that you need to sort through in order to find relevant information and place it on litigation hold.

Worse, that unstructured information is growing dramatically: at a rate of up to 80 percent a year in many enterprises. Unmanaged and unplanned-for eDiscovery tasks increase both risk and headaches for legal, IT, and business unit organizations. Outsourcing eDiscovery to litigation services firms makes sense if you don’t have much data or rarely face litigation, but it doesn’t make good financial sense as your organization grows. That’s particularly true if you work in highly regulated and litigation-prone industries such as banking, insurance, energy, or utilities.

Here are 10 tips to choosing an eDiscovery solution that can get up and running quickly, solve the problems you need it to, and pay for itself within months.

1. Make sure your solution covers the full breadth of the eDiscovery process as defined by the industry’s EDRM (Electronic Discovery Reference Model) standard.<http://www.edrm.net> Your solution needs to cover everything from information management, identification, preservation, and collection, to processing, and early case analysis – handing over only the smallest legally defensible set of data to the legal review team. Otherwise, you’ll have to cobble together multiple solutions from multiple vendors, and create a bigger headache for yourself. Not to mention the compromised audit liability point solutions present.
2. Insist on an open integration platform that supports various e-mail systems, storage systems, archiving systems, and content and document management systems. If you're in the process of migrating data from a Novell server to an EMC Celerra or vice versa, for instance, you'll need something that can read files from both. Your solution should be able to read data from shared file servers, desktops and laptops including Macs and PCs, from content management systems such as Microsoft SharePoint and EMC Documentum, as well as from storage systems including EMC Centera, NetAPP, Hitachi and IBM.

3. Ensure that implementing your solution doesn’t reduce employee productivity. Flexible job scheduling allows processing to occur after hours, and it’s essential to be able to capture documents needed for litigation without disrupting the production environment of your knowledge workers.

4. When locking down documents for litigation, be sure your system works in conjunction with existing corporate records management policies and functions such as data backup, migration, and file expiration/deletion.

5. Be sure you can map data by system location, custodian, access time, size, and content type. It’s critical to be able to perform prediscovery profiling of data so you can manage it, know your liability, and quickly respond to legal requests.

6. Your solution will need to make available all relevant and responsive electronically stored information to legal, HR, or audit teams before the collection process finishes; the cataloging process must not make your data unavailable.

7. Your software must not alter document properties when copying or moving it, because those properties themselves are important to maintain legal defensibility.

8. Your prospective solution must be able to execute forensically sound collection policies while providing defensible and comprehensive audit logs. These audit trails show where data originally resided, what search terms were applied to collect it, and when copies were made. Attaching unique digital signatures to files before and after they are collected proves that none of the actions performed altered the original content.

9. Insist on rich and sophisticated search capabilities, including natural language concepts within files and e-mails and their attachments. Besides being able to search on common metadata and simple text strings, are you able to perform sophisticated natural language-based searches that can differentiate between “Will” (the name) and “will” (the legal document) or “will” (the auxiliary verb)? Accuracy provides the smallest legally defensible set of data to be reviewed by the legal team, significantly reducing eDiscovery time and cost.

10. Finally, be sure your solution is easy to deploy and maintain. If you have to spend weeks or months getting a system working before it can even begin accessing, categorizing, and reporting on information, you’re at a huge disadvantage. Ideally, look for a self-contained, out-of-the-box appliance combining hardware, software, and storage, that can provide results back to you within 24 hours.

Bringing eDiscovery in-house is a big step. Many organizations find that in doing it, they’re able
to save themselves hundreds of thousands of dollars, dramatically reduce the time taken to respond to legal requests, and better organize their own internal processes and data storage. But finding the right solution is key. An incomplete solution that only addresses part of your needs, and only responds to yesterday’s list of legal requirements, is bound to cause more headaches. Take the time for thorough evaluation, and make your decision carefully.

You’ll be glad you did.

* * *

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance <http://www.graduate.norwich.edu/infoassurance/> and CTO of the School of Graduate Studies at Norwich University in Northfield, VT. Mich can be reached by e-mail at <mailto:mekabay@gmail.com>; Web site at <http://www.mekabay.com/index.htm>.

Copyright © 2008 U. Talley & M. E. Kabay. All rights reserved.

Permission is hereby granted to Network World to distribute this article at will, to post it without limit on any Web site, and to republish it in any way they see fit.