

How to Create and Implement an Information Management Policy

Mitigate potential legal risks and costs by applying clear, consistent rules to all data

Information Management Newsletters, December 12, 2011

by Tom Turner

As is invariably the case in technological advances, the many benefits of digital records are offset by significant risks. Chief among these risks is the cost of electronic discovery during litigation. E-discovery is the use of sophisticated sampling and search tools to mine databases for documents relevant to a lawsuit.



The more files there are to search, the larger a company's e-discovery costs are likely to be. Thanks to IT professionals' commitment to being excellent stewards of data, a company can have tens of thousands of backup tapes stored, each of which can contain 10 million documents – all of which may be subject to e-discovery. The result could be millions of dollars in e-discovery costs in the event of litigation.

The solution to this potential problem is obviously to store less data. But how does a company know what to keep and what to delete? If they are not careful, company executives could find themselves in serious legal trouble (perhaps accused of destroying evidence) if they delete the wrong documents. There is also the danger of deleting information that is vital to company operations.

In the face of these big unknowns, many companies simply do nothing and hope for the best. But, as the old saying goes, hope is not a strategy.

The solution is to create and thoroughly implement an information management policy that clearly lays out what kind of data should be kept and what kind should be deleted. In my experience as

continued next page

an e-discovery professional, very few companies have done this. Fortunately, I worked with a large national firm that recently spent a year designing and implementing such a policy that is working quite well.

The chief information officer of this firm agreed to freely share information regarding his company's IM policy, provided that the company's name is not used, so I'll refer to it as ABC Corp. in this article.

Step One: Take Inventory

To establish a baseline, find out how much disk space is being used to back up and archive data, how many backup tapes are stored off-site and how much data each tape contains. Don't forget paper files; most companies have thousands of boxes of files stored off-site.

Then take a sample of the data to get a rough idea of how much qualifies for transfer to the Safe Harbor folder –the area where electronic documents are kept that meet the company's criteria for retention – and how much can be deleted. If your sample is truly random, and depending on the volume of data that you have, as few as 500 documents may provide a statistically valid sample that can be extrapolated to the entire system.

Step Two: Identify the Types of Records that Must be Retained

This will vary by industry. If you are a regulated industry, like ABC Corp., regulations lay out for you that certain records must be kept for at least 10 years. In ABC's case, this included:

- Documents about how the company acquires customers, such as marketing materials.
- Documents about how well the company serves its customers, including customers' requests for services and the company's responses to these requests.
- Documents that pertain to the company's pricing practices, such as proof of the bidding process used to procure products the company needs to serve its customers.
- Financial records.

Any document that fell within these criteria was moved to the Safe Harbor folder.

For ABC Corp.'s nonregulated records, determining which records must be retained and for how long was more difficult, because it required an examination of how the company does business and what information is essential to running the business. This would be the case for nonregulated companies/industries, as well. One method for determining criteria is to convene a committee of people from throughout the organization. The criteria decided by this committee are then subject to final review and editing by company leadership.

However, nonregulated companies may find that ABC Corp.'s four criteria for document retention fit their situation, as the criteria identify the kind of data that is essential to running any successful enterprise. To summarize, these four types of documents are:

continued next page

1. Marketing plans and materials.
2. Customer service records.
3. Purchasing records.
4. Financial records.

Step Three: Appoint Records Coordinators Throughout the Company

The actual implementation of the IM policy is carried out by records coordinators at the business unit and department level. ABC Corp. currently has about 150 records coordinators, which works out to one coordinator for every 22 employees. (Interestingly, the ideal student:teacher ratio is often calculated to be somewhere between 20:1 and 25:1.)

The CIO stressed that department heads, not he or his staff, are the final arbiters on what to keep and what to delete because department heads, not the IT department, know what information is important to keep in their area of expertise. However, to prevent department heads from being overly accommodating in deciding what to keep, the CIO's team conducts periodic audits. And because the company president has made it clear that he firmly supports the IM initiative, department heads want to have a clean audit.

