THE NEXT STEP IN EDRM

Five Essential Benefits from Coordinated Risk Management and E-Discovery

GUIDANCE SOFTWARE is now

opentext™

INTRODUCTION

With more – and broader – legal actions taking place every day, the coordination of risk management and e-discovery activities can improve an organization's processes, reduce costs, and shorten the e-discovery timeframe. While businesses in general have already begun to bring disparate applications together into more capable systems, this trend is also starting to influence the tasks and applications that support legal teams and law firms.

Risk management and e-discovery is a natural pair for combined use. The Electronic Discovery Reference Model (EDRM) clearly shows that these two functions are strongly linked in the volume phase of e-discovery, where the goal is to reduce the volume of information for a more streamlined relevance phase. E-discovery and risk management share common components that, when handled together, can simplify and improve the intelligence and processes of each.

Beyond the cost and time savings of coordinating risk management and e-discovery, doing so can:

- Improve compliance with key directives
- Improve an organization's position during litigation
- Enhance the consistency of EDRM activities in general

Here are five key benefits you can realize from coordinated risk management and e-discovery.

Minimize Unnecessary Data-Related Risks — Legally Defensible Retirement

Reduce the Volume of Discoverable Data

Data Privacy Protections & Retention Regulations for Non-U.S. Information

Save Time and Money with Auto Redaction

Improve E-Discovery Collections from Emerging Data Sources

MINIMIZE UNNECESSARY DATA-RELATED RISKS — LEGALLY DEFENSIBLE RETIREMENT

Pressure from litigation and legal hold processes has induced palpable fear among today's organizational managers, resulting in a natural reaction to "save everything" in order to avoid running afoul of retention requirements. The problem is often exacerbated by inconsistent implementation or a lack of clear policies dictating how and when to retire specific types of information. This issue has become even more complex as more relevant data exists at endpoints – including PCs, smartphones, and tablets. As a result, many organizations have huge backup databases on which to store information from end users' devices for potential litigation.

A risk management solution with automated remediation capabilities will help solve this problem with legally defensible retirement of unnecessary information. For example, if a specific type of information must be kept for six years, a risk management tool could read file metadata and automatically delete files that exceed this retention period. Keeping sensitive information, like credit card data and personally identifiable information (PII), beyond its business use can actually lead to regulatory non-compliance and fines. With the ability to systematically and legally retire information, it is equally important to retain the ability to create exceptions to automatic data deletion for situations when users may in fact need this information beyond its retention period.

By developing and deploying a capable risk management or e-discovery system to identify information that can be defensibly deleted, organizations can ensure consistent deletion with an approved system that meets applicable guidelines. This can minimize the potential for unwelcome surprises during discovery, such as files or folders overlooked during manual review or searches, and reduce the overall risk of data loss or theft and regulatory non-compliance.

REDUCE THE VOLUME OF DISCOVERABLE DATA

Potentially incriminating evidence or information is especially problematic when it surfaces during litigation, but if that information could have been defensibly deleted, organizations have nobody to blame but themselves.

More importantly, once an apparent "smoking gun" is found – no matter how irrelevant it actually is – opposing counsel may be encouraged to go "fishing" in the hopes of finding even more information during e-discovery that could further undercut an organization's position. This increases the scope of potentially relevant information, and can extend the e-discovery process, draining additional time and resources.

When aged data stands to reveal potentially damaging information, this is generally due to limited or nonexistent remediation policies and the lack of a capable system. Again, the problem is particularly common in organizations that save all records, even those past their retention periods. Ideally, defensible remediation or deletion should be systematic and based on pre-defined and approved processes. The ability to systematically delete obsolete data — which no longer has any business value — will not only improve operational efficiencies, storage costs, and business decisions, but reduce the overall volume of discoverable data that will have significant cost savings downstream.

DATA PRIVACY PROTECTIONS AND RETENTION REGULATIONS FOR NON-U.S. INFORMATION

In many cases, the discovery process can uncover private information located in other countries or originating outside of the United States. This can create serious problems if sensitive or personal information is disclosed or redacted in a manner that contravenes existing discovery-blocking statutes. Recent legislation in the EU, China, Mexico, and Russia has changed how private information can be transmitted to other countries. It is important that any e-discovery solution allows for the transfer and disclosure of private information in accordance with relevant statutes.

Most non-U.S. privacy regulations tend to focus on personally identifiable information. There is, however, an inherent conflict in the fundamental principles of the Federal Rules of Civil Procedure (FRCP) and the new EU General Data Protection Regulation (GDPR): FRCP generally believes that broad discovery is essential to getting to the heart of the matter, while the EU regulations tend to support greater personal privacy. The GDPR also introduces a number of detailed e-discovery obligations and restrictions. Pending adoption of the new EU-US Privacy Shield agreement also adds additional complexity. And it appears that new electronic data regulations are forthcoming in Japan, Hong Kong, Singapore, South Korea, and Taiwan.

If there is any chance of identifying and collecting personal information from outside the U.S., firms and counsel should ensure that this information has been classified – even removed or redacted – before producing it, avoiding the risk of improper disclosure. This is where coordinating risk management and e-discovery systems can provide real benefits.

We should also note that, in cases where discovery involves non-U.S. systems, differing applications or types of technologies are common. This makes it especially important to have a solution that can work with a variety of information storage platforms and across geographic boundaries.

