Author
Marta Farensbach

Sherpa Software
456 Washington Rd. Ste. 2
Bridgeville, PA 15017
(800) 255-5155
www.sherpasoftware.com

Demystifying Defensible Deletion

Best known strategy for retaining and disposing of items based on organizational value and legal requirements.

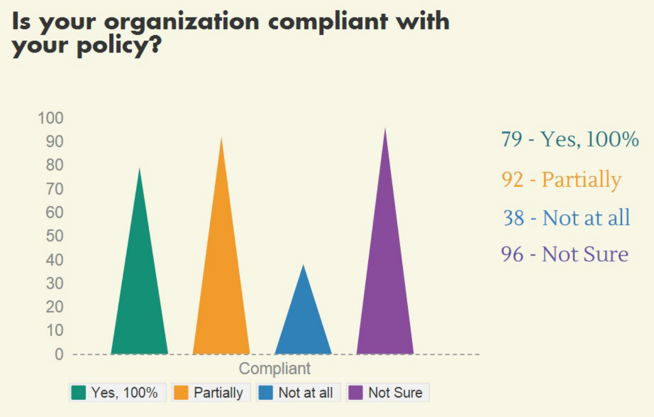
This white paper will define defensible deletion while highlighting some key areas where organizations should take action in order to manage handling and storage costs, and also free up resources that can be better spent elsewhere.

SHERPA SOFTWARE
Solutions for Information Governance

Introduction

In a number of recent court cases, noteworthy fines have been assessed or adverse judgments issued due to ineffective or inadequate corporate deletion policies. This has brought significant attention to defensible deletion practices and has triggered concern amongst key corporate stakeholders.

A recent survey of more than 300 respondents conducted by Sherpa Software indicated that only 19 percent of respondents are fully compliant with their existing defensible deletion policies. A whopping 37 percent had no policy in place, while 23 percent did not even know if they had a policy at all.



Other industry research reports similar findings: Another survey[1] conducted by ARMA drew this conclusion regarding the defensible disposition of ESI, or electronically stored information: ‘Disposition is ineffective and technologies are not yet widely deployed,’ based on the fact that only 34 percent of respondents gave passable ratings to the effectiveness of their organizations efforts. It seems that either companies don’t have defensible deletion policies in place, or their employees aren’t aware of them or compliant. In this paper, we explore why this is a concern and what can be done to help.

What is defensible deletion?

Best known as a strategy for retaining and disposing of items based on organizational value and legal requirements, defensible deletion ‘allows organizations to manage their handling, storage and eDiscovery costs as well as their risk while freeing up resources that can be better spent elsewhere’ (as noted by Deloitte[2]). It is often considered to be an integral part of a comprehensive information governance[3] strategy which treats data ‘generated by day-to-day operations of an organization as a valuable corporate asset that must be managed and disposed of in a responsible fashion.’ Defensible deletion, which is also known as defensible disposal, is about more than just simple retention and removal; it also includes assigning value to your data and reducing operational risk to make the organization more effective and efficient.

[1] Cohasset - Source.

[2] Deloitte Discovery Financial Advisory - Source.

[3] Entire article can be found by clicking here.

The importance of defensible deletion

The price of storage has decreased steadily over the years and there is a strong contingent that favors a 'keep everything' approach to ESI management; however, this argument ignores several critical facts. First, although the average storage cost has decreased significantly, the actual volume of ESI has grown exponentially so that the total expenditure on storage has actually increased[4]. This trend doesn't just reflect online videos or social media postings, the increase in ESI is being fueled by virtually every business process.

And yet, according to noted information governance lawyer Martin Felsky, more than 69 percent of corporate data has no business, legal or regulatory value[5]. Where does this data come from? First, the types of ESI being created today could only be imagined a decade ago; just look at how graphics and videos inflate the size of attachments, while interactive instant messaging and easily accessible repositories spread it out across corporations. As knowledge workers become more technical, they leverage the latest digital tools to increase output and productivity. This often results in even more storage requirements.

