ACC Guide℠

How to Delete Emails and Files Quickly and Defensibly

Sponsored by:

Association of Corporate Counsel
1001 G Street, NW, Suite 300W
Washington, DC 20001
tel +1 202.293.4103, **fax** +1 202.293.4701
www.acc.com

How to Delete Emails and Files Quickly and Defensibly

October 2022

Provided by the Association of Corporate Counsel (ACC)
1001 G Street NW, Suite 300W
Washington, DC 20001 USA
tel +1 202.293.4103
fax +1 202.293.4107
www.acc.com

This ACC Guide℠ addresses How to Delete Emails and Files Quickly and Defensibly. It is intended for in-house counsel or other team members tasked with deleting older emails and files that are expired records or non-records with low business value, as well as ensuring that moving forward this electronic information does not needlessly accumulate. This Guide details why letting electronic information accumulate can be hurtful, and why deleting it can be difficult. It reviews several deletion approaches that are ineffective and highlights those approaches that work well. These smart strategies will enable companies to create effective programs that ensure compliance, reduce risk, lower costs, and increase productivity.

This material was developed by Contoural, Inc. Contoural is a sponsor of the ACC Information Governance Network and of the ACC Legal Operations Network Records Management and Information Governance Foundational Toolkit. For more information about the author, visit their website at www.contoural.com or see the "About the Company" section of this document.

Contoural and ACC wish to thank members of the Information Governance Network for their support in the development of this Guide.

The information in this ACC Guide should not be construed as legal advice or legal opinion on specific facts and should not be considered representative of the views of the Association of Corporate Counsel (ACC) or any of its lawyers, unless so stated. This ACC Guide is not intended as a definitive statement on the subject, but rather to serve as a resource providing practical information to the reader.

Table of Contents

I. Introduction 4
II. Saving Too Many Emails and Files Is Bad 5
A. Email and File Over-retention Costs 5
B. Over Retention Hinders Privacy Compliance 6
C. Hidden Cost of Hoarding – Impact on Employee Productivity and Collaboration 6
III. Defensibly Deleting Emails and Files is Hard 7
A. Many Layers of Buried Information 7
B. Employee Hoarding 8
C. Everybody's Job and Nobody's Job 8
IV. Email and File Deletion Strategies that Don't Work 9
A. Employee Manual Processes Don't Work 9
B. Aggressive Deletion Doesn't Work 11
C. Monolithic Retention and Deletion Doesn't Work 12
D. Standalone Content Analytics Doesn't Really Work 13
V. Deletion Strategies That Do Work 15
A. Implementing the Five Second Rule with Drag and Drop 16
B. When It's Time to Delete a Record, Let Systems Do It Automatically 18
C. Deleting Emails and Files When You Move to the Cloud 19
D. Creating a Working Documents Area 20
E. Implementing Employee Behavior Change Management 21
VI. Creating Your Plan 24
A. Critical Components to Have in Place Before You Start 24
B. Create a Plan for Fastest Disposition 25
C. Reasonable Disposition Targets 26
D. The Hidden Blocker – Legal 27
VII. Final Thoughts 27
VIII. About the Author 28
IX. About Contoural 28
X. Additional Resources 29

I. Introduction

Emails and files are the lifeblood of an organization. These media serve as primary communication and decision-making tools, record decisions, facilitate processes, and allow employees to communicate. According to an article in DMR, it has been estimated that the average employee receives approximately 121 emails per day. Employees can create, modify and view more than two dozen files per day. As employees increasingly work in hybrid offices and work-from-home environments and are not physically situated near one another, these modern communication tools have become even more important for ensuring the ongoing operations of a company.

Yet emails and files can also become too much of a good thing. The persistent, ongoing accumulation of this electronic information spawns a new set of risks and challenges. The pain of over accumulation may only become apparent during a large e-discovery exercise. Or when companies seek to be compliant with privacy requirements. Sometimes the impact is counter-intuitive, such as having too much information to an extent that lowers employee productivity and effectiveness. Companies are realizing that these are real risks creating real problems, and this over-accumulation needs to be dealt with.

Deleting emails and files in a defensible manner can be difficult. Sorting through large volumes determining what to save and not save can be time-consuming. Likewise, adopting large-scale deletion can quickly run into employee and business unit push back. Deletion exercises quickly become overloaded with emotions, both from those trying to delete as well as from employees resisting the actions. Sometimes efforts to delete backfire and drive accumulation of emails and files into unsanctioned storage areas. Frustration builds. Many simply give up.

Do not give up. There are proven strategies used by many organizations to tame their growing piles of accumulating emails and files. While there is no magic formula, taking a smart, real-world approach, combining policies, process and the appropriate use of technology can enable organizations to save the right information for the right length of time and make it more accessible, while at the same time deleting and not letting low-value, unneeded information accumulate.

Companies are doing this, and it works – without having to get into a conflict with document-hoarding employees and business units. While these programs often start to drive compliance or reduce costs, many find a hidden win in that cleaning up the clutter helps their employees work in a better, more collaborative, smarter way.

II. Saving Too Many Emails and Files Is Bad

While email is an indispensable component of running most business, and the use of files is a cornerstone of most organizations' decision-making, there is a dark cloud to this silver lining of productivity. Over a period of months, years and decades, this electronic information accumulates, creating a new set of costs, risks and challenges.

A. Email and File Over-retention Costs

While many companies still have large stores of paper documents, business is increasingly conducted through electronic media.

Data Storage Costs

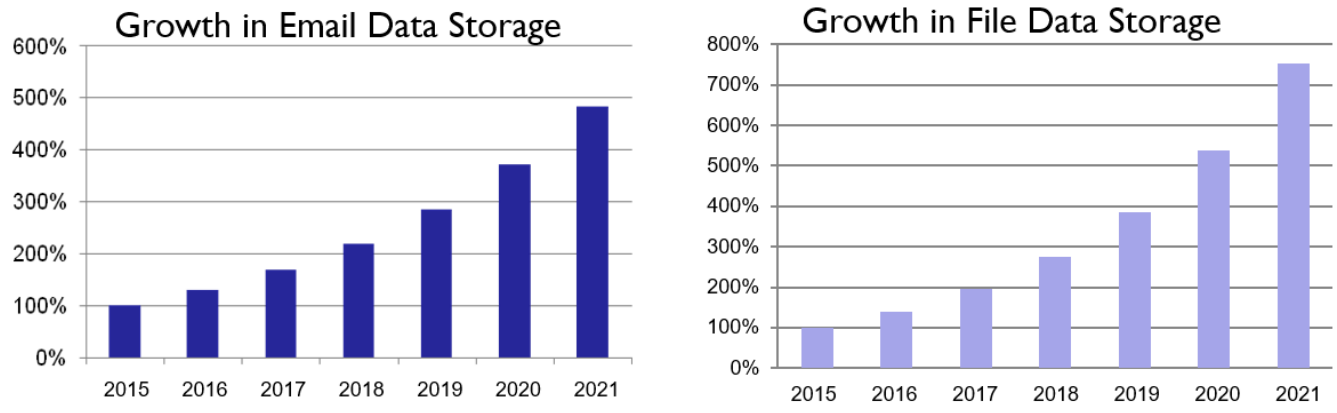

Figure 1. Email and files continue to see increased data storage growth (source: Gartner Group)

Left unmanaged, e-mail and files tend to accumulate and consume data storage space. Traditionally organizations attempted to address this by imposing mailbox "quotas" for email, and storage quotas on centralized file servers, limiting the amount of e-mail or files any single user can store in the server.

