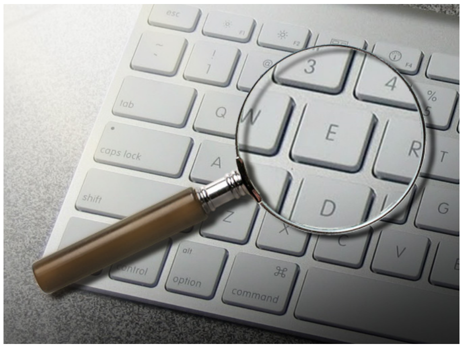
Eliminate eDiscovery Waste

Four reasons it's time to reconsider your eDiscovery environment

Overview

More than 50%[1] of companies claim inadequate eDiscovery capability, placing their businesses at significant risk and financial hardship according to Osterman conducted research. In this paper we will help you assess whether it’s time for your team to consider revising your approach to eDiscovery by reviewing four areas of eDiscovery waste.

50% of organizations believe that their eDiscovery capabilities are lacking.[1]



eDiscovery Pressures Heat Up

eDiscovery has become more challenging in recent years. In the last significant amendment to the Federal Rules of Civil Procedure (FRCP), which provides a legal framework to civil courts, the following two important points were added:

1) Electronic data is discoverable and,

2) The duty to begin preserving potentially relevant information starts when litigation can be reasonably anticipated

These changes to FRCP reflect the views of the Supreme Court that companies have a much higher level of control of their electronic information than previously expected. Herein lies the challenge: new technologies that create and store electronic information are in many cases outpacing the eDiscovery technology that can search, store and preserve them.

Osterman Research Shows Alarming Inefficiencies in eDiscovery

In partnership with Osterman Research, bluesource conducted a survey to find out how organizations rate their eDiscovery readiness. The survey consisted of more than 100 organizations with 500 or more employees mainly from regulated industries. The results were concerning. 50% of organizations believe that their eDiscovery capabilities are lacking.[1] Additionally, only 29% of the firms surveyed indicated that if they had to impose a litigation hold on social media content they could do so with confidence that all content would be held as long as necessary.[1]

[1] The Need for Better Archiving Solutions by Osterman Research

Four areas of eDiscovery waste that are addressable

Make sure your company has an eDiscovery process documented and if not, invest time now to avoid repeating the same mistakes in the future.

Waste #1 Time

When it comes to eDiscovery , many organizations take an all or nothing approach maintaining an overly broad collection process rather than a targeted one. Common sense dictates that the more electronically stored information (ESI) collected at the beginning of a matter, the more time is required to filter through it in the downstream eDiscovery process.

In the past it was common for IT departments to receive requests for restores of entire backups of servers, or disk images from workstation PCs throughout the organization. This was achievable when servers had 500 MB hard drives, but today backups run to multiple gigabytes or terabytes and this type of request only serves to create disruption and wasted effort. In reality, courts typically do not require parties to collect every shred of ESI as part of a defensible eDiscovery process, and organizations following this process are likely wasting significant amounts of time. Instead, organizations should be casting a narrow collection net at the beginning of a case rather than "over-collecting" more ESI than legally required.

There are a number of collection tools on the market today that enable the targeted collection of ESI from multiple data sources in an automated fashion through an organization's computer network. These are designed to limit the scope and size of the collection. For example a targeted collection can be limited to include particular custodians, certain file types or documents that result from a search term or date range.

Again, herein lies the challenge: the ESI collection tools are only as smart as the people who operate them. They will enable organizations to target collections effectively ONLY if they have an effective list of search terms that have been carefully crafted and tested.

Action: It is important that you create a collection team internally and collaborate with outside counsel if you have them. These teams need to follow a properly executed collection plan. Your internal collection team should include a discovery point person, preferably an attorney, and IT personnel. Outside counsel's team should include a supervising attorney, a project manager and a vendor (if one is to be used). This may seem like a lot of cooks to spoil the broth, but the more targeted the initial collection, and the fewer times you need to re-target your collection, the better. This streamlined approach will save your organization time without sacrificing legal defensibility or forensic soundness.

And don't forget to address what is perhaps the most common time waster: not having repeatable processes documented. Simply put, each time litigation strikes, the organization learns. If you don't document what is being acted upon the company is doomed to repeat the same mistakes. Although no two legal matters are the same there are recurring themes and patterns in many eDiscovery exercises, including for example what data lives where, who has ownership of that information, and how legal holds and releases were executed. The collection team will be more efficient if they have a process that they can follow.

