eDJ Group "Defensible Deletion" Series Topic Overview

By: Barry Murphy

With: Greg Buckles, Babs Deacon & Mikki Tomlinson

eDJGroup

Table of Contents

eDJGroup

Background

Throughout 2012, a not-so-new concept began to surface in earnest: deletion of information. eDJ's consultants have supported expiry initiatives for years, but until 2012 few corporate counsel and IT were ready to take responsibility for the potential consequences of expiring ESI that might turn out to be relevant to an evolving matter. This year brought a change of attitude to these initiatives. eDJ consultants have been involved in recent projects that have purged terabytes of non-record files and email.

In **eDJ's Spring 2012 Information Governance (IG)**[1] **survey** results, in which 52.8% of respondents reported having shared drive cleanup or migration projects underway – more than any other IG project mentioned in the survey. This statistic, combined with more and more client inquiries about data dissolution, made it clear that "defensible deletion" is one of the hottest IG topics currently and a priority for organizations in 2013. This report will provide an overview of defensible deletion and analyze some results of the **eDJ January 2013 Defensible Deletion** survey. We are excited to shed some light on this issue with the full results of eDJ's IG survey, below.

Defensible Deletion Gains Visibility

Defensible deletion is the disposal of information assets in a manner that an organization deems reasonable and carries out in good faith related to its knowledge management, regulatory, and legal requirements. Put simply, it is a process for deleting information in a manner that an organization confidently feels it can defend if challenged in litigation or regulatory action.

Deletion isn't just a nice corporate "housekeeping" idea; it is now a necessity due to the high growth rate forecast by business analysts. McKinsey Global Institute, for example, projects data to grow at 40% per year2 ; thus making it virtually impossible to effectively and economically store and manage organizational information without some form of culling.

Meanwhile, another strategy, "non-deletion" or "big data storage" is also gaining adherents. Anecdotal evidence suggests that some organizations want to keep information around indefinitely and use increasingly sophisticated

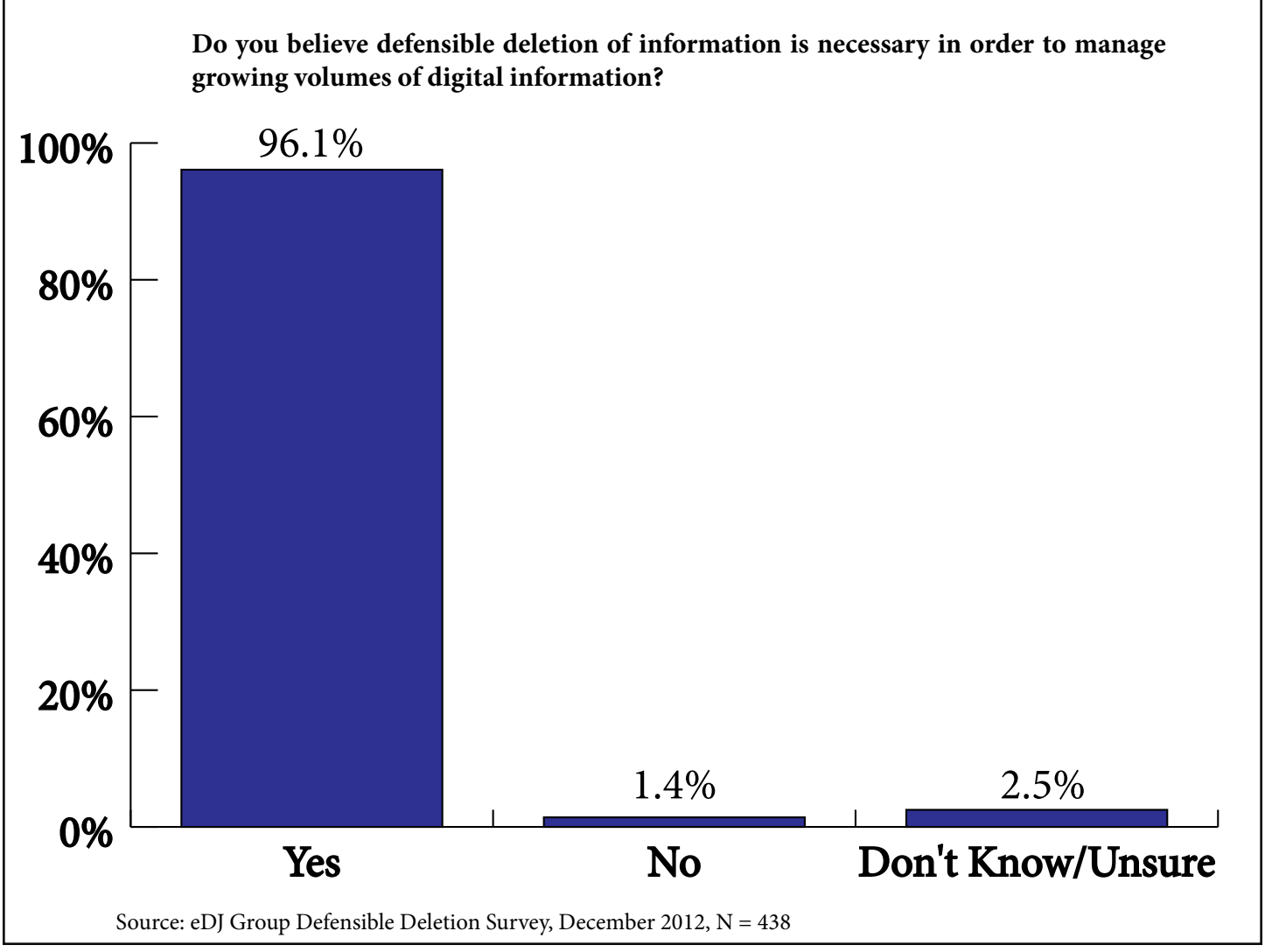
[1]eDJ Group defines IG as "Comprehensive program of controls, processes, and technologies designed to help organizations maximize the value of information assets while minimizing associated risks and costs."