Within a typical e-mail server, the messages – headers, dates and message text – only consume 4% of the storage space. Attachments to e-mails take up the remaining 96%. Most organizations have migrated or are migrating their email and file storage to cloud-based systems. These systems tend to include a per-user storage quota, but when this quota is exceeded – often only after a few years – the organization pays additional fees for the increase space.

Increased Discovery Costs

Accumulation and over-retention of email is a risk during litigation. According to a report published by Nelson Mullins Riley & Scarborough LLP, discovery still can represent more than

50% of the costs of litigation. Much of the discovery is around e-mail. In the words of one class-action litigator: "We always go after the e-mail first. It invariably has the best information." Much of the costs of discovery are incurred from searching through emails and files.

B. Over Retention Hinders Privacy Compliance

A number of global privacy rules mandate the identification, control, and deletion of personal information. These rules strictly limit how long personal information can be retained. Many companies focus their privacy compliance efforts on applications and structured data in database systems, with little focus on the over retention of emails and their attached files.

Nevertheless, emails and files can and do contain in the aggregate a significant amount of Personal Information (PI). Email can include employees' or customers' personal information. Files can contain extracts from databases that can contain significant amount of PI. Privacy rules apply equally to emails, files, and structured data applications. Simply because an email may be harder to search or delete does not relieve a company from applying the appropriate rules.

C. Hidden Cost of Hoarding – Impact on Employee Productivity and Collaboration

There's a final pain point with over-retention: employee productivity. A percentage of emails and files does have business value and should be retained for future access. However, over-retention makes searching for and identifying this business value difficult. Specifically, the small percentage of higher-value information quickly gets lost in the clutter of over-retention.

New employees will re-create existing documents either because they don't know someone else already wrote it or they can't find it. Employees will update or edit the wrong version of a document. And while not necessarily an over-retention issues, as an employee retires and even though his old files are stored somewhere, his successor does not have access to that information, making it effectively lost. These are powerful, real inhibitors driven by over retention that decrease employee productivity and collaboration.

III. Defensibly Deleting Emails and Files is Hard

Deleting emails and files is a type of initiative that looks easy at the outset, but can quickly become difficult.

A. Many Layers of Buried Information

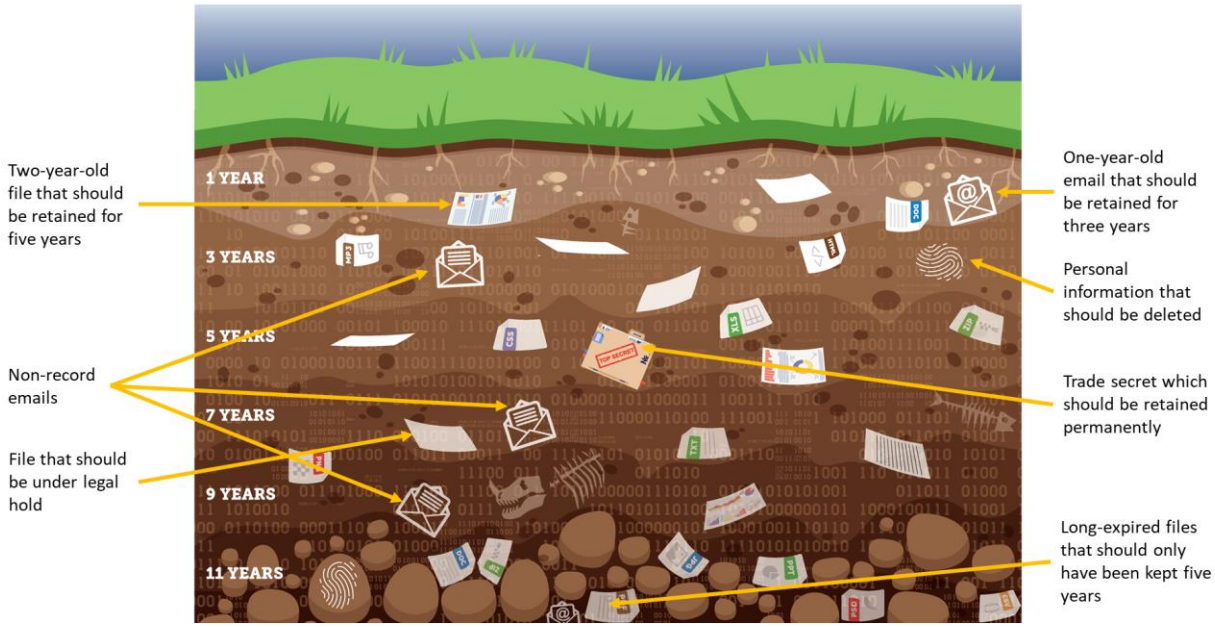

Figure 2. Information horizons. Emails and Files accumulate over the years. These layers contain records, expired records as well as non-record "ROT" or junk. Source: Contoural, Inc.

Emails and files are retained, and month after month and year after year they accumulate creating digital layers called information horizons. These information horizons contain a little bit of everything: records, non-records, copies containing high-value information, no-value information, personal information, intellectual property, and even documents subject to legal hold. What makes deletion efforts hard is often this information is mixed together. Sorting out what needs to be saved requires a type of "digital excavation" in which an information archeologist has to sort through what is important and what is the information equivalent of "dirt" that can be discarded.

B. Employee Hoarding

Perhaps the biggest challenge to deleting emails and files are employees themselves. Most employees hoard their electronic information. They save years and years' worth of information either on their desktop or laptop, or on file shares or cloud storage sites such as Microsoft's OneDrive.

This "save everything forever" approach is motivated by three separate drivers. **First, employees think that this information has business value** and may be useful to themselves or others sometime in the future. This is true: some emails and files do have business value and can and should be saved for a period of time. However, just because some information has future value, that certainly does not mean that all information has future value.

Next, some employees mistakenly believe that they are the custodian of a record or records, and as such this information must be saved. Employees tend to greatly overestimate the "this has to be saved and it's my job to save it" factor.

Third, some employees have defensive motivations for keeping documents –to show in the future if asked that they did or did not do something. Thinking "I better save this to show I did/did not do something" retention is driven by a "just in case mentality."

Finally, the above three reasons often combine to drive habitual retention. It is easier for many to save everything than parse through the above reasons as to why something should be saved.

As alluded above, discussion of deletion can quickly surface emotional pushback. Employees become fearful of the company deleting "my stuff" that "I need to do my job." Unless addressed, this powerful employee resistance can slow or even stop corporate-wide deletion initiatives in their tracks.

C. Everybody's Job and Nobody's Job

The final challenge is organizational responsibility. Most companies have traditional records, e-discovery, privacy and information security programs. Yet none of these programs necessarily are responsible for email and file deletion. Worse, standalone compliance programs can, and increasingly do, conflict with one another. Unless coordinated and integrated, these programs can easily conflict with one-another, thrwating effective deletion efforts. For example:

- Records management that involves minimal data retention can conflict with European and US privacy requirements for time limits on retention of privacy information

- Legal hold preservation obligations can be undermined by records retention processes that require ongoing deletion
- Intellectual property management may be undermined by data cleanup projects that inadvertently delete files and emails documenting the organic development of IP
- IT outsourcing of data storage to cloud providers may run afoul of country-specific data residency regulations

This failure to coordinate standalone programs with other compliance requirements can grind work to a halt.

IV. Email and File Deletion Strategies that Don't Work

While started with good intentions, many of the approaches companies have tried over the years do not work. Many of the same mistakes are made across many different companies.