Organizational fatigue and resistence are other culprits in the proliferation of corporate data. It is easier to do nothing, storing unnecessary data, than it is to expend energy to define a policy, classify information, and then move or delete it. Laziness, however, cannot take the entire blame. Indeed, there is significant lack of education focusing on what types of data are important to an organization, as well as lapses in clarity defining the approved methods for the disposal of that data.

Another factor contributing to the increase in ESI is the hoarder mentality pervasive amongst many employees; this results in keeping all kinds of items (electronic documents, email, databases or perhaps even backup tapes) on the off-chance it might be needed at a later point. That data becomes invisible, forgotten or lost in the overwhelming volume of documents created daily. Because ESI is created so easily, it builds up quickly and soon becomes too difficult to handle with manual processes.

“Another factor contributing to the increase in ESI is the hoarder mentality pervasive amongst many employees; this results in keeping all kinds of items (electronic documents, email, databases or perhaps even backup tapes) on the off-chance it might be needed at a later point.”

The effect that such an overload of data can have on a company is striking and manifests itself in several areas.

Operational Clutter

Disorderly data increases the day-to-day costs of running the company. Storage, backup, bandwidth and, yes, even the cloud, become more expensive as ESI grows exponentially. More than 90 percent of ESI has been created in the past few years[6] and given the increasing amounts of text, voice and video, those numbers are projected to get even bigger.

[4] Extracting Value from Chaos - Source

[5] Defensible Deletion, Martin Felsky, PhD - Source

[6] Big Data: Ready for blast-off? - BBC News

The day-to-day workings of an organization are often constrained by this overabundance of information. How often do employees at every level complain they 'can't find anything' or that locating key information is like 'finding a needle in a haystack?' This causes duplication of effort on an epic scale and makes both reporting and metrics a challenge. An easy win in defensible deletion is to utilize policy and technology in order to reduce duplicative ESI by identifying it and deploying consolidated storage and versioning systems.

Obsolete data from legacy systems is often ignored or relegated to an afterthought; yet this grandfathered data carries just as much of a liability burden as an email sent yesterday when seen in terms of eDiscovery, compliance or governmental regulations. Older ESI often falls outside of corporate policy, thereby becoming a challenge to search, move and manage. In turn, this ends up counteracting the goals of information governance and defensible deletion, costing the organization time, money and potential liability for litigation.

Liability & Risk

A huge concern from the legal point of view is the liability of retaining vast amounts of data, or worse, improperly disposing of it. Various cases (for example, Rambus[7] and Arthur Andersen[8]) show that spoliation of data can turn into adverse judgment in court. This risk can be mitigated by including a proactive defensible deletion capability. Information governance consultant Bill Tolson[9] notes, "A documented and approved process, which is consistently followed and has proper safeguards, goes a long way with the courts to show good faith intent to manage content and protect that content subject to anticipated litigation." The 'defensible' portion of defensible deletion is heavily dependent on effective enforcement and auditing of well-established policy.

Another area of legal concern is the dreaded 'smoking gun' hiding in mountains of ESI. As eloquently stated by research firm ESG[10], "The legal exposure from retaining data past its expiration period presents a liability for involvement in potential legal or regulatory requests which might otherwise be avoided."

In reality, many organizations are not involved in headline-making litigation – rather, the real cost of unregulated data is that if they are sued and are not prepared, the organization will endure an enormous expenditure of time and resources searching, culling, preserving, converting and reviewing unnecessary data.

But liability concerns don't end there - a number of companies fall under protocols issued by government or trade groups to which their members must comply. In this case, the concern is not so much about having unwanted ESI, but rather that their data retention policy fulfills the rules and regulations imposed upon their industry. Additionally, a company can open themselves up to privacy concerns (often based on jurisdiction) or compliance infractions based on the prevalence of Payment Card Industry (PCI) data or Personally Identifiable Information (PII) in their ESI repositories. Without an outlined deletion policy, this and other confidential data might be inadvertently released.