[2]Big data: The next frontier for innovation, competition, and productivity. McKinsey Global Institute. Authors: James Manyika, Michael Chui, Brad Brown, Jacques Bughin, Richard Dobbs, Charles Roxburgh, Angela Hung Byers. May 2011. (http://www.mckinsey.com/insights/mgi/research/technology_and_innovation/big_data_the_next_frontier_for_innovation)

analytics software to automatically extract meaning and business value from it. While one could argue that the decreasing cost of storage combined with lower cost information processing platforms like Hadoop makes keeping information in perpetuity economically viable, it is important to remember that the cost and risk of eDiscovery can poke a giant hole in any economic assessment of information management costs.

In November and December 2012, eDJ surveyed over 430 IG professionals about defensible deletion. Overwhelmingly, respondents believe that defensible deletion is absolutely necessary in order to manage the growing volume of digital information.

Defensible Deletion is Absolutely Necessary



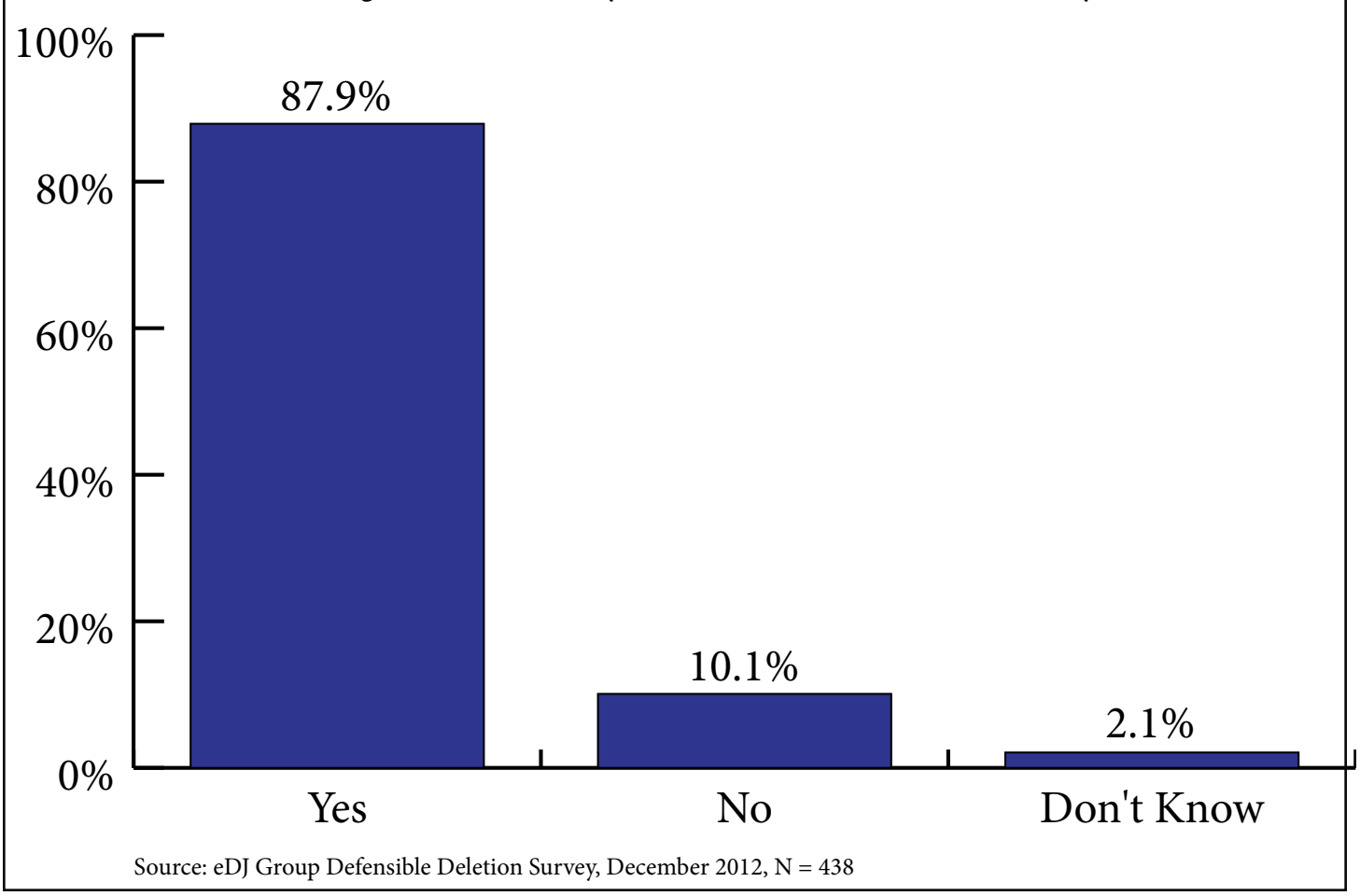
Source: eDJ Group Defensible Deletion Survey, December 2012, N = 438

This begs the question: if virtually everyone believes defensible deletion is necessary, are they actually doing it?

