

## Electronic Discovery: An Academic Exercise or Your Next Crisis?

Electronic discovery (or e-discovery) refers to the process by which relevant electronically stored information (ESI) is produced as evidence when an organization faces legal or regulatory action. Since the Federal Rules of Civil Procedure (FRCP) in the United States were amended in December 2006 to govern the discovery of ESI, attention has been drawn to the need for identifying and producing evidence in “good faith” and through “reasonable efforts.” These preservation and production processes must be defensible. If challenged, a litigant must be prepared to demonstrate that its policies, systems and procedures are sound in responding to three simple questions: Did you get everything, did you miss anything, and how do you know? These are not questions limited to the United States; we see evidence of similar issues in Canada, the United Kingdom and other countries.

These matters are important because parties in a lawsuit now can demand from each other word processing documents, e-mails, voice mails, instant messages, blogs, backup tapes and database files – essentially, everything. Failure to comply with these electronic production obligations can lead to serious sanctions – sometimes to the tune of millions of dollars – and increased compliance costs. The harsh consequences of noncompliance are growing exponentially. It is estimated that American businesses are spending more annually to locate, retrieve and produce required documents and ESI than for Sarbanes-Oxley compliance.

These requests also can span multiple geographies, ranging from desk files in Shanghai and Sydney to backup tapes in a Manila data center to financial data at a Beijing operations center. The challenge of responding to court-ordered evidence requests within a short period of time can present a logistical nightmare. This issue of *The Bulletin* provides ideas for companies to implement practical approaches in proportion to their litigation risk exposure and ongoing operations that will significantly reduce the cost, burden and time associated with records retention and e-discovery.

### Companies are not prepared

Whether companies realize it or not, they are now operating under a new set of e-discovery rules. Amendments

to the FRCP establish guidelines for e-discovery in civil suits brought to U.S. federal courts. State courts likely will be quick to adopt the federal rules, in whole or in part, as they seek solutions to difficulties posed by ESI. The amended rules, along with a host of high-profile e-discovery court cases, have placed discovery risk squarely on the corporate radar screen. Among other things, the amended rules (a) clarify the process for exchanging ESI among the parties to a dispute, (b) establish protocols for the involved parties and the court to address issues related to disclosure and e-discovery early in the litigation process, (c) address inadvertent waiver of privilege, and (d) create a safe harbor for the destruction of data under routine, good faith operations.

Note, however, that the safe harbor does not necessarily protect a company from every type of data loss or destruction. Whether a company’s data management and retention policy is reasonable or in good faith is always subject to challenge. More significantly, the safe harbor does not relieve any party of the burden of preserving ESI and related evidence when a legal dispute is likely. Therefore, a company must be able to quickly institute a “legal hold” as part of any routine data management and retention system. If the court determines that a company failed to preserve relevant data, or worse, deliberately destroyed evidence material to resolving a legal dispute, it could impose monetary penalties. The court also could determine that the missing data supports the opposition’s argument, which could seriously compromise the company’s legal position.

Without a doubt, e-discovery poses new challenges and opportunities for attorneys, their clients, technical advisors and the courts, as electronic information is collected, reviewed and produced during the pretrial process. Discovery risk must be placed in the proper context of the trends affecting the company. The issue of cost alone is eye-opening. Gartner’s *MarketScope for E-Discovery and Litigation Support Vendors*, published in 2007, concluded that spending on e-discovery software technologies and services offerings is forecasted to grow at more than 35 percent annually through 2011.

Raising awareness among executives and directors about e-discovery is important. Only 9 percent of respondents to the “2007 State of the Enterprise Content Management Industry” survey by AIIM, an enterprise content management association, reported being “very confident” when asked, “How confident are you that, if challenged, your organization could demonstrate that your electronic information is accurate, accessible and trustworthy?” In a CFO.com survey, 40 percent of respondents noted that information technology (IT) executives’ knowledge about compliance is not up-to-date. This could leave their corporations in peril if a federal agency were to request ESI during an investigation. In that same survey, more than one-third of the respondents reported they did not have a policy or technology system in place for dealing with a subpoena involving electronic records. This September 2006 survey was corroborated by another survey conducted at the same time by a trade organization, BPM Forum and a compliance software firm, which found that IT executives do not fully understand the new compliance regulations.