A. Employee Manual Processes Don't Work

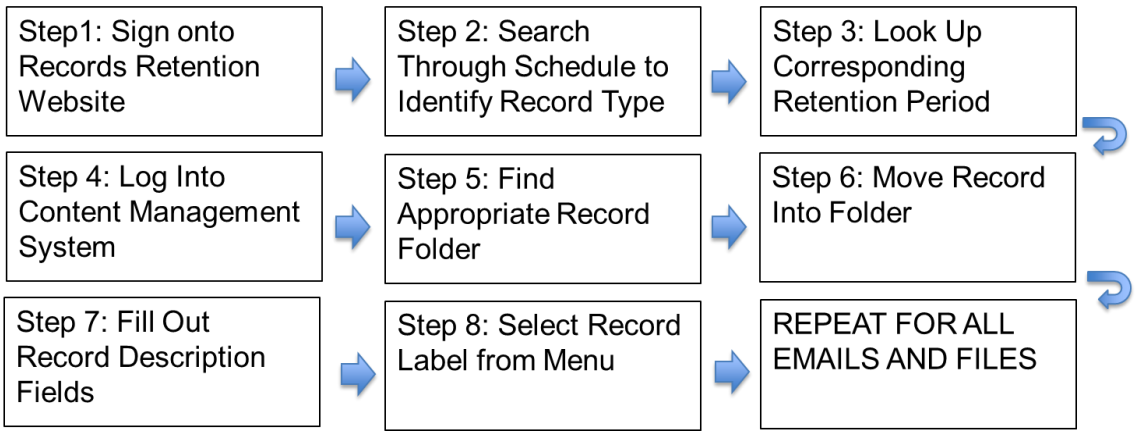

Figure 3. Creating time-consuming processes for managing records simply drives most employees to ignore or avoid these processes.

When most records were either created or received in paper, records management and disposition processes were inherently manual. Today, however, the vast majority of records are created or received in digital format. Unfortunately, **some companies persist in creating detailed, time-consuming manual processes for managing records**. This may include looking up the retention period, labeling an email or file under this retention period, moving it to a folder or repository, or even entering metadata about the document.

The problem is that **these paper-centric processes do not scale.** The sheer volume of emails and files any given employee receives means applying these processes is time consuming, potentially in aggregate taking hours per week. Most employees will not follow them, or they will follow them initially but soon stop applying them.

There is sometimes a mistaken belief that if records management processes are time consuming, they will discourage employees from classifying records, which would serve the larger goal of saving less information. Unfortunately, the opposite occurs where unclassified and unmanaged information simply accumulates. As discussed below, classification processes for records – especially electronic records – need to be easy, fast, and intuitive.

The other risk around manual processes is that **they are less defensible**. The argument made by opponents in litigation is that when employees are doing their own manual deletion, it is difficult for them to be faithful to and consistent with the records retention schedule. The opponents argue that given discretion, employees tend to delete what they consider the "bad stuff" – documents and other information they believe to be inculpatory and only save the "good stuff" — documents or files they believe will be helpful in the event of litigation or regulatory inquiry. This puts companies on the defensive early on, having them try to prove a negative regarding something that they do not (and may never have).

B. Aggressive Deletion Doesn't Work

Figure 4. Aggressive deletion strategies such as deleting email after 30 or 60 days can backfire by driving employee underground behavior. Source: Contoural, Inc.

Frustration by legal and senior management with employees' "save everything forever" mentality can boil over resulting in an "aggressive deletion" strategy that employs automated deletion programs across file shares and email inboxes as well as deleting older files or any emails older than 60 or 90 days. Although also well intentioned, this strategy can quickly backfire.

When companies start an "aggressive" email deletion process, employees often react with a counter behavior of "underground archiving." In a bid to save their emails from deletion, employees save emails on desktops, laptops, centralized file servers, USB drives, and other unauthorized areas. Companies respond by shutting down the ability to use USB drives (generally a good practice).

In an information retention and disposition arms race, employees start forwarding emails, and send files, or other information they believe they need, to their personal email accounts. Some employees have been known to create Gmail accounts solely for this purpose. Companies then try to tighten down on outbound emails, but employees find another way and the arms race continues. Aggressive deletion strategies not only do not work, but they also tend to drive the saving of emails and files in unauthorized, unsecure and hard to access areas, simply increasing the risks and costs of over retention.

C. Monolithic Retention and Deletion Doesn't Work

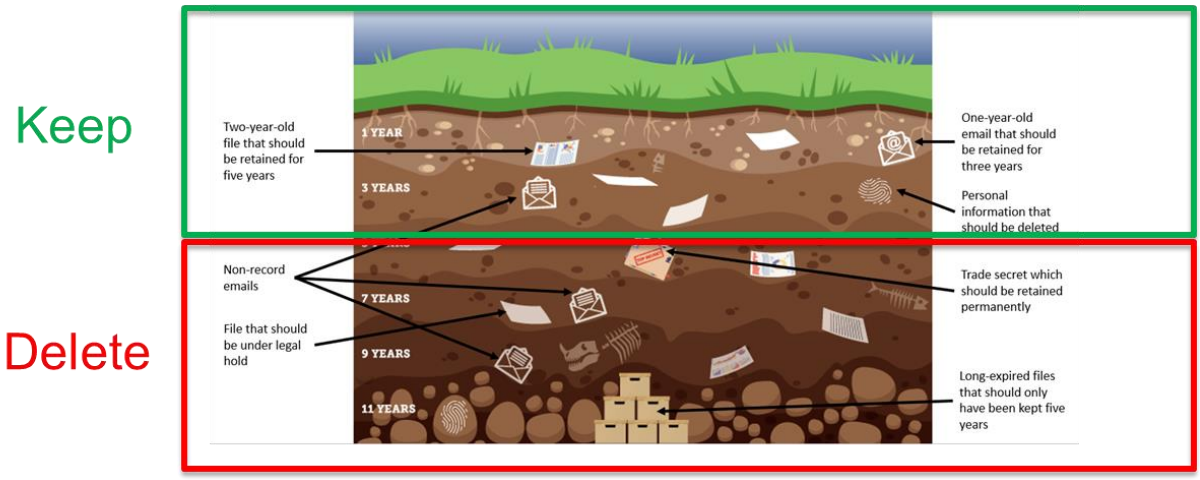

Figure 5. Creating a monolithic retention period such as deleting all emails after three years or all files both can end up deleting records that should be retained for longer. Source: Contoural, Inc.

Another approach to deleting emails and files is to simply define a monolithic retention period of say, three years, and delete all electronic information older than that. It is true that much of this older information is either an expired record, low-value business information, or a copy of information saved elsewhere. Nevertheless, some of this older information cannot be defensibly deleted as it contains:

- Active records that need to be retained longer than the monolithic, three-year period example. (See box below on email.)
- Files or emails that contain business value, including intellectual property, business processes, or reference information
- Files or emails that may be subject to a legal hold

Again, much of the older electronic information can and should be deleted. Yet using one-size-fits-all, monolithic retention periods is likely to result in deleting information that should be saved.

Does Email Really Contain Any Records?