Current State of Defensible Deletion

The foundation for any defensible deletion program is a solid retention schedule that applies to all organizational information because any deletion needs to be conducted in accordance with standard operating procedures. Of the survey respondents, almost 90% indicated having such an information retention policy.

Virtually Every Organization has an Information Retention Policy

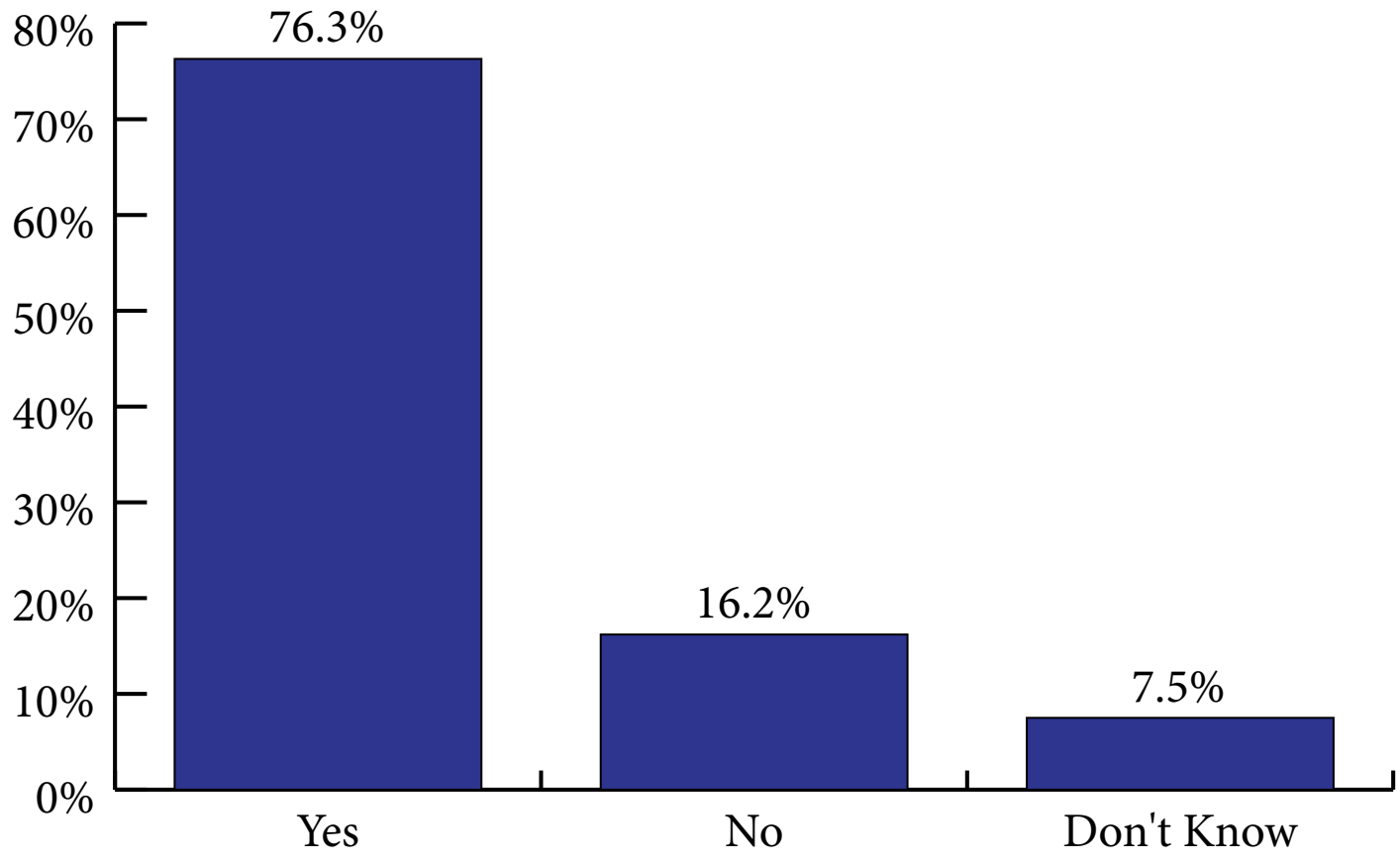


Source: eDJ Group Defensible Deletion Survey, December 2012, N = 438

For the most part, organizations have evolved retention policies from covering only paper-based records to applying to all information whether digital or paper. More than three-quarters of survey respondents indicated that retention policies now apply to all information.

Most Information Retention Policies Go Beyond Paper and Apply to Digital Information

If you have a retention policy, does your information retention policy cover digital information such as email, word processing documents, structured data, etc.?

