White Paper

Stop Hoarding Electronic Documents

Go from "Save Everything" to "Save Smart"

Sponsored by: OPENTEXT

Abstract

Companies that lack a sound information governance strategy often save too much information. This paper discusses why "saving everything" is both an organizational and individual problem and outlines the keys to success in building a program to combat information hoarding.

Disclaimer

Contoural provides information regarding business, compliance and litigation trends and issues for educational and planning purposes. However, legal information is not the same as legal advice – the application of law to an individual's or organization's specific circumstances. Contoural and its consultants do not provide legal advice. Organizations should consult with competent legal counsel for professional assurance that our information, and any interpretation of it, is appropriate to each organization's particular situation.

Table of Contents

Introduction

Hoarding of electronic information is a common problem that reduces employee productivity, raises IT operational expenses and heightens the risks and costs of regulatory action and litigation. Organizations need to assert centralized control of deletion in order to overcome the consequences of information hoarding. But such efforts can run into resistance from employees.

Changing from "save everything" to "save smart" can be achieved with effective policies that accommodate employees' work habits. Everyone has a role to play in reducing the over-retention of information, and there's a "win" for all participants.

Understanding the "Save Everything" Culture

Most organizations let information pile up. New information is like snow and legacy collections of data are like glaciers: each year, layers are added, some melt away, but the accumulation keeps growing.

- The size of the digital universe in 2012 is estimated at 2.7 zettabytes (2.7 trillion gigabytes), and is forecast to be 40 zettabytes by 2020 – a 50-fold growth since the beginning of 2010 (source: IDC).
- Businesses sent and received 89 billion emails per day in 2012, which should grow to over 143 billion by year-end 2016 (source: Radicati Group).
- Unstructured data (files, office productivity documents, SharePoint and other information generated by applications) in the enterprise is growing at up to an 80 percent rate (source: Gartner).

Many IT departments have found that just devoting more storage to the problem is at best a temporary fix. It is true that the acquisition cost – but not the operating cost – of storage is trending downward. And "the cloud" offers manageable costs and virtually unlimited capacity. Still, as the volume of information grows – and content repositories and management systems proliferate – problems crop up. Queries and searches can take longer, confidential data can fall into the wrong hands, and considerable effort may required to respond to eDiscovery requests or regulatory challenges.

The Downside of Aggressive Deletion

Some IT departments react to the growth of information by aggressively deleting it according to established rules. For example, if files have not been accessed, classified or changed for some period of time (e.g., 60 days) then the information is deemed to have little or no business value and is automatically deleted. The rationalizations for such behavior are threefold:

- Storage space can be freed up.

- Information is expunged before the organization finds itself in trouble, and as long as deletion policies are documented, the organization can feel confident if it is challenged in court.
- All employees – from the CEO on down – are (*or ought to be*) aware of the policies so there should not be any surprises.

The trouble with this strategy is that the IT department cannot be certain that everything is truly deleted. Information tends to have a long lifecycle, especially when

- The recycling of offsite backup tapes does not match the aggressive deletion schedule.
- Employees can forward email messages and attachments to colleagues or send blind copies to their personal email addresses (e.g., gmail).
- Files can be saved on USB drives, laptop storage, and at remote office locations, in cloud-based applications like Salesforce.com® or Google Drive, or burned to DVD by employees on their home systems.

The last two scenarios are examples of what we call "underground archiving:" individuals maintain private repositories of documents, keeping information outside of the control of the organization. Underground archiving is often a reaction to the imposition of storage quotas or enforcement of harsh deletion rules; people will squirrel away what *they* deem to be important. We find that about 30 percent of Fortune 500 companies we've spoken with are plagued by information that practically lives forever in underground archives. Such data and documents are discoverable, and the costs of identifying it and recovering it can be onerous.

Why Hoarding is an End-User Problem

Some people are "filers:" they classify information (most often manually), and rely on folder-based navigation to find what they need. Other people are "pilers" – they save all of their documents on the desktop, the email inbox or wherever they originally reside, delete almost nothing and rely on search to find important information. "Deleters" get rid of information as soon as it's determined to be of no use to them.

We find that over 50 percent of employees in organizations of all sizes are pilers. A somewhat smaller percentage are filers, and from 5 to 10 percent are deleters. Pilers tend to drive filers crazy (and vice versa), but most sensible organizations don't enforce uniformity. People are people and they'll work in the way that promotes productivity and comfort.

Some employees have sinister reasons for keeping or deleting documents – to cover their tracks, to help them avoid retribution or to preserve information that may be used against others. And deleters can cause problems because they might permanently remove information that has business value or should be retained for legal or regulatory purposes. But most filers, pilers and deleters have good intentions and believe that what they save has business value and/or is tied to a

business process. If they're wrong, their behavior – in addition to making themselves less productive – can drive up storage and management costs and the risk and expense of eDiscovery.

