

Eight Steps for Keeping Information Management and E-Discovery on Target

Homing in on information management and the records responsive to e-discovery serves the dual purpose of promoting business efficiency and legal compliance.

Randolph A. Kahn, Esq., & Diane J. Silverberg, Esq.



A financial institution embroiled in a lawsuit failed to produce all responsive information to its adversary. At trial, rather than focusing on the underlying business issues, the court focused on the institution's host of information-mismanagement snafus, which served only to magnify the issues about which the lawsuit had been filed. Indeed, under the information-mismanagement spotlight, the company's conduct appeared so bad that the jury punished it in an amount approaching \$1.5 billion – a damages award motivated largely by the company's e-discovery failings. Thus, although the company began with a relatively straightforward legal claim, with reasonable defenses and tolerable downside risk, it ended financially eviscerated, with careers in ruins and interminable bad press.

Under scrutiny, how many organizations would fare better?



For most companies involved in any significant litigation, getting the discovery of electronic information under control is like drinking from a fire hose. Billions of business messages are being sent daily and, according to the 2006 University of California study “Too Much Information,” the equivalent of 30 linear feet of books in new e-information is being generated every year for every person on the globe. It is no wonder that producing “anything and everything potentially responsive” to a document request served in the context of a lawsuit seems so daunting as to be impossible.

And, with so much information being generated by every employee daily, applying records retention rules has become a Herculean task. Compounding the difficulties of electronic records management is the fact that records retention and information preservation have become central to notions of corporate accountability and fiscal stability. This means that organizations must not only anticipate and defuse potential e-discovery

At the Core **This article**

- ▶ Describes the daunting process of getting e-discovery under control
- ▶ Stresses the importance of self-assessment for dealing with e-discovery
- ▶ Details eight steps for getting control of information and avoiding the potential pitfalls of e-discovery

ery disasters, they also must create more efficient business processes by identifying and retaining essential business record “wheat” and properly disposing of the “chaff.”

Assessing the Issues

Preparedness must begin with self-assessment. The ability to conduct a coherent, meaningful self-assessment is dependent on having a clear understanding of complex business, legal, records management, and technological issues.

To determine records management savvy and ability to withstand a court’s scrutiny, organizations should evaluate whether their records management processes and policies reflect agreement with the following statements:

1. An organization cannot keep all information it creates and receives.
2. Purging information on an *ad hoc* basis can create serious business and legal consequences.
3. Storing information is not the equivalent of managing it.
4. Locally stored electronic mail (PST or NSF) files create technology expense and pose an e-discovery challenge.
5. Information that is not readily accessible is of questionable value.
6. Information that is difficult to access can be a source of significant liability.

7. Disaster recovery is not records retention.
8. Disaster recovery tapes are not an appropriate place for retaining company records.
9. The more information an organization has, the harder it is to find what is needed, when it is needed.
10. Records responsive to discovery requests can be found in e-mail, blogs, instant messaging, or voice mail.
11. Records are different than evidence.
12. Non-records or drafts of records may otherwise need to be produced even if they did not need to be retained initially.

Organizations whose policies aren’t in alignment with these principles will have difficulties, particularly in the litigation context.

Fixing the Problem

Organizations that have not previously gone through a rigorous self evaluation and addressed shortcomings are likely to find through their self-assessments a number of problems relative to information management and potential pitfalls in the event of litigation.

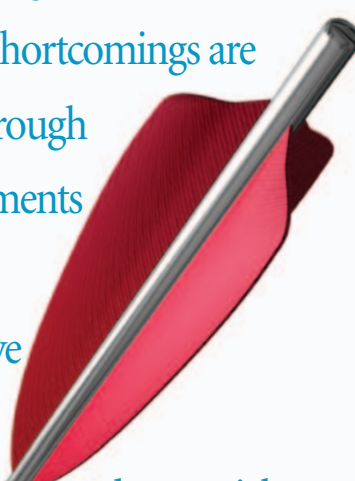
Getting under control both information management and records that are responsive to e-discovery serves the dual purpose of promoting business efficiency and legal compliance. While these arenas are interrelated, they need to be addressed in very different ways – using different staff and technology and involving different policies. Following are eight steps for addressing these challenges.

1 *Conduct a Gap Analysis to Understand the Issues*
As obvious as it may seem, an organization cannot begin to address its shortcomings until they are identified and understood. Assembling a team that represents a variety of perspectives to conduct a gap analysis will reveal the full scope of the issues.

