

Implementing an information governance program

by Clinton Field

The amount of electronically stored information generated and stored by organizations, including law firms, companies and non-profits, has grown enormously over the past several decades.

Recent studies estimate that the global volume of data doubles every two years. While the costs of digital storage have dropped significantly over this period, maintaining vast quantities of data has repercussions for litigation, and raises risks for information security and privacy. In order to mitigate these risks, organizations have focused on ways to sensibly reduce the volume of data they maintain with the implementation of an information governance program.

Preparation

The first critical step in implementing an information governance program is the identification of the kinds of information that need to be retained by the organization. Three primary factors drive the retention of records and information: operational needs; regulatory requirements; and litigation holds/preservation orders due to litigation, audit or investigation. The first two factors, although potentially complex, are usually able to be clearly delineated by members of the organization.

Operational needs can be gleaned directly from interviews or questionnaires directed to key business departments, or indirectly due to the lack of access activity for a particular system. Regulatory requirements are enforced by an organization's compliance officers or in-house counsel, and organizations in highly regulated environments will generally have sophisticated management systems for the records they are required to maintain.

Data that is subject to litigation hold can pose greater challenges. At a minimum, organizations should have a well-managed, established litigation hold process in place. Whatever form this process takes, it needs to produce three important results, including a centralized listing of individuals under active litigation hold; ongoing notices to information governance procedures regarding new matters and their preservation requirements; and preservation of the information subject to the litigation hold.

Understanding Data Repositories

Once a comprehensive and mature litigation hold process has been implemented, it is possible to move forward with an information governance

program without generating an unreasonable amount of risk. Before starting such a process, however, it is important to identify the individuals who will be implementing and managing the program. Support from the organization's leadership is necessary at the outset, both to assign the needed resources to the program and to ensure that progress is being made and appropriately tracked.

Participants from the legal and compliance groups should be involved to identify the retention requirements. Information technology professionals are also critical participants and should be primarily responsible for the next steps in implementing an information governance program. Those next steps include identifying and describing data repositories that are being used by the organization.

One thing to make clear to IT participants is that this identification process should be much broader than simply a network diagram (and that a network diagram would include levels of detail that are unnecessary for this analysis). While identifying the servers and their locations is a good start, it is important also to determine how these servers are being used. Are they file servers hosting unstructured data or databases functioning as the back-end for applications? Are there additional servers which are not currently being used, but still host legacy data? How are back-ups being performed and does the back-up process produce a large volume of unnecessary data? And how much information is being stored outside the organization's network, either in cloud-based file storage or within the databases of third-party, web-based applications?

Not all of this information will necessarily be known by the IT department, particularly in organizations where there are a significant number of users who administer their own third-party software tools, such as ADP for HR. Even within the IT department itself, there may be separation between the individuals responsible for infrastructure administration and those who are responsible for managing back-end databases for internally-developed applications, such as a customer relationship management database with custom analytics. In order to capture this information about potential data sources effectively, it is usually necessary to either conduct formal surveys and, if practical, meet or interview key departments and responsible IT personnel for the organization.

Reasonableness and Prioritizing Efforts for Data Retention and Destruction

Once all of this information has been gathered, it may initially seem that there is an overwhelming number of possible data repositories to be managed by the organization. However, it is not necessary to focus on every data store at one time or to institute immediately an organization-wide information governance program.

One of the Sedona Conference's basic principles for managing records and information is that the "hallmark of an organization's information and records management policies should be reasonableness." Part of the information to be gathered about an organization's data should be relative sizes and frequency of use.

Another factor can be addressed by the legal department or outside counsel. Which of these data sources is the riskiest in terms of litigation exposure or other risks? Which has historically produced the largest volume of discoverable data, driving collection, processing, review and production costs? Answering these questions will help to identify the areas where information governance policies and procedures will produce the greatest return on investment, thereby reducing the organization's risks and costs associated with unnecessarily retaining large volumes of data.

Focusing on Email

For many organizations, email will be an area of immediate concern. The sheer volume of email generated by an organization and the lack of formality in emails makes it a primary focus of information governance initiatives, especially given the potential for careless communications to be taken out of context, if disclosed in litigation or to the public at large as in the Sony hacking incident.

Complicating the matter, though, is the wide variety of ways in which email is used. Different organizations may use email more or less frequently to communicate as opposed to phone calls or face-to-face meetings, and may also have different cultures regarding formality of email communications. Different individuals may also have varying practices in how they manage their email. Some might keep messages in a highly structured folder system, others might keep everything unsorted in their inbox and rely on searches to find what they need, and some users may delete most messages fairly quickly or even save them to another location. Although it is not possible to take every user's preferences into account when managing email, it is important to remember that changes to email policy must be clear and well communicated to avoid disrupting individual workflows.

The simplest form of email management is a time-based deletion protocol, where messages older than a certain fixed period are deleted automatically. The time period that is chosen depends heavily on the organization's need to refer to previous communications. Are there

communications with outside parties which need to be referred to months afterwards? Or is a period of several weeks sufficient? Whatever time period is chosen, the process can usually be set up directly within the email environment, and can also be set as a two-stage deletion process where messages are moved to a separate folder where they can be examined and possibly saved by users before being permanently deleted.

Exemptions and Email Archives

Of course, this brings up the question of where users can save email that they want (or need) to keep for a longer period of time. Non-inbox folders can be used for keeping messages for a longer period of time, for example, or client communications can be kept indefinitely within a central network location. There may even be certain individuals or departments (such as legal, insurance, or real estate) that are exempt from the deletion process. Whatever decisions are made in this regard, it is important for consistency and defensibility of the process that written policies are drafted and disseminated to accurately reflect the procedures taking place, and that any exemptions or changes are diligently tracked. Also, the litigation hold process must be directly tied to email deletion procedures to ensure that relevant documents are not inadvertently lost.

Another potential challenge is archived information, which might not even exist within the active mail environment. When using Outlook, for example, this can take the form of PST files, which are personal mail folders that may reside on either local computers or on network storage outside of the exchange environment. Remediation of PSTs and other externally stored email can be done in a variety of methods – using software tools, by re-ingestion into the active environment, or by direct deletion – which depend greatly on the size, location, and organization of these archives.

Summary

With executive support, a team responsible for information governance can investigate current data repositories and retention practices, and construct a reasonable, well-documented procedure which is then clearly communicated to the organization as a whole. Finally, the legal and compliance teams must be involved at every step to ensure that no regulatory retention requirements are being violated, and that the litigation hold process promptly provides information about the specific preservation requirements of new litigation matters which arise. When these ingredients come together, you are able to take the first steps in building an auditable, defensible information governance program. ■

About the Author: Clinton Field is a solutions architect for bit-x-bit LLC, and consults with corporate clients on the technical considerations for computer and technology use policies, implementation of appropriate information governance programs and litigation holds.

ALIGNED PARTNERS



“Success is Simple.”

Do what's right, the right way, at the right time.”

—Arnold Glasow

Put Your Trust in Us

707 Grant Street
2800 Gulf Tower
Pittsburgh, PA 15219

www.alignedpartners.com

412-258-3590

ALIGNED PARTNERS

Trust Company

Allegheny County Bar Association
Raising the Bar on Legal and Community Service

www.acba.org