

What CIOs Should Know About Records

IT has proven its strategic value as a conduit for attaining business objectives and sustaining growth. Has IT also unwittingly assumed the risk associated with enterprise information?

By Julie Gable

The sheer chaos of electronic records makes them high risk, and the probability of consequences is high. Well-respected companies have been scandalized by errant e-mails or fortuitous file clean ups. The resulting reputational damage, and its negative effect on stock value, riles shareholders, rocks the boardroom, and has repercussions throughout the C suite.

Electronic records pose an enterprise risk that is pervasive, affecting operations in every line of business. Possible exposures include legal discovery, regulatory inspections, industry investigations, and privacy rule violations. In each instance, proof of guilt or innocence resides in records made and maintained using information technology. (See sidebar: The Rules of the Game.)

CIOs, as the guardians of corporate data processes, find themselves adding records management to their list of expanding responsibilities. According to a survey commissioned by ARMA International and conducted by Forrester Consulting, CIOs and IT organizations are routinely tapped to provide solutions to compliance, legal, and regulatory challenges involving electronic records. Although responsibility for implementing records control is usually delegated many levels below the CIO, its oversight and effectiveness are not. Here, then, are 10 things CIOs should know about managing electronic records:

1. Managing e-records is about control, not access. Basic control elements are the ability to identify a record, attach a retention rule, keep the record unalterable for as long as required, enforce the retention rule through reliable destruction, and, alternatively, suspend destruction if investigation or litigation is pending or imminent. Retrofitting control to systems designed for information access is difficult and imposing requirements on users is not popular.
2. Policy infrastructure is key. Managing e-records requires corporate policies, consistent retention rules, defined procedures, employee training, and audit capability. This programmatic approach to keeping and eliminating records in the ordinary course of business assures that records needed as evidence are preserved. It also demonstrates an expectation of consistency, responsibility and accountability that has a better chance of standing up to outside challenges.
3. Clout is important for practical and political reasons. Effective records management requires a mandate from the highest levels. Thanks to Sarbanes-Oxley, executives are now personally

accountable for governance lapses, facing jail, sanctions and out-of-pocket settlement payments, so obtaining buy-in is not difficult. Beyond this, most companies put three levels of structure in place:

- an oversight committee of legal, compliance, tax, and corporate management executives who sign off on all policies and rules.
- a records council – consisting of IT, legal, compliance, finance, records management, and human resources – that develops the policy infrastructure, obtains oversight committee approval and recommends changes over time
- a liaison group of process and system owners responsible for day-to-day activities regarding electronic records

4. Investing in technology without thinking through the details is a waste. Technology tools for records don't come with pre-written policies or rules. In order to work at all, solutions must be fine-tuned to the company's internal nuances, for example, which rendition – PDF, Word file, scanned image – is the record? Are all drafts also records or only the final, approved document? The answers require input from process owners and users, not IT.
5. Content determines value, not the transport mechanism. E-mail is one aspect of overall records management, not a separate issue. Generally, the value of messages and attachments depends on their content, and content determines what retention rules apply. Rules based on controlling e-mail storage volume – for example, retaining all messages for 60 days – are problematic because they assume all e-mail is created equal, which it isn't. Products that don't differentiate e-mail by content work well if all messages fit one content category such as customer correspondence in financial services businesses, but such products are not effective in cases where e-mails vary greatly in content and in record value.
6. Records management needs influence ILM decisions. ILM matches storage media with information activity level, age, volume, or other criteria so that older, less active data is stored in cheaper ways. RM's emphasis is on enforcing information management policy, regardless of how the records are stored. The need to preserve certain records long term for retention or legal purposes will factor into storage selection, upgrade and migration decisions.

The Rules of the Game

Unlike corporate knowledge or business intelligence, electronic records are evidence. They accrue to business processes, show what transpired during transactions, confirm rights and obligations, and provide motive for corporate action.

Legal adversaries, regulatory inspectors, and industry investigators can and do use your records to build their case. Some basic facts:

- If you have the requested information, you must produce it, even if you could have or should have destroyed it. This implies knowing what to keep for how long based on industry-specific regulations, federal, state and local laws, compliance requirements, and operational needs.
- Those examining your records must be satisfied that information practices are consistent and take place in the due course of business. Companies must show proof that there is a program in place governing information handling from creation to disposition, and that all employees follow the program.
- To use your own records in defense, you must be able to show that systems responsible for creating, managing and storing them work reliably, produce accurate, authentic records and prevent intentional or inadvertent alteration.
- You can't destroy information that will be needed if a lawsuit or investigation is pending or imminent. There must be ways to suspend ordinary destruction and make sure that needed information is not accidentally erased or overwritten.
- Protecting information from outside eyes by claiming attorney-client privilege must be corroborated by processes that don't allow proprietary information to circulate outside the company.

7. Distinguishing between e-records archives and backups is smart strategy. An archive is a repository that provides secure retention of e-records for compliance and operational purposes. Many companies don't have electronic archives, so attorneys and others go to backup tapes as rich sources of discoverable information. Service costs average about \$250 per backup tape to find, read and process material relevant to discovery requests, and it's common to find thousands of tapes in companies where no retention rules have been implemented or followed. Pending changes to the Federal Rules of Civil Procedure could limit legal discovery to records kept in archives. If the

FRCP changes take effect, adversaries that want backups would have to demonstrate why and share costs associated with producing them.

8. Risk mitigation costs money. The biggest investment is time required to develop or revise policy infrastructure. Consulting rates vary from \$100 to more than \$300 per hour depending on the expertise desired. Hiring an in-house records manager may be more cost effective. Other out-of-pocket costs involve technology purchase, integration and implementation. Records management software costs about \$250 to \$800 per seat, and \$25,000 and up per server. E-mail management solutions are \$60,000 per server and up. Most enterprise content management products have acquired records management capabilities. The offset is cost avoidance. A DuPont study over five years found that half of all materials reviewed for discovery were past retention and could have been safely destroyed under a records program. But because they weren't, and were discoverable, the company spent \$11 million more than necessary responding to discovery requests.
9. Global firms control records policy centrally but implement locally. Best practices are to set corporate policy, provide templates and establish adequacy standards for retention rules, procedures and training. Individual locations formulate their own ways to implement and comply with corporate policy. The result is consistency of approach but ample customization to accommodate local requirements.
10. Build records control into process and system design. Manual intervention does not work. Users will spend 15 seconds or less puzzling through manual classification hierarchies for e-records and will blithely choose defaults wherever possible. It's better to rely on records control methods that use meta data, auto-classification techniques or structured workflows in cases where records can be pre-defined.

Without question, information management is a high stakes game. The paper trail is now digital, and its first stop is the CIO's office. Managing e-records risk pro-actively makes sense for business entities and the CIOs who routinely lead people, processes and technology in strategic enterprise efforts.

(A version of this article appeared on *SearchCIO.com* in April 2005)

Julie Gable is Principal of Gable Consulting and Associate Executive Editor of the Information Management Journal, a publication of ARMA International (www.arma.org). Reach her at juliegable@verizon.net.