What is the point? When this issue arises, executive management typically learns all too late that their organizations are less than fully prepared to respond to discovery requests. By that time, the options for management are limited.

### What is e-discovery risk about?

Lawsuits and governmental investigations have been a reality in corporate America for a long time, and litigation is spreading around the globe. What is new is the changing legal landscape, which has dramatically raised the stakes for companies. Because of the virtual explosion of electronic data created in the normal course of business, discovery requests entail more costs and impose a higher level of risk than ever before.

Companies in every industry are vulnerable to the inherent risk that arises out of improper management of ESI and e-discovery. If the industry is highly regulated, the risk increases further as there is an increased possibility of regulatory inquiries. The vital signs of this issue are not difficult to spot. To name a few, the indicators include:

- Challenges dealing with backup tapes and e-mail
- The absence of a defined records retention policy (leading to “pack rat” retention behavior, where everything is kept)
- Increasing storage and retrieval costs
- Recent or ongoing investigations or litigation
- Adverse experience or outcomes in litigation or investigations
- Lack of defined roles and responsibility around keeping and deleting records

If the company has outdated policies and technology and is experiencing significant cost, time and burden associated with e-discovery, the operating inefficiencies alone may warrant adoption of a more proactive and process-based approach.

Understanding the dimensions of e-discovery risk begins with recognizing two things: The sheer volume of electronic information existing throughout the enterprise, combined

with an utter lack of cost-effective organization. The scope of e-discovery efforts can cast a massive net over potentially millions of documents throughout the company. The legal implications of this significant volume of information can drive up the costs, time and effort associated with preserving, handling, reviewing and producing ESI.

The challenge is exacerbated when a company does not have a records retention policy, and more than a few companies do not have one. Although there are companies with a comprehensive policy, a significant portion of them do not operationalize or enforce what they have. Which is worse: Having no policy at all or having one that is either not understood or not enforced?

Some companies purge hard-copy and electronic information after the expiration of a predetermined time limit. As noted earlier, so long as such activities are “routine” and are executed in “good faith,” a company will not be sanctioned by the courts. However, if the organization becomes aware of potential or actual litigation, it must preserve relevant information notwithstanding pre-existing retention policies. This issuance of a legal hold is not enough, as the company also must demonstrate that the hold is effective in operation. Not only that, but the hold also must be released at the proper time; otherwise, it becomes a vise-grip on the organization’s operations.

Some companies believe they can claim undue cost or burden to produce ESI. Sole reliance on this tactic is risky. Courts are not always sympathetic to a plea that a company lacks adequate financial, human or technical resources to comply. The argument always boils down to weighing the value of the information against the burden of production. If the court concludes the value of the evidence supports its production, it can demand results within a very short period of time. For example, after presenting an exhaustive argument as to why production of ESI was cost-prohibitive, one company was ordered by the judge to produce the documents within a few days shy of one month.

Getting it wrong when it comes to fulfilling ESI discovery obligations can result in costly sanctions and other penalties. A major software firm found this out when a judge ordered it to pay additional damages of \$25 million, as well as \$2 million in attorneys’ fees for litigation misconduct. A large wireless company was slapped with an \$8.5 million sanction for attorneys’ fees and other costs incurred by another party in litigation. An investment banking firm was fined \$2.5 million for a lax archiving process. A large consumer products company was penalized with a \$2.75 million sanction and denied admission of a witness at trial. Another firm lost a case due to the alleged destruction of electronic evidence, indicating that erasure of the wrong file or backup tape too soon can result in penalties imposed by the court. Such penalties can and have included forfeiture of the case itself.