SAVE TIME AND MONEY WITH AUTO REDACTION

When it comes to the unintentional disclosure of privileged or private information during e-discovery, pitfalls abound due to U.S. domestic statutes and an increasingly bewildering array of non-U.S. regulations. (These rules are typically more fluid in the Asia/Pacific and South American regions.) As a result, it can be costly and time-consuming to manage and redact privileged, confidential, or private information during e-discovery. Manual redaction in these cases is still common, despite the substantial resources it requires and the risk of human error. This makes a compelling case for automated redaction or remediation of privileged information. The ideal approach is to remove this information at the source, rather than simply masking it.

IMPROVE E-DISCOVERY COLLECTIONS FROM EMERGING DATA SOURCES

All electronic information must be available to support accurate e-discovery and risk management. To start, make sure that you can use these solutions — not only with enterprise information management (EIM) tools, corporate archives, and backups, but also with cloud, personal applications, endpoints, and remote systems. With the ever-increasing volume of organizational information — and less and less of that information residing in formal, centrally-managed systems — "blind spots" can lead to costly omissions in e-discovery.

E-discovery and risk management processes, then, must work together to discover and manage unstructured information in a substantial and varying number of applications and data types. This may include social media data, a great deal of emails, and many personal files relevant to litigation that are contained in unstructured data. The best practice for collecting this information is through the source or server-based information, rather than the end user's machine.

Personal applications, such as Gmail, may be within the scope of e-discovery depending on the nature of the litigation. In this example, it is better to access the data via the POP-3 email server than endpoint memory. This will require authorization. Many case precedents now allow for discovery within an individual's non-corporate email service or social media accounts. For example, in a recent case from Louisiana, *Shane v. Parish of Jefferson*[1], it was determined that, if accessed from the organization's system, emails from a private account are subject to disclosure. And Facebook posts and information relevant to the case became subject to disclosure during *Largent v. Reed*[2] in Pennsylvania. As more of these precedents are set, e-discovery solutions must possess the functionality to obtain it from the source or server.

Given the increased focus on unstructured data, risk management tools must similarly identify and manage the information stored within these applications in order to proactively and defensibly delete old, superseded, or sensitive information. Therefore, it is critical to have the ability to execute data retention policies across a wide range of applications without the fear of spoliation.

In addition, with more information residing in cloud applications and platforms, both e-discovery and risk management tools must be able to find, classify, and analyze information contained in all types of cloud infrastructure, including Amazon Web Services (AWS), Box, Dropbox, and Office 365. The ability to work with "cloud native" information is a key feature, as information in cloud services is unlikely to reside in any company-owned IT infrastructure.

GUIDANCE SOFTWARE'S SOLUTION FOR RISK MANAGEMENT AND E-DISCOVERY SUPPORT

Guidance is a leader in both e-discovery and risk management, with a client base that includes 75 of the Fortune 100 and nearly 20 years' experience providing software to support in-house attorneys and litigation support teams. In addition to e-discovery and risk management, Guidance offers forensics, endpoint security, and endpoint investigation software and services.

Guidance's EnForce Risk Manager provides a best-of-breed solution that helps organizations manage their most critical or sensitive business data. EnForce Risk Manager proactively identifies, classifies, and remediates sensitive and private data across any organization's enterprise. The automated remediation capabilities, used to remediate both sensitive and aged data, is unmatched in the industry.

The EnCase eDiscovery and EnCase eDiscovery Review solutions are based on advanced technology that allows users to leverage previous discovery work product to gain efficiency and accuracy with each litigation notice. EnCase eDiscovery provides three key benefits: early case assessment, robust automation, and unparalleled collections to help organizations gain a strategic advantage in the e-discovery workflow. EnCase eDiscovery and EnCase eDiscovery Review are complete end-to-end solutions that work across six key aspects of e-discovery:

- Legal hold
- Pre-collection analytics
- Collection and preservation
- Processing
- Review
- Production

SUMMARY

It is likely that your organization has already faced or will face litigation at some point. A recent study by *Norton, Rose, Fulbright*[3] shows that 55 percent of enterprises have more than five currently pending lawsuits, and more than 32 percent have 20 or more actions pending. It is, therefore, critical to adopt an e-discovery solution that will help you create and implement a repeatable and defensible in-house e-discovery process. Additionally, a risk management solution that can proactively manage your ESI data landscape will reduce or mitigate e-discovery risks and costs.

By coordinating risk management and e-discovery solutions, organizations can realize clear benefits. By viewing e-discovery through the lens of accurate and timely management and classification of sensitive and stale information, you can improve discovery and eliminate spurious data that may hinder how your organization responds to litigation.

[1] *Shane v. Parish of Jefferson,* 2015 La. LEXIS 2549 (Dec. 8, 2015) [case no. 2014-C-2225]
[2] *Largent v. Reed,* PICS Case No. 11-4463 (C.P. Franklin Nov. 8, 2011)
[3] http://www.nortonrosefulbright.com/files/20150514-2015-litigation-trends-survey_v24-128746.pdf

GUIDANCE SOFTWARE

ABOUT GUIDANCE

Guidance exists to turn chaos and the unknown into order and the known-so that companies and their customers can go about their daily lives as usual without worry or disruption, knowing their most valuable information is safe and secure. The makers of EnCase®, the gold standard in forensic security, Guidance provides a mission-critical foundation of market-leading applications that offer deep 360-degree visibility across all endpoints, devices and networks, allowing proactive identification and remediation of threats. From retail to financial institutions, our field-tested and court-proven solutions are deployed on an estimated 35 million endpoints at more than 70 of the Fortune 100 and hundreds of agencies worldwide, from beginning to endpoint.