Step Four: Institute a Strict Email Retention Policy

At ABC Corp., the email policy is that any email not moved to the Safe Harbor folder within 90 days of its creation or receipt will be automatically deleted. No exceptions. This policy is also subject to audit.

The CIO believes this may have been the hardest part of implementing the company's IM policy, because many people are conditioned to treat their email as a to-do list. That is, they are being managed by their email instead of managing it. However, he found that it is quite possible for a large, national company to run very well under this policy. No essential information was lost, no projects were imperiled. Actually, by forcing people to deal with their email within 90 days, he believes that ABC Corp. became a more efficient company.

Again, he noted that strong support from the top was essential. The company's president was the first person to clean up his email folders by moving all messages that met the criteria for being retained into the Safe Harbor folder – and he asked all of his direct reports to do the same. Anyone who wanted to be exempted from this policy had to apply to the president. Perhaps not surprisingly, there have been no applications for exemptions.

Step Five: Kick Off and Sustain the Program with Records Retention Weeks and Periodic Audits

Each business unit and department had a deadline for cleaning up their records, which culminated in a "Records Retention Week," during which everyone in the business unit or department went through

continued next page

all data under his or her control – both electronic and paper files – and decided what to keep, archive or trash. Extra paper shredders were brought in to handle the paper files thrown away.

A notice went out weekly for four weeks in advance reminding employees that records retention week was coming and how to prepare. At the end of records retention week, the IT department conducted an audit to make sure that the process was successful. This audit is now performed annually to make sure the company does not backtrack in its commitment to maintaining well-organized records.

Step Six: Prevent Unauthorized Data Removal or Archiving

An IM policy would be meaningless if data can be removed from the audit process, which is why ABC Corp. requires that all data be saved on the company's servers, not on individual desktop computers.

There are also no USB ports, CD burners or any other data removal devices on any terminal. All of the data that employees work with resides on the company's servers. A secure mobile access system allows them to access their data from anywhere, anytime, so they can work off-site or after hours with complete access to all of their files if the situation requires it.

Reasons to Have an Information Management Policy

Reduce IT Costs

Because the vast majority of information produced today is stored digitally and because the use of email has exploded, the need for computer disk space has expanded exponentially. The purpose of an IM policy is to reduce the amount of data that is kept in the system, which naturally leads to a reduction in the expenditures for electronic storage, or at least, a reduction in the rate at which storage costs are rising.

Reduce Risk

Continually adhering to an established system and process can shield a company from exposure. If sued, having an IM policy in place can help you withstand a claim that you deliberately destroyed only potentially harmful data – since the same rules apply to all data.

ABC Corp. has very clear rules for what to keep and what to delete. That is, company management can clearly articulate reasons for keeping any document that are based on regulatory or business requirements. This is by no means about hiding "smoking gun" type information. If there is a document that adversely affects the company but falls within its criteria for keeping it as long as 10 years, then it will be in the Safe Harbor folder.

Having this program in place has prevented ABC Corp. from needing to put enormous legal holds in place because the company is ready to prove to a court that any document that might be responsive to a case is in its Safe Harbor folder and nowhere else. So there is no need to put a legal hold on data that might exist outside of the Safe Harbor.

continued next page

Reduce E-discovery Costs

If there is less data to feed into the e-discovery process, the cost of e-discovery should be correspondingly lower. It's that simple.

Increase Productivity

Because it forces you to categorize data, an IM policy leads to better organized data on the front end, reducing the lost productivity that results from searching for data in a disorganized system and yielding better product outcomes. It's the old IT adage: "Garbage in, garbage out."

Tom Turner is president and founding partner of Document Solutions Inc., a litigation support company providing e-discovery and digital forensics services as well as traditional litigation support. Tom is a certified e-discovery specialist with more than a decade in the industry.