Once collected, ESI can provide the transparency that hard-copy documents normally cannot. For example, metadata (“data about data” of any sort in any media) is a reality of the discovery process in today’s environment. In ESI, metadata shows the date an electronic document was created, as well as who authored it, and discloses previous versions and edits

to the electronic document. It may be found in virtually any type of electronic file, and may include pictures, video clips, documents or other types of digital files. The effective use of metadata can reveal information that was never intended to be disclosed by the author of a document, and can provide a formidable advantage to one side in litigation. Metadata can torpedo an otherwise ironclad legal argument.

### What needs to be done?

The time to learn whether your company has adequate e-discovery capabilities is not when faced with legal action or a regulatory inquiry. A good place to start is documenting and understanding the current state of the organization's records retention and e-discovery policy and process, discussing the risks with general counsel and the board, evaluating the appropriate "right-size" approach the company should have in place, and assessing whether appropriate training and awareness programs exist. These steps enable management to understand the key risks, identify control weaknesses and potential process improvements, and evaluate recommendations that would mitigate the risks around records retention and e-discovery. A fact-based understanding of the objectives and current state of the process is where it all begins, including the key factors influencing the organization's need to create and maintain administrative, legal, business and other records.

Following the policy and risk assessment, management should determine the key components to be included in the records retention policy and process. Following are examples of appropriate steps to accomplish this task:

- Review the defined job roles and responsibilities around records retention, with the purpose of determining whether they are articulated effectively
- Ascertain whether there is a common understanding within the organization as to what constitutes an "official record"
- Understand the reasoning behind current corporate policies dictating data retention requirements
- Using the documented current state of the process, obtain a perspective from general counsel and the chief compliance officer as to how existing records retention procedures should be applied in practice
- Review and assess current data classification protocols and guidelines, handling of e-mail and backup tapes, disposition and destruction controls and processes, and security and privacy considerations
- Review the applicable international standards (e.g., ISO 15489-1 and ISO 15489-2) and best practices

With respect to determining the key components that should be included in the e-discovery policy and process, following are examples of appropriate steps:

- Gain a baseline understanding of the legal function and supporting processes and related technologies
- Evaluate the ESI map and litigation-readiness plan
- Review the inventory of applicable software application profiles, and evaluate systems, technologies and tools

- Review the chain-of-custody template and evaluate a sample of completed requests
- Evaluate data retention and deletion procedures related to data placed on legal holds
- Review co-sourced or outsourced e-discovery functions

The above activities can help establish a framework for the organization's policy and provide a context for evaluating the current state process. Through these activities, management is in a position to compare existing practices (the current state) to the key components necessary to achieve process objectives (the desired state). An assessment of the current state also should include an evaluation of the organization's compliance with established record retention policies, including a review of data retention and purging procedures related to data placed on a "legal hold." Other considerations include: a review of the adequacy of the organization's training curriculum; an evaluation of how the current records retention process integrates into the overall business continuity and disaster recovery plans; a review of co-sourced or outsourced records retention functions; and an assessment of the adequacy of periodic monitoring, enforcement and internal auditing activities overseeing these functions.

The above review process requires the right mix of industry and subject-matter experience, compliance and governance expertise, and technology skills. It should leverage efforts already undertaken to assess, understand and document the organization's current records management practices and infrastructure. It also should consider the results of monitoring and testing program effectiveness pursuant to either an internal audit plan or a self-assessment program.

### What is the value proposition?

Through the above efforts, companies accomplish four things:

- They ensure compliance with internal policies and applicable legal and regulatory requirements.
- They establish defensible processes as part of routine operations and avoid excessive costs in responding to investigations, litigation and regulatory requests.
- They identify practical solutions that may result in significant cost savings in storage and retrieval.
- They minimize disruptions to operations while also creating more efficient ways for employees to create, use and dispose of data.