[7] Bloomberg News - Source

[8] Dead Men Tell Some Tales - Source

[9] Bill Tolson's blog - Source

[10] Defensible Disposition in Practice - Source

Delete Everything?

Given the very real liability and risk, why not just delete all ESI after a certain time, or let the employees decide what to delete? Disposing of all ESI in this manner has two big drawbacks. First, this approach may impair business operations. Day-to-day running of organizations is fueled by ESI; it cannot just be cut off. Furthermore, much of the value in today's corporations lie in their information assets. These resources need to be protected from accidental deletion. Otherwise, items may be destroyed based on considerations other than legal, regulatory or business needs. Additionally, there are many types of ESI that are just not accessible for casual deletion – think of the legacy systems and obsolete data that permeate organizations of a certain age.

Even if not under a regulatory burden to keep data, the second drawback of the 'delete everything' approach revolves around the fact that organizations might have to suspend the deletion of data for purposes of legal action. If the free-for-all deletion policy described above was implemented, what happens when a company is sued or subpoenaed (or if such is reasonably anticipated)? At that point, under the United States Federal Rule of Civil Procedure, 26(f)[11] a company is required to stop deletion of any potentially relevant documents that may affect litigation. These litigation holds[12] are essential to a defensible deletion strategy and a key factor for any ongoing proceedings. Could automatic deletions be stopped, or employees be relied upon to change their habits without a policy in place? History suggests not.

Starting the right way

For most organization, creating a defensible deletion policy makes sense, but it is often difficult to get started. The following tips can help with implementation:

- Get a champion, create a team of key stakeholders at the top that have influence to force buy-in
- Realistically assess the current state of affairs by identifying:
    - Technology in use
    - Business silos
    - Regulatory requirements
    - Current policy shortcomings
- Outline risks and costs of status quo
- Establish ROI, define goals and set expectations for crucial groups:
    - Legal
    - Compliance/Risk
    - Information Technology
    - Business/Management
- Establish effective exceptions

[11] For more information on FRCP rule 26f, refer here.

[12] For more information on litigation holds refer here.

Implementing effective strategy

"Policy is 10% of the problem, implementation is 90% - how to change the culture of convenience?"

Martin Felsky

Each organization has its own requirements and challenges, so there is no one-size-fits-all approach to implementing an effective defensible deletion strategy; however, there are some common themes that can be identified.

Automated technology can be a big help with the setup, processing and auditing of policy and procedures; effective software can simplify the rollout and takes the burden off individuals. It is critical to the defensibility portion of the defensible deletion strategy. As noted by Deloitte, "Employees are often loath to eliminate their own files… they think they may need them again, or because they are just too busy."

However, any automation technology must accommodate the exceptions that are a critical part of establishing a defensible deletion strategy. These exemptions are often due to legal, compliance and business needs. Litigation holds are typically the primary exception mechanism used by the legal team.   In addition to sparing documents from deletion, the litigation hold process should include procedures for notifications, acknowledgements and a process for aging out data once the hold is lifted.

Other exceptions may include compliance with privacy laws, security concerns and most importantly, ongoing business needs. These exclusions should be well-defined at the start of the implementation by recognizing the information assets that have organizational value. There are a number of methods to help pinpoint and exclude this so-called 'active data' from deletion policy. Identify employees who can assess ESI then arm them with the right tools and educate them about the policy constraints. In some organizations, all employees have this capability. Other places use technology to create categories for items that can then be automatically grouped by type (e.g. insurance claims, personnel files, broker-dealer communication, tax records, etc.). Regardless of how the exception is formed, it is essential that it is monitored for abuse – exempting all ESI from policy is as useless as having no policy at all.

Incremental approaches are often a preferred strategy rather than attempting to deploy wide-ranging policies all at once. One helpful technique is to define silos based on organizational needs, then prioritize them according to risk factors or ease of implementation.