One approach taken by many companies is to simply declare that they have no records in email, thus clearing the path for their defensible deletion. Unfortunately, while on average any given email is unlikely to be a record, email does contain some records, and quite a few in the aggregate. Many of these records live in email exclusively. They can include:

- Shipping (Completion) Notifications
- Supplier Contracts
- Vendor Transmittals
- Contract Negotiations (for proving "intent")
- Employee Vacation Request
- Expense Approvals
- Budget Approvals
- Project Approvals
- Internal Correspondence
- External Correspondence
- Requisitions
- Employee Reviews
- Quarterly Reviews
- Legal Opinions
- Filings
- 3rd party Subpoenas

D. Standalone Content Analytics Doesn't Really Work

Computers can be taught to identify and classify a document based on its content, and automatically classify as per predetermined instructions. This type of autoclassification is most often used in eDiscovery through a technology-assisted review to sort relevant documents from non-relevant ones. Theoretically, the same technology can be used to sort records from non-records. The holy grail of records management is to have a technology that automatically classifies all records in all electronic media with no user involvement.

While we believe this approach holds great promise and will drive records management in the future, these technologies are not quite ready. The typical corporation may have thousands of record types across multiple media. Records classification can be a couple of magnitudes more complex than the discovery associated with a single legal matter. Furthermore, the case law

supporting record types by true autoclassification – without human involvement - is lacking.

There is one area, however, where autoclassification is being used successfully today. It can do a pretty good job identifying certain types of specific information, such as **Personally Identifiable Information (PII) and Protected Health Information (PHI)** for privacy or searching through a series of contracts looking for a particular term.

While these true autoclassification systems are not quite ready for identifying all record types, they can do an adequate job of **identifying non-record, low-value information** that should be deleted. Sometimes cleaning up the redundant, obsolete or trivial data (called ROT) can go a long way to reducing costs and risks.

Can a Vendor Come in and Just Delete Older Information for You?

Many eDiscovery vendors are proposing to use their discovery tools to "clean up" file systems and large stores of emails, promising that their tools will identify records that need to be saved and sort out all the information that can be deleted. While these vendors and their tools can sometimes identify files containing privacy information or being a record, they do not identify who the owner of that information is or how it might have gotten into a file system. They don't address the source person, process, or system that created the information

Worse, such blanket, black-box programmatic deletion of emails and files – even for information that should be deleted – may freak out employees, and in turn drive underground archiving. This technology-only approach disconnects employees and business units from the reasoning behind saving the right information for the right time.

To be clear, file and email content analytic systems can provide value, especially when identifying certain types of content such as privacy. However, they in themselves are not the "silver bullet" solution as advanced by many of their vendors.

Other Approaches that Do Not Work

In addition to the above, there are additional failed approaches or pitfalls that companies should be wary of when looking to defensibly delete their emails and files:

Telling the IT group that this is their problem to solve – An unsuccessful ploy is for the legal group to declare that it is exclusively IT's job to manage data storage and retention. Nice try. IT rarely has the records management, legal hold, or behavior change management expertise to handle this themselves. Simply handing everything to IT will result in nothing being done (at least not defensibly).

Declaring there are no records – Sometimes companies make broad proclamations that no records exist in email or on file shares. This is simply not true (see above), and such statements are likely to increase non-compliance.

Printing all Emails and Files to Paper – One large offsite record storage vendor recently told a company they should simply print all electronic information and store the subsequent paper. (They of course were happy to help store this paper.) Typically, paper is around 100 times more expensive to store and manage than data. Furthermore, defensibly deleting offsite paper storage can be both expensive and difficult.

Deciding you will tackle this problem next year (just as you did last year) – Procrastinating means the risk and pain will continue and will more likely grow due to another year's worth of unrestrained data collection.

Waiting for another group to address the problem – Sometimes the legal department is concerned about over retention, but fearful that raising this issue will drive them to owning the entire data deletion process. As discussed below, successful programs are a team effort across multiple groups. Unfortunately, waiting for another group to step up and start these programs could lead to some very long waits.

Executing an ineffective or unworkable deletion strategy not only prevents the cleanup and deletion of unwanted electronic information, executing the wrong strategy can set efforts back months or even years.

V. Deletion Strategies That Do Work

It can be argued that saving files, emails and other types of electronic content is the easy part. The real test for an effective records program is how consistently it can dispose of expired, duplicative, low-value content. Equally important is disposing of information in a compliant manner that will not be challenged in the future (either during litigation or by a regulator). While developing and executing successful disposition programs can be challenging, there are strategies that do work.

A. Implementing the Five Second Rule with Drag and Drop

Figure 6. "Five Second Rule" – Employees will spend up to five seconds manually classifying documents. If it takes longer, they will use the five seconds to subvert the classification process. Source: Contoural, Inc.

Traditional records management classification and storage processes and procedures require employees to take time-consuming steps. While these manual steps may only take 60 seconds, this minute multiplied against the hundreds of records employees may receive or create each week potentially equals many hours of records management burden per week.

Instead, successful deletion starts with the five second rule: **employees will spend at most five seconds looking up a retention period, manually classifying an email for file, moving the email or files to a repository, and applying any labels.** If the manual records classification and management process takes longer, even well-meaning employees will soon start ignoring the process.

Most modern content management systems such as Microsoft 365, OpenText, and others provide the ability to automatically apply metadata tagging (also referred to as labeling) based on where a record is stored. In other words, these systems allow a type of "drag and drop" tagging: Under this method, when employees drag and drop a file or email into a folder or specific location, the system automatically tags it.

The system can automatically tag and track the document for multiple types of governance controls, including records retention requirements, data security classification, access controls, and even legal hold capabilities. These retention periods, security levels, and other policy attributes are pre-configured into a given managed folder. When the user places a document into the folder, the content management system then automatically tags and applies these controls to the file. No action is required on the part of the user other than storing the document into the right folder; the system does the rest.

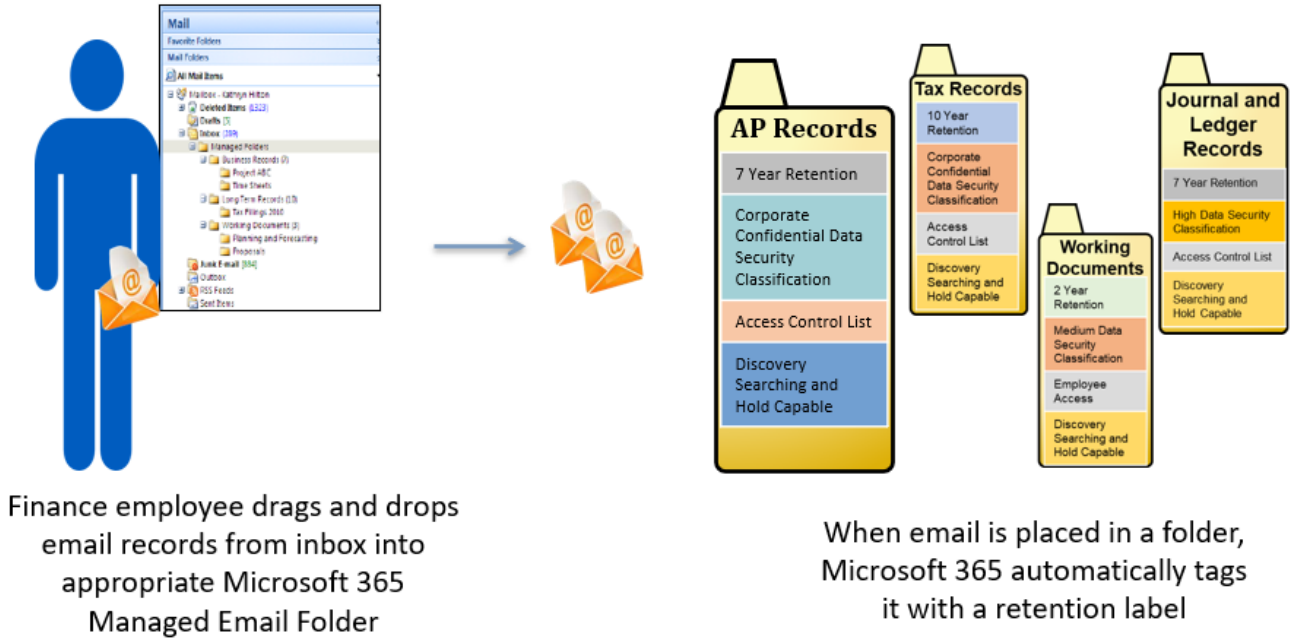

Figure 7. Microsoft 365 (mentioned in this figure) and other content management systems have auto-tagging capabilities for automatically apply retention, data security classification, access controls, and eDiscovery to emails, files, and other documents stored within the system's folders. Source: Contoural, Inc.