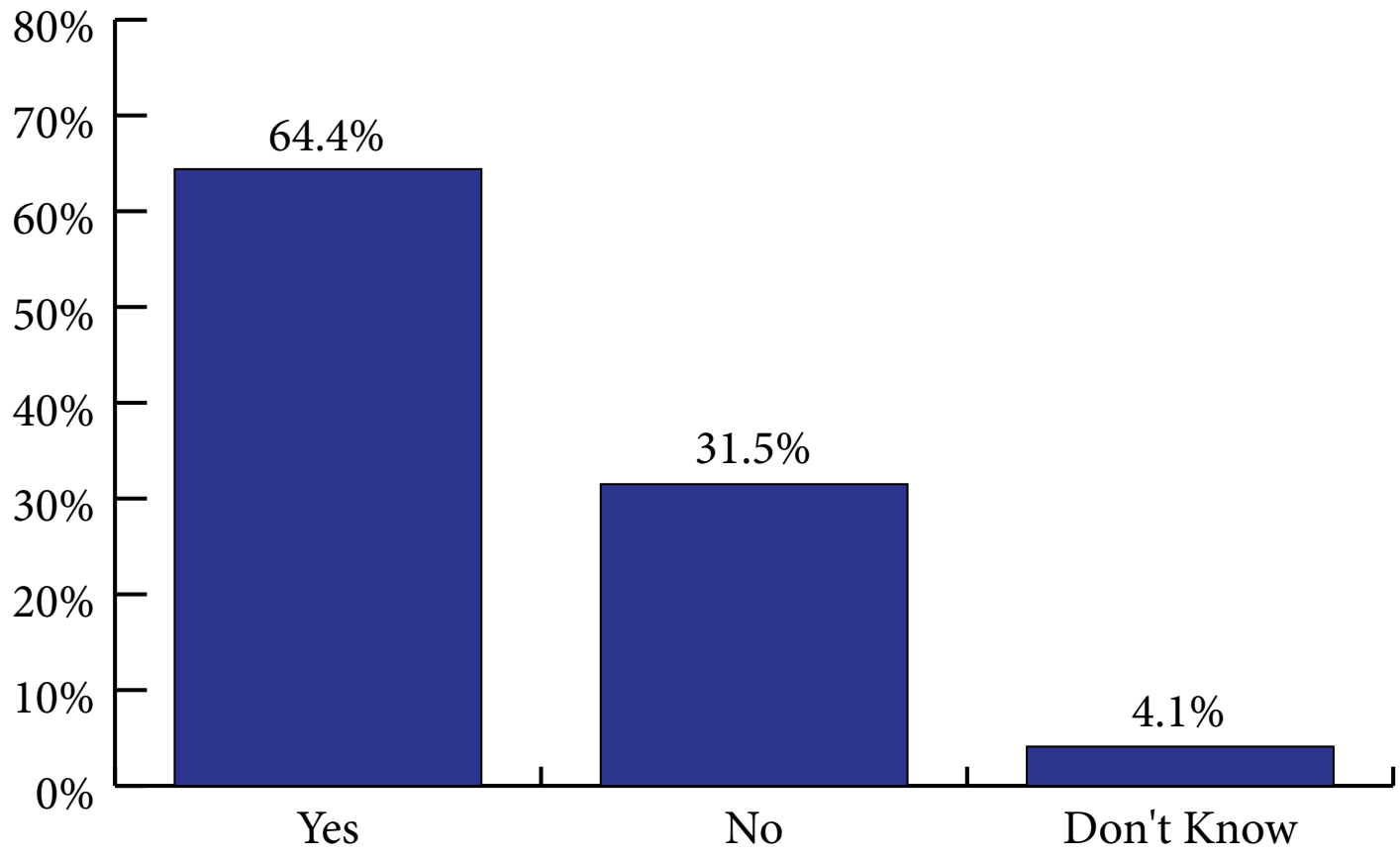


Source: eDJ Group Defensible Deletion Survey, December 2012, N = 438

A retention policy that applies to all information is a good start, but is not, by itself, enough to reduce risk. An organization that does not have a consistent, systematic process for enforcing its retention policies may as well not have a policy at all. While a significant percentage of survey respondents signal that retention policies are systematically enforced – 64.4% - it is somewhat alarming that almost a third of respondents do not enforce retention policies. This leaves those organizations with substantial risk for problems down the road should eDiscovery arise. Policy without process and documented compliance is potentially worse than no policy at all – the policy shows that the organization knew what it should be doing with ESI.

Majority of Organizations Report Enforcement of Retention Schedules

Does your organization currently have a systematic process (e.g. records management policies that are described and executed) to enforce your retention schedules?