2 *Implement Policies to Deal with Retention and Preservation*
Retention and preservation are different activities that require different policies and procedures. Rules governing *retention* provide guidance on what information should be considered a business record and how long that information needs to be retained to satisfy records retention laws, whether for regulatory purposes or to establish the organization’s business position within any applicable limitations period. *Preservation*, on the other hand, is keeping potentially relevant evidence in its unaltered form while a lawsuit is pending – or beginning when the organization reasonably anticipates that litigation may be brought against it.

Being able to demonstrate the promulgation and adherence to documented retention rules is the best means of both “cleaning house” and being able to defend credibly against claims of evidence destruction. Indeed, courts have long observed that an organization that regularly destroys records in compliance with its policies is safe against allegations of spoliation, or intentionally

Organizations that have not previously gone through a rigorous self-evaluation and addressed shortcomings are likely to find through their self-assessments a number of problems relative to information management and potential pitfalls in the event of litigation.



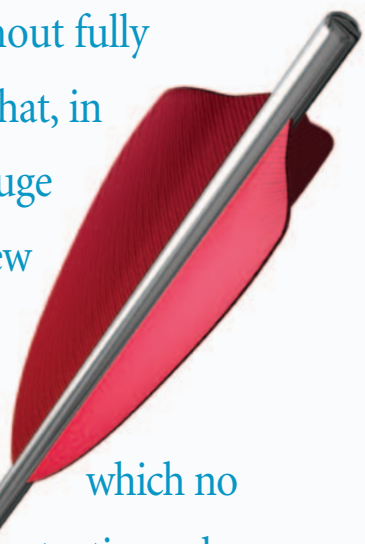
destroying information relevant to litigation. For example, the court said in *Moore v. General Motors*:

“... We see no evidence of fraud or bad faith in a corporation destroying records it is no longer required by law to keep and which are destroyed in accord with its regular practices. As we have previously observed, storage of records for big or small businesses is a costly item and destruction of records no longer required is not in and of itself evidence of spoliation.”

The *U.S. Federal Rules of Civil Procedure* (FRCP) provide a “safe harbor,” protecting a party against sanctions for failure to provide data lost “as a result of the routine, good-faith operation of an electronic information system.” However, the comments to the rule make clear that intervention is required to prevent the deletion of data that is subject to a duty to preserve it.

Furthermore, purging the contents of any system without regard for retention laws or threatened or actual discovery obligations is tantamount to disaster. In *Applied Telematics v. Sprint*, the innocent actions of a technology professional in cleaning a system to make room for more information, without regard for an existing lawsuit for which the information was needed, was viewed as destruction of evidence. Even though the court did not find the destruction to have been undertaken intentionally to prevent *Applied Telematics* from obtaining evidence, it imposed monetary sanctions.

For decades now, organizations have applied technologies to their business processes without fully appreciating that, in the process, huge volumes of new information were being created to which no retention rules were being applied.

A red feathered arrow is shown in flight, hitting a target. The target has concentric rings of blue, red, and yellow. The arrow is positioned diagonally across the page, pointing towards the bottom right.

3 *Clean up the Past – Carefully*
For decades now, organizations have applied technologies to their business processes without fully appreciating that, in the process, huge volumes of new information were being created to which no retention rules were being applied. As a result, organizations that would never allow paper copies of documents to accumulate unfettered in bankers’ boxes in warehouses now have accumulated huge volumes of largely unmanaged electronic information.

And, such electronic information can be found in virtually innumerable places, such as shared drives, local e-mail storage files, and back up tapes. Left unmanaged, these electronic records generate unnecessary human and technical expense, as well as potential risk and liability.

While the contents of shared drives, legacy systems, or e-mail servers that have gone unmanaged need to be cleaned up, employees are ill-positioned to make decisions about what records should be retained, and how, without clear directives from upper management.

Aside from the logistical challenge of determining what constitutes a record required for business or litigation purposes, is the practical challenge for employees with already-busy workloads to take on the additional job of reviewing and organizing years of stored electronic data to determine which should be considered records and what needs to be preserved for a lawsuit. While the desire simply to purge various systems of their contents is likely strong, doing so without regard for the organization’s preservation obligations or retention requirements may have major consequences – as it did in *Applied Telematics v. Sprint*.

Careful sorting of an organization’s electronic records likely will require reliance on the IT department or the assistance of companies specializing in analysis of electronic records to determine into which categories the records fall, whether they have business significance and, if so, how they need to be managed.

4 *Follow Existing Policies*
Organizations with policies in place that address the proper disposition of information should redouble their efforts to ensure they are being followed. In *Murphy Oil v. Fluor Daniel*, one party was compelled to review 20 million e-mail messages, at a cost of around \$6.2 million – and the additional expenditure of six months of time, exclusive of its attorneys’ time – because it failed to follow its recycle schedule for disaster recovery backup tapes, which properly required the tapes’ contents to be purged after 45 days. Had the company simply followed its policy, a major discovery headache and expense would have been averted. Building audit standards into information management practices is essential and can infuse credibility into the information management program.