This **"drag and drop" classification strategy** requires more upfront work. The records management or Information Governance team needs to configure the managed folders or other repositories with the applicable records retention, data security, and access rules. Ideally, a complete Information Governance framework – retention, security, and access– should be so configured.

Translating the records retention schedule, data security classification and access control policies into specific system configurations can be tricky, and requires **ongoing collaboration** between the records, security, and IT groups.

While the backend configurations can be complicated, **the user view and experience need to be kept simple and intuitive**. Different employees will have different folders to store their information, and collectively across the repository there may be many different folders. Any given employee should **only see four or fewer folders.**

The upfront investment is worth it. Those companies that do take the time and effort to configure their systems for proper records management may suddenly find classifying records, personal information, and other governed content much easier. Employees find the "drag and drop" approach easy to use and so, not surprisingly, usage rates are high.

B. When It's Time to Delete a Record, Let Systems Do It Automatically

Figure 8. Repositories can be configured to automatically dispose documents when their retention period expires. This deletion can be suspended for legal holds. Source: Contoural, Inc.

It is very difficult to get employees to manually delete older emails and files. It is better to get content management systems to delete information automatically. This removes the employee from the disposition process, and instead depends on leveraging technology to dispose of records when the retention period expires.

To make automated disposition work, documents need to be classified per the "drag and drop" classification strategy discussed above when they are first received. Then the employees don't need to do anything. Office365 and other repositories will automatically dispose of documents once the expiration date has been reached, based on when it was entered into the system. The old information simply fades away.

C. Deleting Emails and Files When You Move to the Cloud

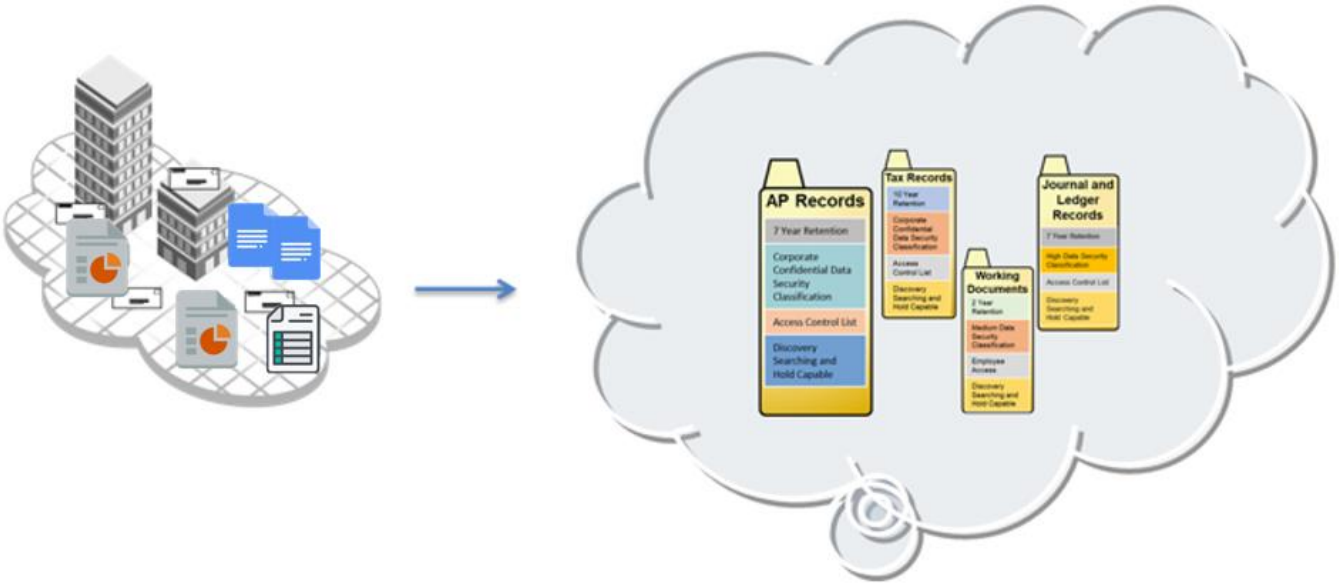

Figure 9. Migrating systems to the cloud provides an excellent opportunity to defensibly deleted older, unneeded emails and files. Source: Contoural, Inc. Microsoft 365 is a trademark of Microsoft. Source: Contoural, Inc.

Many companies are moving from on-premise storage of their emails and files to cloud-based systems. This switch to cloud-based systems is an excellent opportunity to clean up old emails and files. First, **identify all the information to be migrated**. Do not necessarily assume that everything stored on the old system should be moved to the new systems.

Next, instead of simply dumping straight from the old file system into the cloud storage, **set up the appropriate folders** that are configured with the appropriate retention period. Once everything is set up move the selected older content into its new location.

Doing this type of "smart migration" does require some pre-planning and configuration ahead of time. Avoid the temptation to simply throw everything up into the cloud and planning on sorting it out later. The benefit of thinking this through is two-fold: first, it can clean up and greatly reduce the amount of emails and files. Second, by configuring the cloud system with appropriate retention, moving forward there will be much less accumulation of information.

D. Creating a Working Documents Area

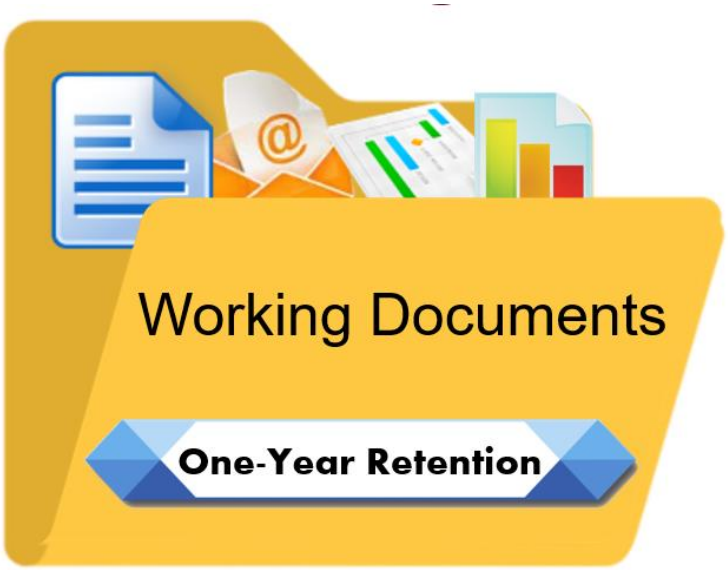

Figure 10. A working documents strategy creates a working documents area in a managed area that permits employees to save whatever they want for a limited period, say one or two years. Older information gets automatically deleted. Source: Contoural, Inc.