Waste #2 Resources

In the same way that having an eDiscovery process can save time, an ongoing, routine and defensible data deletion processes can save resources (both human and technical). No organization, even if it is highly regulated, is under legal obligation to keep every piece of information generated or received.

Year after year companies accumulate electronic data, which in turn can drive up eDiscovery costs. Very few organizations have implemented ongoing, routine and defensible data deletion processes as a regular business process. Yet, if done intelligently, older information can be deleted without incurring any negative impact on the business.

Easier said then done? Maybe, but the challenge isn't entirely a technical one, in fact it's more of a methodology problem. It is easier to keep everything, even when it's wasteful. Yet just because it is easier, doesn't mean it is the right policy. The problem is that keeping things for too long, especially if they are no longer required, (e.g. Personal Health Information, or Personal Credit Information) can be just as risky as deleting them too soon.

Given the desire to delete data, how can this be done in a legally defensible manner? To be a defensible process, an organization must be able to demonstrate that it made a good faith effort to locate and protect any content that is subject to regulatory and legal retention rules. Any data that falls outside of these guidelines is a potential candidate for deletion. Before acting however, additional diligence is required. Organizations need to show by documenting reasonable policies, processes and technology that the data is indeed worthy of deletion. Lastly, before hitting the delete switch an organization will need to ensure that it has a lack of a duty to preserve deleted data at the time of disposal.

All companies can and should delete data on a routine basis.

One of the most important litigation requirements is that all potential parties, to an actual or anticipated lawsuit, find and secure all potentially relevant content with a legal hold – ensuring that spoliation (or evidence destruction) does not occur. Many older archive solutions do not allow for granular legal hold of content, requiring the entire archive to be put on hold until the discovery phase has passed. This is not desirable since only a small percentage of the archive may be relevant to a specific legal matter.

Action: If granular control is absent from your system you should consider migrating your archives to a system that allows a more targeted approach to legal hold.

Another common waste of resources stems from the belief that making a forensic copy or mirror images of every custodian hard drive is required to avoid spoliation.

This isn't required for most civil cases. Looking at Federal Rule of Civil Procedure 34 and case law help dispel the myth that forensic copies are required for most civil cases. The notes to Rule 34(a)(1) state that:

"Courts should guard against undue intrusiveness resulting from inspecting or testing such systems."

There is also a growing trend for respecting "proportionality" i.e. the amount of data that is to be preserved and the burden on the defendant to produce it should be proportional to what is at issue in the case. In fact, changes have been proposed for Federal Rule of Civil Procedure 26, which would require courts to consider "proportionality" when dealing with discovery issues. This amendment could become effective as early as 2015. Again, eDiscovery personnel should work with counsel to figure out what the burden of preservation for data in a matter is and look for a reasonable approach to limit unnecessarily preserving data.

No matter where your waste might be originating tested and documented defensible disposal processes can save valuable human and technology resources.

The median cost to review files collected for eDiscovery is $13,636 per GB.[2]

Waste #3 Money

Even large organizations with disciplined supply chain controls often fail to track and control spend on eDiscovery. Many eDiscovery costs are buried within individual matters, and little effort is made to identify the total eDiscovery costs separately from overall litigation spend, or use total spend to negotiate better rates with providers.

Tracking spend on eDiscovery can be as much an art as a science. The first stumbling block to cost control is that costs are often not recorded in a way that makes extracting any helpful data easy. Law firms send a bill with hours and itemized costs, and nothing more. Vendor invoices to the law firms are often similar. Therefore, reviewing lawyer bills is messy and takes time and energy – after all, allowing clients to track eDiscovery costs wasn't the goal of the attorney writing his time charges.

Action: a good project manager that understands legal processes should be able to track spending by looking at the underlying activities and compare it to industry norms or prior case experience. For example, if you know what the average per-custodian cost for ESI for a particular matter is, it should be possible to build a spreadsheet to budget for each activity and then cross compare the estimate with the outcome. Too different? Ask for a more detailed breakdown of the billing. Also there are now common billing codes used by many Legal Service Providers (UTBMS codes for example Uniform Task-Based Management System - LEDES - Legal Electronic Data Exchange Standard) that can be used for better tracking of costs. At the very minimum you should know what that average cost per custodian or cost per hosting GB with outside counsel or the average amount of data collected per custodian from which you can model.

[2] Where the Money Goes: Understanding Litigant Expenditures for Producing Electronic Discovery by RAND Institute for Civil Justice 2012

It's time to reconsider how your eDiscovery capabilities are managed. Good-bye eDiscovery waste. Hello efficiency.