5 *Know the Law and Understand How IT Actions Affect or Create Legal Liability*
According to FRCP 26(b)(2)(B), a litigant may not have to produce information that is “inaccessible.” At a recent executive information management risk workshop, one of the atten-

dees asked for clarification of the “inaccessibility” standard, which generally is equated with extreme cost and inconvenience. Backup tapes created for disaster recovery purposes might well be considered inaccessible, for example. The attendee learned, however, that because his IT department routinely accesses such backup tapes to retrieve records mistakenly deleted by employees, his organization would be hard pressed to argue that these tapes are inaccessible for purposes of discovery should it be sued.

Organizations that have litigation in the federal courts should map sources of information across the enterprise (an exercise strongly encouraged by the FRCP committee writers), establish an IT liaison to work with the law department on discovery issues, and implement a litigation response plan and legal hold policy.

6 Provide Needed Technology to Address Multiple Business and Legal Drivers

Failing to manage technology or to have a policy in place to inform employees about what they can and cannot do records-wise contribute to information mismanagement, the net effect of which is to make e-discovery more painful.

For example, Microsoft Outlook PST and Lotus Notes NSF files are compilations of e-mail employees may create to make their saved e-mail “transportable,” perhaps because the IT department has limited their e-mail box size or because they believe the IT department has otherwise failed to provide sufficient accessibility to needed e-mail.

PST or NSF files, then, have the practical effect of allowing employees to circumvent e-mail access limitations – and possibly to circumvent carefully drafted records management policies. Accordingly, in the event of litigation, these employees’ organization will be required to search for and through PST or NSF files on top of other sources of data storage – all at huge expense and potential exposure.

To alleviate the risk of circumvention, an organization’s e-mail policy must address alternative data storage sources directly. One way is to promulgate and enforce the proper maintenance of an employee e-mail records archive, allowing employees’ requirements for access within officially sanctioned confines.

7 Use the Right Technology for the Job

Many organizations have learned the hard way that when technology is used for something other than its intended purpose, new problems often arise. For example, many companies retain one-of-a-kind records on disaster recovery backup tapes, which is the worst possible location because it is the most difficult and expensive place in which to locate a single needed record.

Furthermore, mixing records with other content on a tape creates a retention issue because different records may have different regulatory or other business-purpose retention requirements, making disposition of the tape tricky.

Indeed, unless there is an on-going retention or preservation reason to the contrary, disaster recovery backup tapes should be kept for as brief a period as possible and for only one purpose – to bring a damaged system up immediately. There is no reason to bring up a damaged system with old data.

8 Simplify Existing Rules

The reality is that to manage information properly, most organizations have to rely on their employees. Employees, however, often balk at dealing with retention rules, arguing that they are too complex and voluminous to follow. Making retention simpler will make not only comprehension, but adherence, far more likely.

Reaping the Benefits

Following these eight steps for aligning policies and procedures with fundamental information management principles will produce dual rewards for organizations – improving their business processes and minimizing their risks in the event of litigation. ■

Randolph A. Kahn, Esq., founder of Kahn Consulting, Inc., is an educator, speaker, and author of dozens of published works including Privacy Nation, Information Nation Warrior, Information Nation: Seven Keys to Information Management Compliance and E-Mail Rules. Kahn was the recipient of ARMA International’s Britt Literary Award for the year’s best Information Management Journal article in 2004 and in 2005. He may be contacted at rkahn@kahnconsulting.com.

Diane J. Silverberg, Esq., is a principal of Kovitz Shifrin Nesbit, a general practice law firm in Buffalo Grove, Ill., where she works as one of the firm’s senior litigators. Silverberg’ 20-plus years of practice span a number of areas of business and complex litigation. In 2007, Silverberg earned the distinction of being named a “Super Lawyer” in the area of business litigation by Chicago Magazine. She may be contacted at dsilverberg@ksnlaw.com.

References

Applied Telematics v. Sprint, 1996 U.S. Dist. LEXIS 14053 (E.D. Pa., Sept. 17, 1996).

Arsenault, Amelia. “Too Much Information?” University of California (Berkeley), 2006.

Moore v. General Motors, 558 S.W.2d 720, 737 (Mo. Ct. App. 1977).

Oil v. Fluor Daniel, 2002 WL 246439 (E.D. La. 2002).

U.S. House of Representatives, The Committee on the Judiciary. *Federal Rules of Civil Procedure*. Washington, D.C.: U.S. Printing Office, 2007.