Employees feel compelled to save everything. Instead of trying to fight this tendency, give them a safe, manageable place to save content. Within your Microsoft 365 or other content management system, provide a "working documents" folder. A working documents folder is a "personal file "area that allows employees to save any document for short-to-medium term retention. Allow employees to save whatever they want in these folders for whatever reason.

Because they have been provided with a viable place to save any type of information in the working documents folder, prohibit them from saving unneeded information on desktops, file shares, and other unmanaged and uncontrolled places. Explain to employees you are not stopping them from saving what they need, rather only asking that they save it in the right place.

A working documents folder does not, however, enable employees to retain their files and emails forever. Set the retention for these folders anywhere from one to two years. Then let the system dispose of the information when it expires. The key is that while employees can save whatever content they want, working document folders exist in a controlled and secure environment, with disposition automatically enforced. Microsoft 365 and other repositories are terrific at saving information. They are even better at deleting it.

In one sense, working documents folders provide a safe and approved version of the "underground archiving" behavior discussed above. There are no restrictions on what can be saved. Unlike underground archiving, a working documents folder allows information to be searched, secured and easily deleted at the appropriate time. Likewise, there should no longer be a reason for employees to engage in actual underground archiving.

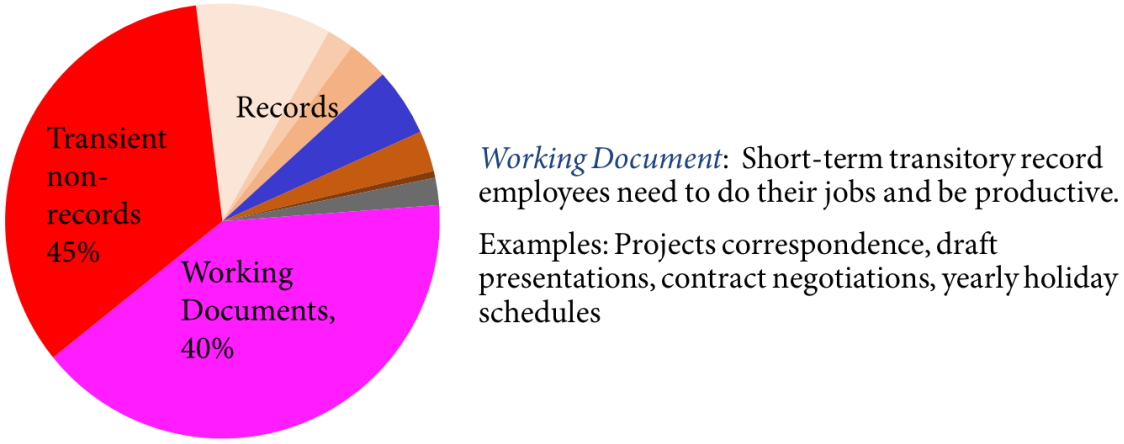

Figure 11. Allow employees unlimited ability to save working documents in a searchable, centrally managed controlled repository, typically a managed folder. Auto-delete these working documents after established period of two to three years. Source: Contoural, Inc.

Once records management and working documents folders are configured, employees should be trained to drag and drop emails from their inbox into one of these folders. Everything that needs to be retained, or an employee wants to save, should be moved to these folders. It can be assumed that any email left in an employee's email inbox for more than 90 days is truly junk – it is neither a record nor does it have any transitory business value (otherwise it would have been saved in the working documents folder). It is now safe to automatically delete email older than 90 days from the inbox.

E. Implementing Employee Behavior Change Management

Creating policies and configuring technology are key steps to getting rid of old emails and files. However, the most important step is often overlooked: employee behavior change management.

Behavior change management is **a combination of messaging, communication strategies, training, and audit**. Designed to drive users toward a target behavior set and to measure **progress** in achieving compliance, these activities are also beneficial for providing formal, consistent communications to employees and executive sponsors during implementation.

The goals of behavior change management include:

- ***Drive User Adoption*** – Drives program adoption by business units and employees.
- ***Communicate Messages that Resonate*** – Identifies key messages likely to resonate with employees.
- ***Sell Program as a Win*** – Messages program as a win for all employees, not a compliance burden.
- ***Test Consistency*** – Ensures messages and trainings are effective for all groups across the organization.
- ***Demonstrate Compliance*** – Demonstrates compliance with requirements and the company's intent to follow policies.

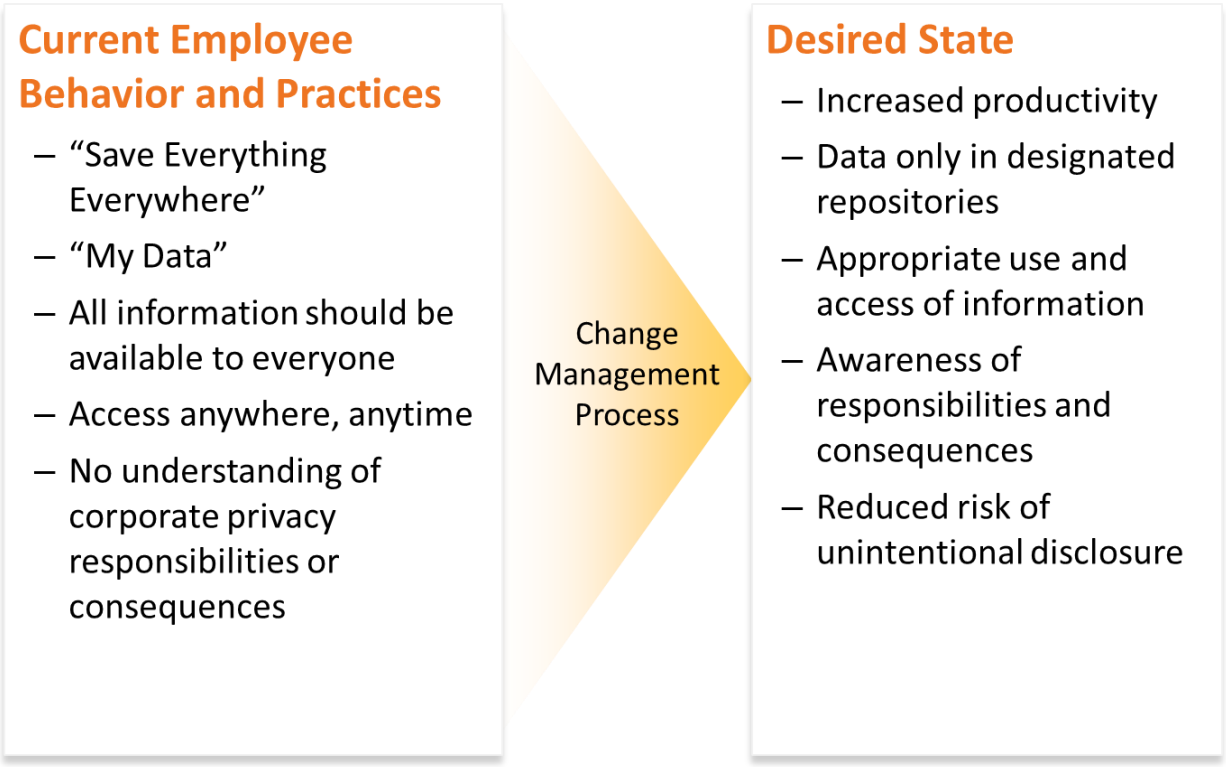

Figure 12. Behavior change management is the most important yet overlooked component of disposition programs. Source: Contoural, Inc.