Handing over the entire eDiscovery process to outside counsel in its entirety does not necessarily reduce risks, but certainly invites waste - especially if the case is complex or the amount of time before deposition is short. A better approach is to supplement document review with your in-house counsel so that they can continue to own and drive the strategy.

Waste #4 Opportunity

Our fourth waste is the most overlooked: opportunity. This last category has more to do with opportunities that may be open to organizations now or early on in the eDiscovery process. Of course learning from prior error is one way to avoid repeating the same mistakes – and documenting lessons learned mentioned previously. But here are three other concepts that can make a huge difference to the time, resources and money that organizations spend on eDiscovery.

Limit the scope of the eDiscovery request

When a subpoena or deposition motion is served the first step has to be a meeting of minds internally to figure out what can be done to limit the scope of the eDiscovery request. The first request from a plaintiff is always overly broad. Inside counsel and opponents will normally be encouraged by the courts to meet and confer to agree a more reasonable scope before eDiscovery takes place. Failing to negotiate on search terms and other limiting factors is a big opportunity wasted. Sometimes during the reactive firefight of litigation, companies fail to negotiate search terms with their opponent.

Action: it is critical that counsel come to those meetings prepared with concrete measures (such as phased discovery, limits on custodians or search terms, and privilege "claw back" agreements in case something privileged is inadvertently disclosed during the eDiscovery process) so that a concrete plan can be put into place. Finally, if all else fails and the opposing side is demanding unreasonable discovery, counsel should be prepared to provide the court with concrete evidence (including hard estimates of costs) showing that the discovery demanded by the opposing side is disproportionate and that costs should be shifted.

Decide early on whether outside help will be required

It is said that a great white shark can smell a single drop of blood in an Olympic-sized swimming pool and that they can detect blood from up to a mile away in the sea. Interestingly many outside eDiscovery vendors have the same acute sense when it comes to smelling panic. Some even have two pricing sheets -one set of lower prices that are for those companies not in a rush; the second set of higher prices is for companies who are in a rush and need to find a provider immediately.

Action: if you are going to need outside help, make that decision early so your vendor can be part of the early planning process and your organization can get the benefit of competitive pricing. Alternatively develop your in-house early case assessment practice so that you are less reliant upon outside help. And of course you can always use an outside vendor that will work with your in-house practice on a retainer basis with rates agreed in advance.

Plan for potential litigation – and educate employees

Under the Federal Rules of Civil Procedure (Rule 34), a party to litigation must produce any responsive electronic documents that are stored on devices under its control. An organization can be found to control devices that they do not own or physically possess – such as an employee's personal devices used to transmit or store company data. Technology even exists to audit and preserve social content since organizations are increasingly using social media such as Twitter, LinkedIn and Facebook to interact with their customers. Unfortunately, there is no single magic bullet that captures everything. As a result policies should be created, transmitted and understood widely to ensure that spoliation and other risk is limited. This is particularly important when considering a BYOD policy in which case companies should consider the type and volume of data that will be transmitted through the devices they will be supporting.

Action: a competent plan for litigation should be put in place and your employees should be notified about the potential for a litigation hold or collection procedure, should their devices become subject to eDiscovery. When creating a policy the following points are important: First, clarity; your organization must have sustainable, auditable and consistent messaging around social media content's reputational risk implications. Second, you should be able to verify that the policy has been received and understood. Lastly, boundaries on the reasonable expectation of privacy should be clear. And don't forget, policies without the ability to enforce them only creates more liability.

The four areas of common eDiscovery waste (time, money, resources and opportunity) can be draining on your organization. But once recognized there are many technologies and best practices that can be implemented to mitigate loss and reduce risk. The experts at bluesource are here to assist.

.

About bluesource

bluesource can help your organization address its compliance and legal discovery needs, leveraging the best-of-breed functionality in the industry's leading archive & eDiscovery solutions- Enterprise Vault and Clearwell eDiscovery Platform.

We work with a range of global organizations, enabling them to retain far greater ownership over corporate information, and providing a platform which removes the burden on IT departments of searching across the information estate.

Let us show you how to implement best practices, enable quicker response times and implement a full lifecycle case management solution that will stand up to court scrutiny. Contact us at sales@bluesource.net to set up your customized assessment.

Only qualified attorneys may provide legal advice. While we've done our best to include best practice guidance, this paper does not constitute legal advice.

bluesource US office
1900 Enchanted Way
Grapevine, Texas 76051
+1 817-328-6130

sales@bluesource.net **www.bluesource.net**