Obstacles to Defensible Deletion

Some organizations have adopted policies for "defensible deletion" that allow them to dispose of information that has no business value. Such policies demonstrate that reasonable steps are in place to protect the information and the organization itself. Courts have held that such policies must be routine, transparent, carried out in good faith and consistently applied. Defensible deletion means that

- Deletion decisions can be readily understood and explained to non-IT and non-records professionals.
- The organization has some level of protection against litigants and regulators who, in the future, may ask uncomfortable questions about why specific documents have been deleted.
- The removal of unneeded information that would otherwise drive up cost and increase the risks of eDiscovery can be justified.

But even though defensible deletion policies may be in place that are "…designed, programmed, and implemented to meet the party's technical and business needs…" (FRCP Rule 37(e)), the behavior – or misbehavior – of employees can run counter to the goals of the organization.

To prevent hoarding, organizations must establish programs to align the behavior of end-users with enterprise-wide defensible deletion policies. And by "alignment" we don't mean that the activities of pilers, filers and deleters must be curtailed; that probably won't happen in any case! Rather, they must understand "what's in it for them" so that their behavior can fit within the organization-wide guidelines and procedures.

Stop Hoarding – The Keys to Success

Centralized control of deletion – as an element of a broader "information governance" program – is needed so that organizations can overcome the consequences of information hoarding. But making it happen is often easier said than done.

We encounter many customers who believe that they know just how to implement an information governance program. By analogy, when "information technology" initiatives such as ERP are introduced, a significant amount of effort surrounds system deployment: what happens when a new tool is moved into production, what are the effects on infrastructure, process and user experience.

The objective of an "information governance" program, on the other hand, is to modify user and organizational behavior. Chances are that new software and tools are required, but at least as much energy must be expended on policy and process

development, articulating the benefits for the company and employees, monitoring and auditing of ongoing behavior, and, in some cases, developing customized approaches for separate audiences.

Organizational Willpower

We recommend that a cross-functional team be formed to oversee an information governance project. It would include representatives from the records and information management (RIM), legal and IT departments, as well as executives and end-users. Once each group understands the severity of the issues at hand and the "win" that's in it for them, they'll be more willing to participate or at least to not sabotage the effort.

Know What You Have

Start by creating an information "map." Automated tools can help, but some manual effort will be required to determine the location and the value of information. Employees make great use of unstructured data (email, SharePoint, files, etc.) in daily work and in business processes. Such information is often hidden in underground archives, so be sure to include the data that reside on employees' laptops, tablets, smartphones and workstations as well as in production systems. All of it carries potential for exposure to regulatory, legal or eDiscovery risk and the associated costs.

Current Document Retention and Deletion Policies

Up-to-date retention schedules specify just how long information should be retained. Early in the process, strive for agreement among the cross-functional team members about retention and deletion rules. Be sure that policies identify processes and the "authority" (for example, a legal ruling, business practice or regulatory mandate) which justifies retaining and deleting documents.

Consistent Legal Hold Policies and Processes

The deletion process is often complicated by ongoing litigation and lack of a process for identifying which data are and are not under legal hold. Create a clear and consistent legal hold process that clearly delineates data being held, prevents the purging of data that by policy might otherwise be deleted, and allows the routine deletion of data not under hold. The more clear and unambiguous a legal hold process is, often the more aggressively older, non-relevant data can be deleted.

Records Management

Organizations are often reluctant to engage in deletion knowing that some of the data contain records which must be retained for a period of time to satisfy regulatory or legal requirements. We refer to these as "Records" – with a capital "R." Another category is "records" – with a lower-case "r" – information that has business value but for which there is no external mandate to keep, and "transitory information,"

which is everything else. We recommend that RIM professionals take the lead in guiding the definition, identification and classification of “big R,” “little r” and transitory information, with policies and procedures embodied in a records archiving program.

A common mistake we see is that such programs can be focused too narrowly, often solely on the “big R” records. Other parts of the organization may see value in content beyond big R. The value of a cross-functional team to decide on priorities and resolve conflicts is obvious.

Keep It Simple for End-Users

Our surveys indicate that without clear direction, more than 90 percent of employees tend to save more documents than they need. Their reasoning is no one ever got in trouble for not deleting a document. On the other hand, given clear guidance we have found that 80 percent of employees will follow a reasonable, intuitive policy.

