

PREPARE FOR ELECTRONIC DISCOVERY

ELECTRONIC DISCOVERY: IT'S IN YOUR FUTURE

With the exponential growth of e-mail as evidence, and the increasing sophistication of lawyers using electronic discovery as part of their litigation strategy, if you haven't received an electronic discovery request yet, you almost certainly will in the near future.

Over 90% of new corporate data is generated electronically, 70% of which is stored on disparate systems across the enterprise. Rule 26 of the Federal Rules of Civil Procedure (which regulate the production of evidence in litigation) explicitly requires that defendants provide "relevant" discovery information early in the litigation process — regardless of the information's format.

Despite the fact that an increasing percentage of major cases will involve electronic discovery, very few companies are properly prepared. Their inability to produce e-mail and other electronic records in a timely manner exposes them to potential fines, sanctions, and damage to their reputation — ultimately lowering their stock price and image in the marketplace.

Making matters worse, the more electronic information a company generates, the costlier it is to search through it. Discovery searches can cost \$1000 to \$2500 per backup tape and involve thousands of tapes. [Computer Forensics Inc. 2001]. A single search can quickly climb to seven figures. Companies that think they can avoid electronic discovery costs because they consider it an undue burden to restore "inaccessible" e-mails are in for a rude awakening. In *Zubulake v. UBS Warburg LLC*, the U.S. District Court of New York set a clear precedent that e-mail should be treated like any other "accessible" data to be produced in discovery, and therefore the producing party is responsible for the vast majority of the e-discovery costs.

For example, in a recent breach of contract case, 2003 WL22283835 (S.D.N.Y.), a leading financial service company requested that the plaintiff be required to bear half the costs of producing the electronic documents. The company argued that the documents at issue were deemed to be "inaccessible," as they were stored on optical disks and DLT tapes. Applying the *Zubulake* case cost-shifting test, the court found that cost shifting was not appropriate and ordered the company to bear its own costs — estimated at \$400,000 — to produce the electronic data.

How can your company react to a pending electronic discovery request in a timely manner to avoid sanctions and a loss of public trust? And, what proactive steps can you take to reduce the risks and costs of e-discovery in the future? This white paper provides recommendations on how to:

- Quickly and effectively restore evidentiary data for a pending request
- Establish an end-to-end process for capturing, archiving and organizing data to reduce your e-discovery risks and costs.

HOW TO BEST REACT TO IMMINENT ELECTRONIC DISCOVERY REQUESTS

Your company has just received a discovery request that includes all e-mails that reference a specific client from January 2001 through July 2003. Typically, the most onerous part of the discovery process is restoring thousands of backup tapes and making the data easily accessible for review. Here are recommendations on how to restore requested data quickly and effectively.

#1 — Understand the scope of data requirements

Define the parameters of the data gathering required to meet the discovery request. You will need to determine:

- Who are the specific employees affected?
- Are their specific e-mails or documents requested?
- What are the date boundaries?
- In what form does the data have to be produced?
- What systems did the affected employees use (such as e-mail servers and file servers)?
- Do you have the resources (hardware, software and staff) to rapidly restore the requested data from your backup tapes?

#2 — Locate the specific backup media you need to restore

The affected employees may have worked in different divisions in the time period covered by the discovery request. You should work with your Human Resources department to determine what divisions the affected employees were in at the time, so that you make sure you have identified the right backup media you need to restore. Create a master list that includes an itemization of the backup media that is required, where that media is presently located, and how you are going to consolidate all of the media.

#3 — Consider outsourcing the data restoration process

After completing the first two steps, you are likely to find that you need to restore from:

- Tapes in multiple formats (i.e., DAT & DLT)
- Optical media
- Numerous backup software environments (i.e., Tivoli, Arcserve, Netbackup)
- Three or more e-mail systems (i.e., Exchange 5.5, Windows 2000, Notes, CcMail)

If you are under a time constraint to restore the data, or you feel your IT staff can't execute this complex restoration and still manage their day jobs, you should know that Iron Mountain has extensive experience executing both small, straightforward data restoration projects as well as large, complex ones. We have securely and rapidly recovered critical e-mails, documents and other records in thousands of backup media — from a broad range of backup software applications and e-mail systems. Our service ensures that potentially relevant information such as e-mail attachments and important metadata are included. Most importantly, we have been able to produce the data in less than half the typical time and with dramatic savings — as much as 65%.

We can help you establish reasonable turnaround times with the regulatory agency or court. For example, if you have been requested to provide the production in thirty days, working with Iron Mountain, we can state as an independent third party, that the request is unrealistic and will require ten or more business days just to restore the data from backup tapes. The agency or court will generally accept this third party opinion for a more reasonable execution period. Plus, having your production executed by an independent third party increases the likelihood of admissibility of that data.