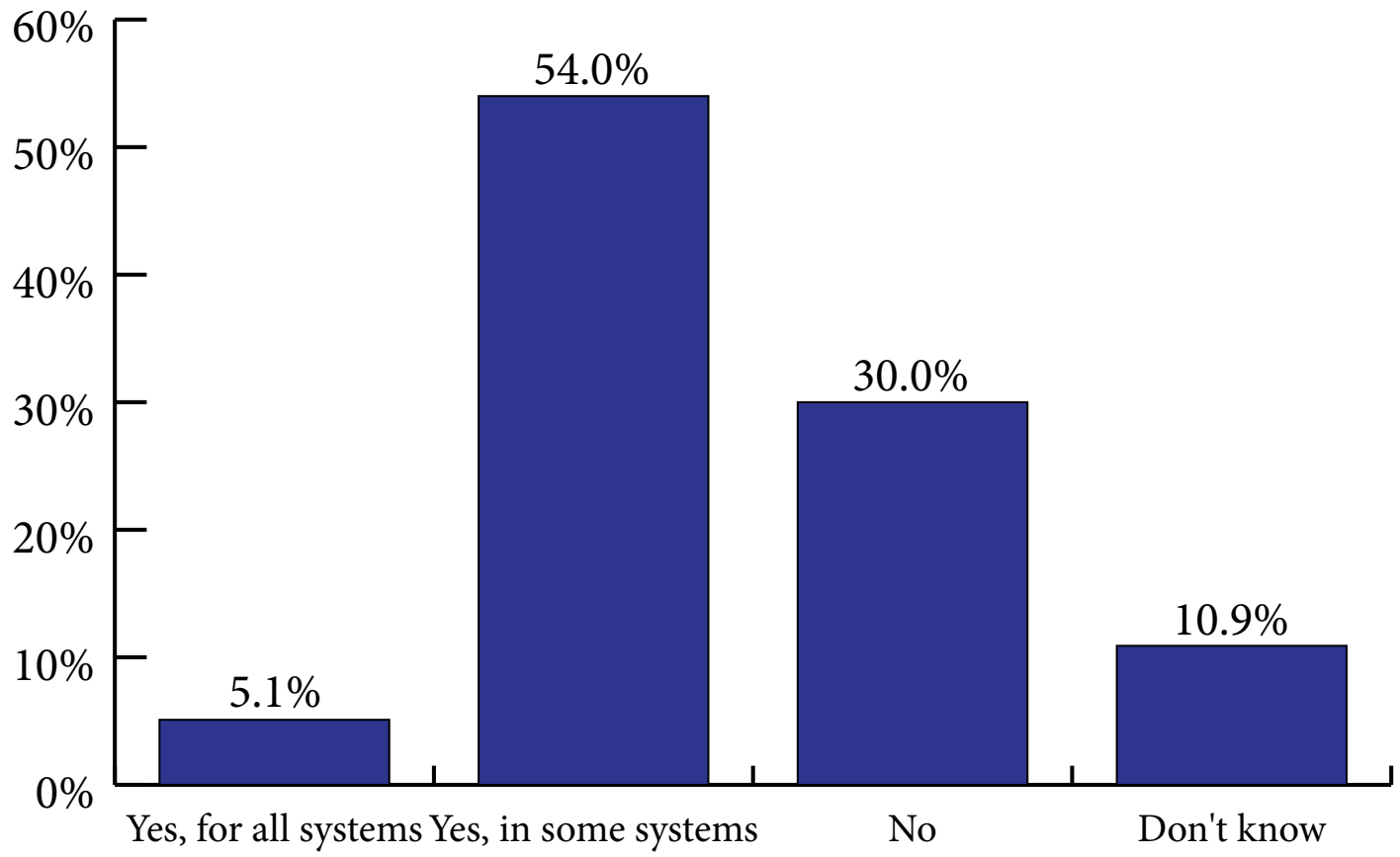
Source: eDJ Group Defensible Deletion Survey, December 2012, N = 438

Even if retention policies are systematically enforced, there is a question about just how consistently that enforcement is applied. Only 5% of respondents use technology to enforce retention policies across all organizational systems. Almost a third of respondents do not use technology at all for enforcing retention policies. Just over half use technology to enforce retention policies on some organizational systems. Keep in mind that the Federal Rules of Civil Procedure (FRCP) call for companies to make reasonable efforts to identify and produce information"… that is relevant to any party's claim or defense…",[3] including ESI. For many organizations, it may be perfectly reasonable to only use technology for enforcement of retention policies on a select number of systems. Each organization needs to make an assessment of what is reasonable for its given circumstances.

[3]FRCP Rule 26(b)(1)