Employees need to understand what the policies are, and they need to be using the right processes. With the right training they are now aware of their responsibilities and what the consequences are for non-compliance. Putting together an effective change management program involves working with a communications and training group to:

- understand what kind of communication plans have been successful in the past in the organization, and
- understand which platforms are available for training.

To ensure a successful change, it is key to identify which audiences need to be addressed, what platforms are available to deliver the training to the right audience, and what messaging needs to be developed.

Case Study: A Health Insurance Organization Classifies and Deletes Email

Information problem: A health insurance provider needed to get better control of emails as, for many years, employees had adopted a de facto "save everything" policy, storing their emails in their own personal folders. These emails contained a variety of active records, privacy information, and corporate confidential data, as well as significant amounts of low business value or expired information. In addition to the security risks, the ongoing accumulation of this data significantly increased discovery costs and was burdensome during regulatory inquiries.

Information governance projects: The company embarked on a multiple month email policy and archiving project that included email policy updates, technology acquisition, employee training, behavior change management, and audit programs.

Impact: Emails that were records or had sensitive information were properly classified and more than 45 million emails were defensibly deleted during the pilot — all with no employee complaints.

VI. Creating Your Plan

Taking an ad hoc or knee-jerk approach to a deletion initiative often produces projects that get off track and stall out. Take a small step back and think about what needs to be in place and done before rolling out your plan.

A. Critical Components to Have in Place Before You Start

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) that justifies retaining and deleting documents.

Ensuring Records Retention Schedules Include Business Value

Organizations are often reluctant to engage in deletion knowing that some of the data contain records that 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 mandatory retention, and "transitory information," which is everything else.

We recommend that Record Management 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 thus obvious.

Consistent Legal Hold Policies and Processes – Before automated deletion can commence, companies need to ensure that information under legal hold is protected. An effective hold process addresses the following requirements:

- *Hold notification* – The issuance of a litigation hold notice that lets custodians (employees and non-employees, as applicable) know of their obligation to preserve relevant information and specifies how they should do so.

- *Information security* – To prevent the deletion, loss, or inaccessibility of relevant documents, such information needs to be saved in a repository that is separate from other information assets.
- *Ongoing preservation* – A process must be put in place to ensure that once a hold notice is issued, all future relevant documents are also subject to the legal hold and are properly preserved.
- *Hold release* – Once a particular matter has been resolved, and provided that future litigation is not anticipated, the organization should "release" the hold, notify custodians, and resume normal retention and disposition programs.

All these elements of the legal hold process must be supported by documented procedures, standard templates, repeatable workflows, and forms (or electronic tracking and management systems), along with the appropriate training for litigation support staff, organization managers, IT, and all other impacted employees. Ensuring the information under preservation is properly protected, the deletion process is freed up to allow all other deletions without fear of spoliation.

Consensus with the Business – Even if the legal group has the authority to delete emails and files, it is important to not surprise business units with "middle of the night" deletion activities. Even if it is technically possible to delete emails and files, doing so without communicating to employees might work *once.* Thereafter, employees will be fearful their information might be deleted, and this can kickoff a large-scale underground archiving. There are examples of companies that spent quarters developing their deletion strategy but failed to appropriately engage the business units and their entire initiative was shut down in a couple of days. After such failures, it may take years before the organization is open to trying to clean up information again.

B. Create a Plan for Fastest Disposition

Email and file deletion projects are often driven by problematic events, including large eDiscovery bills or privacy non-compliance findings. Addressing them is often an urgent, sometimes even emotional response, with pressure from senior management to get the deletion done.

Defensible deletion should be executed as quickly as possible. However, projects done in an ad hoc, knee-jerk manner get started quickly but often get stuck and stall out just as quickly. Sometimes moving a little bit more pragmatically, avoiding pitfalls, leveraging technology, and engaging business units can be the fastest and most effective way to delete the most unneeded information.

Moving fast starts with **having a plan for all the steps and laying this plan against the timeline**. The plan should not skip critical steps such as ensuring the schedule is up to date or the legal hold process is complete. It is fine to start with smaller pilot groups, find success, and then leverage these processes across the rest of the organization.

Resist the siren call of "miracle" products that claim to automatically delete everything with little effort. Unfortunately, these either do not work, drive the wrong behavior, or delete information which needs to be saved. Your plan should not only address the first wave of deletion and clean up, but also how do you make this an ongoing, routine - and even boring - process. Boring deletion is good. Build it into your plan.

Finally, ensure the plan includes behavior change management. Sending a well-crafted message such as "we want to identify your important information and then get rid of the clutter that prevents you from finding and accessing it" will get more buy in and drive more deletion than announcing a company-wide deletion campaign that may raise concerns. Same activity, just different messaging. Build time in your plan to communicate these effectively.

C. Reasonable Disposition Targets

How much email and files can be defensibly deleted? This of course depends on the age and size of the organization, as well as if the organization has suffered from a "hoarding" culture. In general, following the strategies addressed above, most organizations can expect to delete more than 40% of their emails and files.

As noted, this deletion requires a focused approach, and needs to happen over a period of time. However, even companies that initially believe that they are beyond hope because "our employees save everything forever" can expect to defensibly delete large amounts of unneeded information.

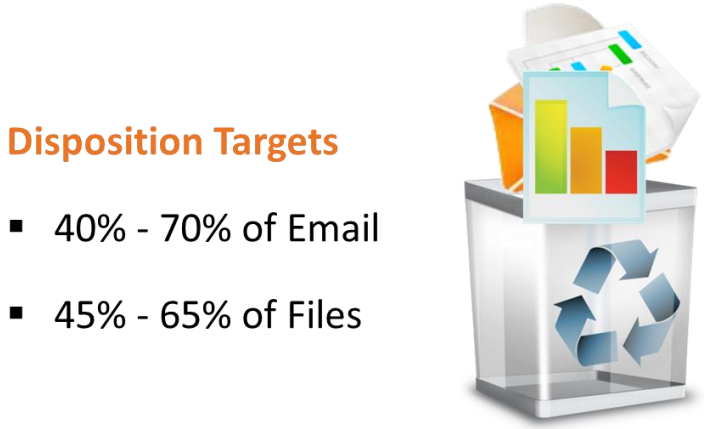

Figure 13. A well-executed deletion program can dispose of significant amounts of emails and files. Source: Contoural, Inc.

When setting disposition targets, flexibility is the key. A marketing group, for example, may want to retain campaign development materials, for say, 10 years. While one could argue that this is unreasonably long (which it probably is) you may want to allow this longer retention period for this one document type.

Sometimes compromising on a few document types that might in the aggregate comprise less than 1% of the information store, can then free up the group to look at the other 70% of their older information which should be deleted. Conceding over retention on a few areas emotionally frees up employees and business units to then be more aggressive on the rest of their content. Don't pick a battle over a small hill, when there is a much larger mountain that can be conquered.

D. The Hidden Blocker – Legal

These initiatives sometimes face a hidden blocker – the legal department. Legal is often the loudest advocate for the need to get rid of all the "junk" employees keep, as they often suffer the most pain from over retention. Ironically, once policies are established, processes are created, and companies are ready to hit the "go" button, it is not uncommon to see a timid litigation or compliance group who is fearful to hit the delete button.

It is not that they say no, but rather they just will not say yes. This reluctance needs to be addressed. When done correctly, effective deletion is defensible and, perhaps more important, helps the company (including the legal group) be more productive.