Pilers, filers and deleters all have different views on what is “reasonable and intuitive.” People’s natural tendencies are hard to change, but it can be made easy – or at least *not difficult* – for them to participate in an organization-wide program. Studies show that the typical accuracy of employee decisions on classification and deletion varies tremendously – from 20 to 80 percent. To improve the results, don't burden employees. Use a departmental or level-specific file plan (a subset of the document retention schedule) to communicate the categories and which documents need to be saved in them. Keep it simple and straightforward by offering only a few choices of retention periods. Finally, ensure that the retention schedule takes business value into account. Otherwise employees will save documents in underground archives. Keeping documents within control of the record retention program – and having employees willingly participate – enables much easier deletion later when the documents are not needed.

Apply Psychology – and Technology

Help employees accept and embrace changes to their current working environment. While introducing the program:

- Provide options – let employees make decisions within the boundaries of policy.
- Keep documents accessible; merely the perception of “taking information away” encourages underground archiving.
- Programatically control deletion. Most users are filers and pilers; if regulatory compliance is important, don’t rely on them to delete information on their own.
- Strive for invisibility – nobody is any the worse off if information is deleted without end-user intervention…within the rules, of course!

Of course, technology plays an important role in an effective program to stop hoarding. The best approaches enable consistent policy governance across all repositories and reflect – rather than challenge – the way people work. For example:

- Data and file intelligence applications search for and index information across multiple repositories and endpoint storage devices without moving it from its native location. They provide insight into information that could cause eDiscovery exposure.
- Federated information management solutions go further than data and intelligence applications. They build a "master" location for storing metadata and index information and typically offer a central console or a "single pane of glass" through which IT and business unit managers can *take action* to define and modify policies for retention, deletion and security against data.
- Autoclassification software has recently made significant advances in accuracy. It can be useful for categorizing large accumulations of legacy data and is helpful in augmenting manual classification and deletion decisions.
- On-premise or cloud-based archival software diminishes the perceived need for underground archiving by keeping information accessible and retrievable without IT intervention.

Not everything must be done all at once. Certain collections of unstructured and semi-structured electronic information – SharePoint, files, and documents, email – may require near-term attention because of urgent eDiscovery or regulatory pressure. It's acceptable to attack the problem in phases; just have a technology roadmap in mind.

Auditing and Monitoring

Once the elements of an information governance program are in place, frequent evaluation and oversight are critical. Look for gaps between policy and practice. For example:

- Are employees lazy, classifying information only according to the longest retention period?
- Is information still hidden in private repositories?
- Is there too much emphasis on properly managing "big R" records to the detriment of other valuable documents?

Focus on employees that are not following the policies as the exception and not the rule. Going from a "big" problem, where hoarding is rampant and deletion is hardly defensible, to one where just a fraction of users still require some level of behavior modification is a big win for most organizations. Don't let "perfect" be the enemy of "good enough."

Conclusion

The unprecedented growth of electronically-stored information has consequences. Organizations of all sizes should implement policies to thwart the intentional and inadvertent over-retention of data. Changing behavior to prevent hoarding requires

a good measure of organizational fortitude, innovative technologies and accommodation for employees' work habits. With these – and a sound information governance strategy – organizations can realize the benefits of centralized and defensible control of deletion.

About OpenText

OpenText provides Enterprise Information Management software that enables companies of all sizes and industries to manage, secure and leverage their unstructured business information, either in their data center or in the cloud. Over 50,000 companies already use OpenText solutions to unleash the power of their information. To learn more about OpenText (NASDAQ: OTEX; TSX: OTC), please visit: www.opentext.com.

About Contoural, Inc.

Contoural is a leading independent provider of business and technology consulting services focused on litigation readiness, compliance, information and records management, and data retention strategy. Contoural's clients include more than 15% of the Fortune 500, as well as many small and mid-sized industries across the U.S., with engagements throughout the world. The company sells no products and takes no referral fees, offering clients truly independent advice. Contoural believes that creating a consensus across a client's organization is a cornerstone to an effective strategy. The company's services encompass all electronically stored information (ESI), including email, as well as paper documents.

With an average of 14 years industry experience, Contoural's team is comprised of attorneys, former compliance officers and records managers who have a deep understanding of the legal, compliance and business requirements for retaining and managing information -- as well as seasoned IT professionals with expertise in document archiving, search, litigation management systems, data classification and data storage, all focused on effective program execution.

Contoural services include:

- Assessment and Roadmap Development Services
- Records and Information Management Policy Development Services
- Data Classification Services
- Autoclassification Process Development
- Litigation Readiness Services
- Solution Design, Technology Evaluation and Vendor Selection Services
- Solution Implementation Services
- Ongoing Program Management Services

With these services, Contoural helps enterprises ensure compliance and reduce risk, while also achieving litigation readiness and reducing costs.

Contoural, Inc.
5150 El Camino Real Ste D30
Los Altos, CA 94022
650-390-0800
www.Contoural.com
info@contoural.com