Retention Policy Enforcement Not Always Supported by Technology

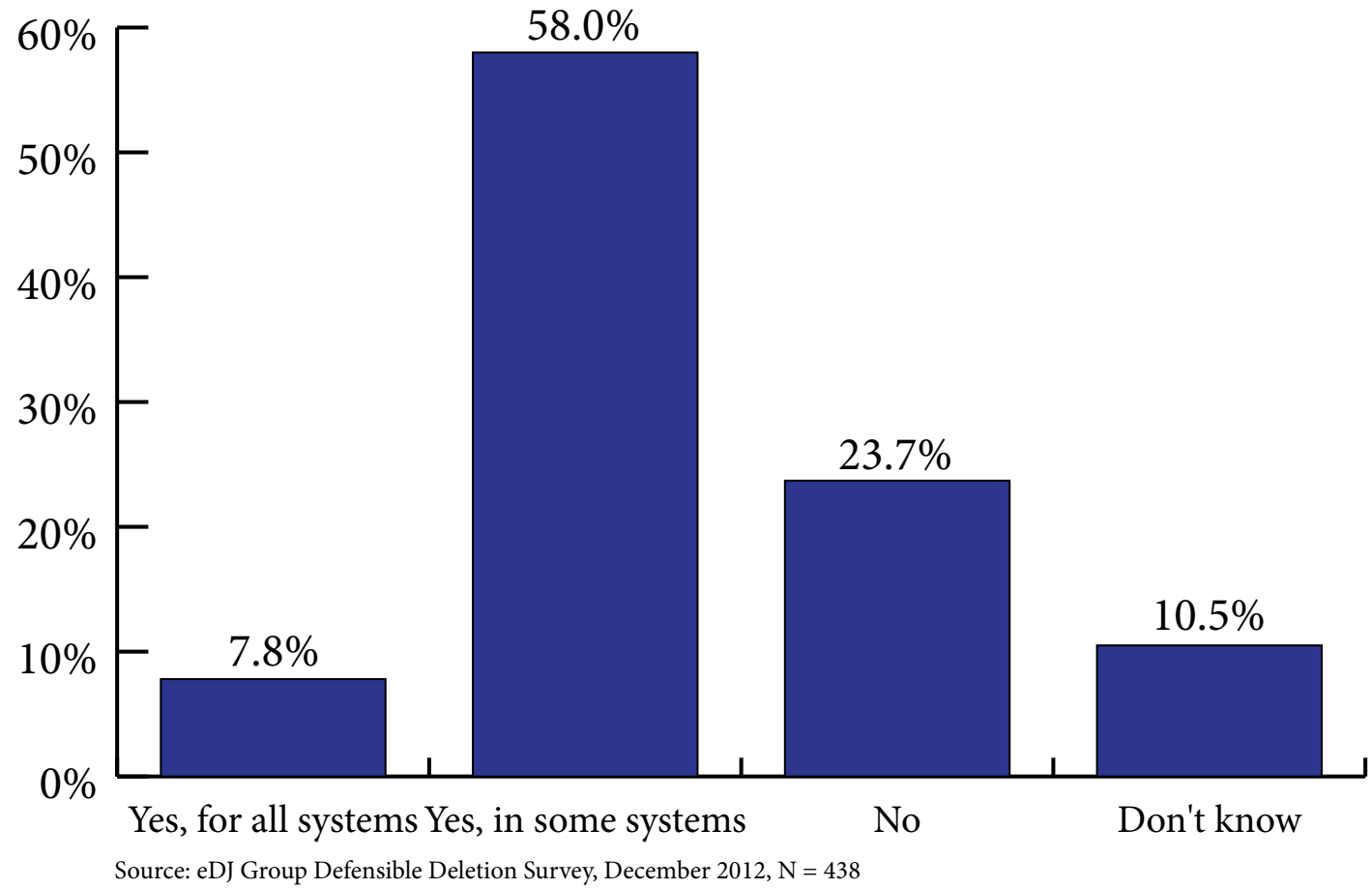
If enforcing retnetion policies, is this process supported by technology for enforcement (e.g. software to dispose of information after its retention period is up)?



Source: eDJ Group Defensible Deletion Survey, December 2012, N = 350

These statistics start to shed light on the current state of defensible deletion as 2013 kicks off. Many organizations report actually deleting information, but few (7.8%) do it across all systems. Almost 60% of survey respondents report defensibly deleting information in at least some systems.

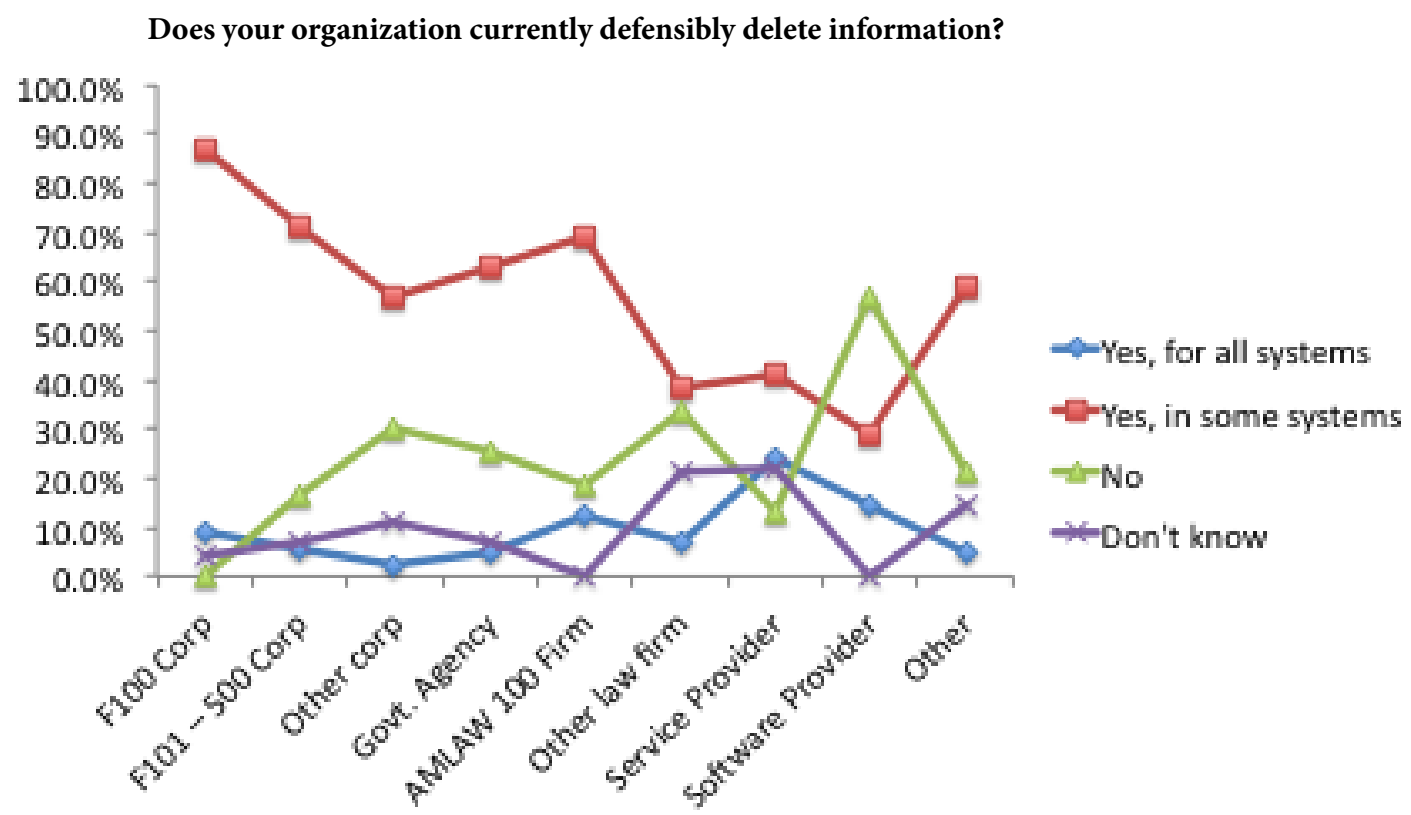
Defensible Deletion Occurs Sporadically Within Organizations