VII. Final Thoughts

Perhaps the biggest barrier to deleting files and emails is fear. Fear that employees will not put all the information in the right place. Fear that some of it will be misclassified or retention will not be properly applied. Fear that records under legal hold will be deleted. Fear that records will be deleted before their expiration date.

Information Governance is an inherently imperfect process. Fortunately, **the courts and regulators do not expect perfection. Rather, they expect reasonable, good faith efforts**.

In your policies, declare what will be done. Execute those policies with processes, technology, and training. Demonstrate that policies are being complied with through metrics and audits. Show that a plan has been developed. Show that the plan is being executed. Audit the results and remediate any shortfalls. Not perfect? That is fine. No one expects it to be perfect. Start with good and just keep moving forward.

VIII. About the Author

Mark Diamond is an industry thought leader in records management and Information Governance, encompassing records and information management, litigation readiness, control of privacy and other sensitive information, defensible disposition, and employee collaboration and productivity. Mark is a frequent industry speaker, presenting at numerous Legal and IT industry conferences. Additionally, Mark delivers more than 50 onsite Information Governance seminars to internal corporate audiences each year.

Mark is the founder, President & CEO of Contoural, Inc. Previously, Mark was co-founder of Veritas' (OpenVision) Professional Services group; founder and General Manager, Worldwide Professional Services for Legato Systems; and Vice President of Worldwide Professional Services at RightWorks. He has also worked as a management consultant. He also served as Chair of the Storage Networking Industry Association's customer advisory board on data security. He sits on the board of advisors for several high technology companies.

He has a bachelor's degree in Computer Science from the University of California San Diego. Mark is a former President of the UC San Diego Alumni Association and served as a Trustee of the university's foundation.

Mark welcomes any questions and comments regarding this Guide. He can be reached at mdiamond@contoural.com and for more information, on Contoural's site at www.contoural.com.

IX. About Contoural

Contoural is the world's largest independent records management, Information Governance and privacy strategic consulting service. Contoural does not sell any products or take referral fees, store any documents, or provide any lawsuit-specific "reactive" e-discovery services, serving as a trusted advisor to its clients by providing unbiased advice. Contoural has more than 30% of the Fortune 500 as clients, across all industries, as well as federal agencies and local governments. Contoural offers a range of records management and Information Governance consulting services:

- Defensible Disposition Strategies
- Information Governance Assessments and Roadmaps
- Records Retention Schedule Development and Refresh
- Data Placement Strategy
- Employee Behavior Change Management and Training
- Legacy Data Remediation
- Personal Data Inventory and Data Mapping

- Privacy Policies, Notices and Procedures
- Privacy-enabled Incident Response Development
- Privacy Communications and Training

Contoural is a sponsor of the ACC Information Governance Network and of the Records Management section of the ACC Legal Operations Maturity Model. More information on this and other Information and Privacy topics can be found at www.contoural.com or for resources on a specific topic email us at info@contoural.com.

X. Additional Resources

A. ACC Maturity Model Resources

ACC Records Management Maturity Model

ACC U.S. States Privacy Capability Maturity Model, ACC Information Governance Network

B. ACC Guides

"Information Governance Primer for In-house Counsel," (2016), *available at* https://www.acc.com/resource-library/information-governance-primer-house-counsel

"Creating a Modern, Compliant, and Easier-to-Execute Records Retention Schedule," (2017), *available at* https://www.acc.com/resource-library/creating-modern-compliant-and-easier-execute-records-retention-schedules

"Executing Your Records Retention Policy and Schedule," (2018), *available at* https://www.acc.com/resource-library/executing-your-records-retention-policy-and-schedule

"Operationalizing the California Consumer Privacy Act," (2019), *available at* https://www.acc.com/resource-library/operationalizing-california-consumer-privacy-act-united-states

"Automating Your Records Management Program" (2020), *available at* https://www.acc.com/resource-library/automating-your-records-management-program

"Introduction to Records Management" (2022) *available at* https://www.acc.com/resource-library/introduction-modern-records-management

C. *ACC Docket* Articles

"Should You Combine Your Privacy and Records Management Programs?," Jennifer Couture and Mark Diamond, *ACC Docket* (January 2021) *available at* *https://docket.acc.com/should-you-combine-your-privacy-and-records-management-programs*

"Everybody's Job, Nobody's Job: The Best Way to Create an Information Governance Program Without Going Crazy," Patrick Chavez and Mark Diamond, *ACC Docket* (April 2019) *available at* *https://www.accdocket.com/everybodys-job-nobodys-job-best-way-create-information-governance-program-without-going-crazy*

"Upgrading Your Traditional, Paper-centric Records Program to Be More Modern, Compliant, and Useful," Andrea Meyer and Mark Diamond, *ACC Docket* (December 2018) *available at* https://www.acc.com/resource-library/upgrading-your-traditional-paper-centric-records-program-be-more-modern-compliant

"Building a Business Case for Information Governance," Annie Drew and Mark Diamond, *ACC Docket* (October 2014), pp. 26-40, *available at*

https://www.acc.com/resource-library/building-business-case-information-governance-program

D. ACC Legal Quick Hits

"How to Prevent Employees From Saving All Documents Forever" (2020), *available at* *https://onlineed.acc.com/learn/course/internal/view/elearning/360/how-to-prevent-employees-from-saving-all-documents-forever*

"Nine Ways Companies' Records Programs Sabotage Compliance, Raise Risks, Increase Costs and Lower Productivity" (2021), *available at* *https://onlineed.acc.com/learn/course/internal/view/classroom/1076/nine-ways-companies-records-programs-sabotage-compliance-raise-risks-increase-costs-and-lower-productivity-sept-16-2021*

"Using Native Office 365 to Manage, Publish, and Automatically Enforce Your Records Retention Schedule" (2020), *available at* *https://onlineed.acc.com/learn/course/internal/view/elearning/357/using-native-office-365-to-manage-publish-and-automatically-enforce-your-records-retention-schedule*

E. ACC Webcasts

"Creating a Records Retention Schedule That Does Not Create Problems (And Actually Solves Them)," *Webcast* (2020), *available at* *https://onlineed.acc.com/learn/course/internal/view/elearning/645/creating-a-records-retention-schedule-that-does-not-create-problems-and-actually-solves-them*

"Introduction to Modern Records Management" (2021), *available at https://onlineed.acc.com/learn/course/internal/view/elearning/644/introduction-to-modern-records-management*

F. ACC Information Governance Network Resources

"Information Governance – Glossary of Terms" (2019), *available at* https://www.acc.com/resource-library/information-governance-glossary-terms

"Employee Behavior Change Management Programs for Information Governance," *Quick Overview*, (2017), *available at* https://www.acc.com/resource-library/employee-behavior-change-management-programs-information-governance

"Creating a Data Classification Standard" (2017), *available at* https://www.acc.com/resource-library/creating-data-classification-standard

G. Contoural White Papers

"Reducing Your Offsite Paper Storage Risk and Cost," *White Paper,* (2018), *available upon request at* https://www.contoural.com/white-papers/ on Contoural's website www.contoural.com

"Defensible Disposition: Real-world Strategies for Actually Pushing the Delete Button" *White Paper,* (2014), *available upon request at* https://www.contoural.com/white-papers/ on Contoural's website www.contoural.com

"Stop Hoarding Electronic Documents," *White Paper,* (2012), *available upon request at* https://www.contoural.com/white-papers/ on Contoural's website www.contoural.com