The operational efficiencies from a well-designed and effectively implemented records management program cannot be overemphasized. Taking action now can help companies to not only update their records management and retention policy and implement sustainable practices, but also to put in place the key elements of a litigation-readiness program in anticipation of, or in response to, lawsuits, regulatory actions and other business disputes. Implementation of a sustainable solution can reduce the cost, effort and time associated with e-discovery by as much as 65 percent to 85 percent, without increasing the risk profile.

## Five steps to take now

Here are five actionable steps executive management and directors can take now, if they have not done so already:

- (1) Become educated on records management and e-discovery risks. Have legal, IT and other subject-matter experts explain these risks to you.
- (2) Determine whether the organization has adequate, current, documented policies and procedures for records retention and e-discovery.
- (3) Consider the organization's records management risk profile as it relates to the frequency of lawsuits and/or regulatory investigations it can expect in the future.
- (4) Review the company's "legal hold" processes and capabilities and ensure that roles and responsibilities for records retention are defined and communicated clearly.
- (5) Perform a gap analysis to understand how current records retention capabilities compare to needed capabilities based on your risk profile.

## Deploy the internal audit function

Historically, the chief audit executive (CAE) has not considered discovery risk to be an integral part of the risk assessment that he or she assists management and the audit committee with completing. CAEs should consider their company's litigation and investigatory risk profile during the audit planning process

to ascertain whether to allocate audit resources to the monitoring of records management activities.

With its systematic, disciplined approach to assessing risks and the effectiveness and efficiency of a company's operations, internal audit is in a strong position to raise awareness of records management and e-discovery risks and ensure that both management and the board consider and take the necessary steps to mitigate them. Internal audit reviews that lead to improvements in the efficiency and effectiveness of the company's records retention and e-discovery policy and processes will help provide an even stronger basis for asserting defensible processes and routine operations under fire during litigation.

## Summary

General counsel and top-level executives must pay attention to the amended rules. The stakes are far too high for companies to scramble and sort through electronic information in the charged atmosphere of a pending lawsuit or regulatory investigation. A defensible and sustainable records retention process that is part of routine operations is best practice, particularly when it is designed to manage risk proactively in view of the organization's discovery risk profile. Even at companies where litigation or regulatory investigation activities may be unlikely, significant operational benefits can be realized through a cost-effective records and information management program. The potential benefits are certainly worth a close look.

# Key Questions to Ask

## Key questions for board members:

- Are you satisfied with the state of the company's litigation readiness? Does the company have the ability to establish defensible processes relative to its records retention practices embedded in routine operations, and to secure safe harbor, if any, under the applicable legislation in the event it is unable to produce electronic information pursuant to litigation or an investigation?
- Is the audit committee satisfied with the breadth of coverage of the internal audit plan of the organization's risks related to records retention and e-discovery? Is the audit plan's emphasis on compliance appropriate, regardless of jurisdiction? Are resources adequate to cover all critical risks requiring attention?

## Key questions for management:

- Do you have a records management and retention policy that addresses ESI?
- Are you aware that all electronic information created in your company is now potentially discoverable in litigation? Do you know if your backup tapes can be restored to produce information in litigation?
- Could you implement a comprehensive legal hold with little or no notice? Can you demonstrate that the hold is operationally effective?
- If challenged, can you readily demonstrate compliance with internal records management policies and applicable legal and regulatory requirements? Do you have the tools and expertise required to recover and produce potentially relevant and responsive e-mail sent to or received by the employees in your company?

Need help? Are you having to tackle the cost, time and burden of records management? Are you finding yourself reacting over and over again to the demands of litigation and investigations? Are you jumping from one fire drill of electronic discovery to another? Protiviti has the industry and subject-matter experience, compliance and governance expertise, and technology skills to assist you with your discovery risk management needs. For more information, contact Frank Wu at [frank.wu@protiviti.com](mailto:frank.wu@protiviti.com) or visit [www.protiviti.com](http://www.protiviti.com).