Source: eDJ Group Defensible Deletion Survey, December 2012, N = 438

This would indicate that the Big Data "keep everything forever" attitude is not as prevalent as some might think. This is especially true for companies that commonly experience litigation or regulatory action. Larger companies in the Fortune 100, which tend to be serial litigants, are much more active with defensible deletion. Not even one respondent from a Fortune 100 company reported having zero defensible deletion within the company. A full 87% indicated that defensible deletion is currently happening for at least some systems. For smaller companies like small law firms, service providers, and software providers, it was more likely that defensible deletion projects had yet to take hold.

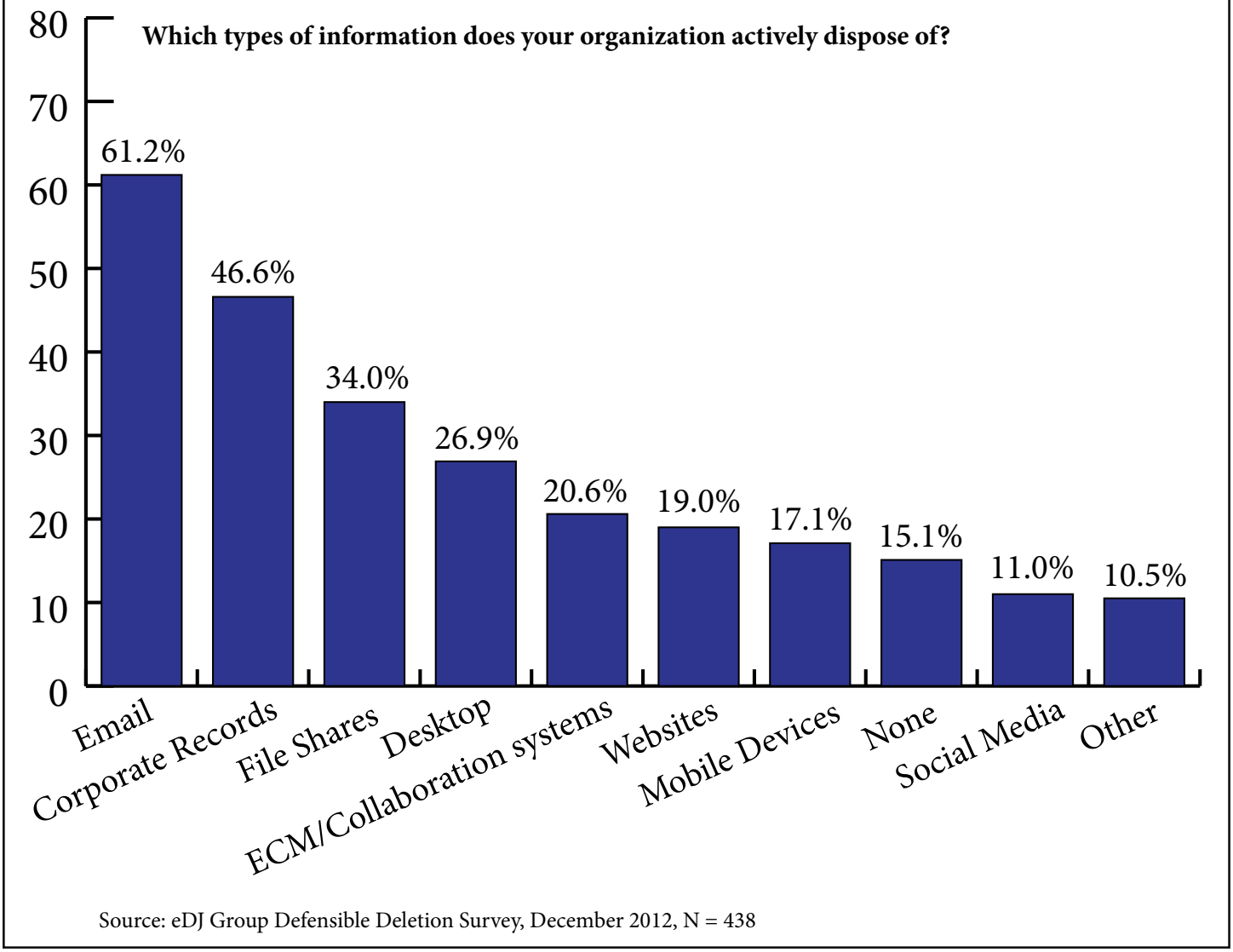
Larger Companies Tend to Have More Active Defensible Deletion Programs