Tips

Implementing a defensible deletion strategy takes time and effort. The following tips may be helpful:

- Keep the focus of strategy simple. Make the resulting policies as reasonable and realistic as possible. Maximum adherence is usually proportional to minimal disruption.
- It is essential to get buy-in from a ‘cross-disciplinary’ team who have the authority to execute policy. Get the right mix of expertise – business needs, technical experience, records management and a legal understanding of requirements.
- Different types of media require different rules; for example, cloud-based systems cannot be handled in the same manner as on-premises data stores. Legacy data will have its own special challenges that may require a modified policy.
- Different departments will require different rules; don’t try to force a highly-regulated department, such as legal, to fit in the same box as customer service.
- Make sure the policy is inclusive and applies to everyone in the silo, including senior management.
- Ensure confidential information types (e.g. Intellectual property, HIPAA PCI, PII) stay confidential, and privileged data stays privileged.
- Don’t forget to educate the workforce about critical policies. This step is important to ensure maximum effectiveness and helps foster a culture of efficiency.

Consider establishing separate policy for a number of areas, including:

- Personal data vs. business data
- Legally-defined records (claims, personnel files, etc.) vs. ordinary business data
- Department requirements (HR and legal have more focus than maintenance, for instance)
- Organizational role of content creator (for example, broker-dealers are under an impressive weight of regulation, but an administrative assistant likely is not)
- Physical location of data for jurisdictional considerations (e.g. privacy laws in Europe vs. the United States)

Even though it is helpful to phase the rollout of policy, be sure to plan for all types of ESI storage, structured and unstructured; for example, the initial rollout may only address data going forward. However, it is essential to make the process flexible enough to address legacy systems, and to leave room for emerging technologies and future changes.

The most effective tool in maintaining an effective defensible deletion process is proactive enforcement and auditing. The best procedures and policies will do no good if they cannot be defended in a court of law. Check backup systems, retention policies and classification methodologies. Highlight areas that are non-compliant and address them with senior stakeholders, and don’t implement a policy without knowing how it will be policed, then audit that process on a regular basis.

Pitfalls to look out for

- Policies need to be flexible enough to grow
    - New technology, new areas (e.g. social, BYOD, smart phones, cloud) all may need their own rules
- Policy must be enforced
- Policy must be audited
- Stakeholder buy-in starts at the top
- An effective team working toward the same goals is essential
- Saving data outside the system – the ‘auto-delete’ problem – is a no-no
- Keep an effective work process – don’t make the policy so stifling that knowledgeable users will go outside the system to get their jobs done
- Implement effective education
- Encourage and enforce routine oversight

Conclusion

The goal of defensible deletion is to safeguard critical digital resources while maintaining effective responsiveness to legal, operational and compliance needs. If left unchecked, the electronically stored data created by today's organizations can clog systems, increase liability and make identifying critical information assets a challenge. While not an easy undertaking, the rewards from establishing an effective defensible deletion policy include more efficient business processes, improved litigation readiness and reduced risk for your organization.

Resources

The following organizations have very helpful publications and resources to help getting started.

- ARMA
- AIIM
- The Sedona Conference
- Information Governance Initiative
- InsideCounsel
- EDRM
- Sherpa Software

Marta Farensbach, Author

Marta oversees the development and growth of Sherpa's on-premises products for the Microsoft environment and is responsible for ensuring customer satisfaction. Since joining Sherpa in 2003, she has done extensive research on eDiscovery while expanding her expertise in litigation preparedness, compliance and content management. Prior to joining Sherpa Software, Marta oversaw the management of the information technology department for a leading logistics firm. During her tenure, Marta was instrumental in increasing profitability and efficiency of real-time data inventory reporting, while guiding the deployment of a number of web-based applications.

mfarensbach@sherpasoftware.com | 412.206.0005 x214