Source: eDJ Group Defensible Deletion Survey, December 2012, N = 438

With so many organizations reporting deletion of information in at least some systems, it makes sense to understand which systems tend to be well managed and which ones may pose challenges and risks going forward. As expected, email is the most common system from which our respondents reported defensibly deleting data. This seems logical because estimates are that 95% of all organizational information travels through the email system and that it is the highest priority target for eDiscovery. In addition, email is a high-volume system containing enormous amounts of duplicate or unnecessary content. Getting rid of as much email as possible reduces both risk and cost. New sources of high-volume, user-generated content – mobile devices, social media, and websites – present a higher eDiscovery risk than more traditional forms of content because they exist outside the direct, hands-on control of the organization. Very few organizations are defensibly deleting information from these systems.

Email, Corporate Records and Fileshare Data Most Common Information Deleted



Source: eDJ Group Defensible Deletion Survey, December 2012, N = 438

There is the real possibility that these systems will become digital landfills in the way that email did a decade ago. So many of these new systems are Cloud based that it poses a serious risk that the organization will not be aware of this accumulation until it is tasked with preserving, collecting and reviewing for it for eDiscovery. That is why smart organizations are creating policies around these types of information and trying to get ahead of the curve before it is too late.

Moving Forward With Defensible Deletion

The threat of eDiscovery has already forced most large organizations to take IG seriously. The survey data shows that virtually all large companies are actively deleting information. Smaller and medium-sized organizations will need to get on the defensible deletion boat or risk having out-of-control eDiscovery costs down the road. Again,

the new Cloud solutions targeted at SMB actively encourage unlimited retention in users. A recent eDJ interview with a two year-old software company using entirely Cloud based infrastructure revealed email collections averaging 100 GB per user.

IG programs are broad and challenging. It is always best to focus on projects that are at least somewhat discrete and tenable, and defensible deletion is one such project. As organizations begin or evolve defensible deletion programs, here are some points to consider:

Be sure to have a formal, documented, and effective legal hold process in place on critical systems. The Legal Hold process is the foundation for defensibility and gives in-house Legal and outside counsel confidence that potentially relevant ESI has been preserved. The standard is 'reasonable effort' rather than 'perfection'. Third party consultants or auditors can support the diligence and reasonableness of these efforts.

- **Prioritize information for deletion.** Very few organizations are deleting information across all systems. It can be overly daunting to try to apply deletion to all enterprise information. Choosing the most important information sources – email, for example – and attacking those first may make for a reasonable and tenable approach.
  - Why email? Companies can fairly easily put systematic rules on email because the technology is already available to manage email in a sophisticated manner. Because it is such a critical data system, email providers and email archiving providers, early-0n, provided for systematic deletion or application of retention rules. However, in non-email systems, the retention and deletion features are less sophisticated; therefore, organizations do not systematically delete across all systems.

- **Strive for consistency.** While it may be necessary to attack information stores one at a time, the method of deletion will have to be consistent in the long run. An organization must review whether or not it has one retention policy for email and a different retention policy for file shares, for example. The end goal should be to retain information based on its content as opposed to its repository. Longer-term strategies should address information classification by content and ways to optimize how classification is applied.

- **Use multiple measures to initiate projects.** Every project needs a business case and defensible deletion is no exception. The good news is that defensible deletion can deliver multiple benefits. For the Legal team, there is reduced risk and potentially lower cost of eDiscovery. For the IT team, there is the benefit of lower storage costs and more manageable active systems. For users, there is less time spent looking through buckets of useless data to find the information "needle in a haystack". And, for the records manage / IG team (should it exist), the benefit is active compliance with organizational policies. It is critical that IT, Legal, IG, and business units work together to define defensible deletion requirements.

- **Centralized ownership of defensible deletion projects can help.** It is easy to say that IT, Legal and Records Management must work together, but getting the teams on the same page can be very challenging. Defensible deletion can provide benefit to all teams, but it is not necessarily the priority for Legal, IT or upper management. If a Records Management or IG team exists, that is when defensible deletion becomes a priority. Just over half of the respondents in the survey (50.6%) reported that a records or IG team was principally responsible for defensible deletion programs. Centralized management, with an agreement as to how project funds will be budgeted, can push projects forward while allowing Legal and IT to jointly participate, but not have the burden of project ownership.

About the eDJ Group:

eDJ Group offers unbiased information and pragmatic advice, based on years of experience and proven industry best practices. Whether researching a technology or service solution, conducting an eDiscovery Bootcamp or finding the right expertise to answer your specific questions, eDJ Group is the source for all eDiscovery professionals.

We are committed to helping eDiscovery professionals get the information necessary to excel in their professions, rather than offering legal advice or counsel. We operate with the utmost integrity and commitment to our clients on these guiding principles:

- Independence – All research, reports, advice and services are agnostic and conducted independently without influence by sponsors.
- Highest Ethical standards – All content is honest perspective based on real experience and interactions with thousands of practitioners; detailing both successes and failures without favoritism.
- Pragmatic, Experienced Expertise – All services are conducted by industry experts with decades of experience in eDiscovery and strictly vetted by the eDJ Group founders.

For further information about the eDJ Group and their research, please contact Barry Murphy (barry@edjgroupinc.com) or Jason Velasco (jason@edjgroupinc.com).