Here's another thing to consider. Like most companies, your backup tape environment probably has some level of corruption. There will be instances where data can't be restored from a corrupted backup tape. Iron Mountain has a well-defined, documented process for trying to restore e-mail off of corrupted backup tapes. If we determine that a tape is "unrecoverable", we will provide documentation that identifies the steps Iron Mountain took to reach this conclusion. Our Data Restoration Process Audit gives your legal teams an independent validation that every effort was made to restore the data on the corrupted tapes, but that this data could not be produced.

#4 — Make sure the data is not modified in any way

It is very important to make sure none of the metadata is modified during the gathering process. Simply copying information for the purpose of creating data sets may inadvertently change file metadata for the files. If you are working with Iron Mountain, our technology preserves the original file's metadata.

#5 — Organize the data for easy review

Many requests require you or your legal team to be able to search through the contents of the data, including attachments, to find specific names or other information. In order to be able to do this quickly and cost effectively all the restored data needs to be de-duplicated and indexed. Large production requests can involve thousands of backup tapes so you need to make sure that you have the tools for efficient extraction and de-duplication of hundreds of thousands of records.

Iron Mountain's Data Restoration and Electronic Discovery Support Service removes duplicates and indexes all the restored files. These files can then be securely stored in our highly scalable Digital Archives. Thanks to our sophisticated indexing and powerful search tools, you can locate and access restored e-mail, e-mail attachments and other e-records instantly from any Web browser, anytime.

#6 — Make sure your review environment is secure

Many companies learn the hard way that reviewers can unknowingly change or delete information. Simply opening a file for review can change the metadata. If your data is stored in our hosted Digital Archives, you can be assured that both your internal team and outside counsel can view it without being modified in any way. Our service even tracks and logs every interaction to provide a complete audit trail. You always know who has accessed the restored e-records, and when they accessed them. You can even setup multiple levels to define who has access to what information.

#7 — Ensure chain of custody

It's critical that you are able to guarantee the identity and the integrity of the electronic evidence from collection through production. The complete lifecycle of the electronic evidence must be documented. If you are using Iron Mountain's Data Restoration and Electronic Discovery Support Services, we can provide fully defensible chain-of-custody for you. After all, we have been providing data protection, recovery and chain-of-custody for backup media to businesses around the world for over 30 years.

Why You Need to Get Proactive with e-Discovery

Understanding how to efficiently react to e-discovery requests is only a short-term fix. If you have had an e-discovery event, you may be more at risk of having another request in the near future. If you don't proactively establish the right processes and archiving environment:

- Your company will have no idea what its legal exposure is from information lurking in backup tapes
- Each subsequent discovery event is probably going to cost you just as much as the first one

By implementing repeatable, reliable end-to-end processes and the proper archiving environment for discovery data you will be able to:

- Assess your legal exposure for a pending litigation event early in the process — potentially saving millions in settlement costs and production fees
- Reduce the costs of subsequent e-discovery requests by 30% or more

How to Get Proactive with e-Discovery to Reduce Risks and Costs

Here are Iron Mountain's recommendations on how to rapidly implement effective processes and archiving technology for your discovery data — without tying up all of your IT resources with non-core IT functions:

#1 — Form a records management team

Assemble a response team that includes legal, IT, records management, HR, outside counsel and your electronic discovery vendor. This team should be responsible for:

- Identifying what types of records have been or are likely to be requested
- Deciding what systems should be included in the discovery environment
- Defining the archiving system requirements
- Establishing the company's rapid response collection and review processes

#2 — Migrate records from backup tapes to a searchable archive

All key records identified by your records management team should be migrated from backup tapes to a searchable, Web-based archive repository. Potential discovery records that were virtually inaccessible on backup tape could now be accessed anytime, anywhere. This will allow your response team to respond quicker and more efficiently. Your team could assess your legal exposure at the first sign of pending litigation. The end result? You can save millions in settlement costs and electronic evidence fees. Plus, by selecting our Digital Archives outsource service, you can migrate records to a secure Web-based repository in a matter of weeks, instead of the months it might take to implement it internally.

#3 — Apply retention policies to e-mail

Applying corporate retention policies to e-mail and other electronic records can significantly diminish your company's litigation risk and lower your e-mail storage costs. By establishing a consistent e-mail retention policy across your organization you can ensure that the necessary e-mails are being retained and that the majority of e-mails, which are not official records, are purged on a regular basis.

Our e-record consulting services can show you how to implement a consistent, legally credible e-mail retention policy and our e-mail archiving service can provide complete Information Lifecycle Management (ILM) for all your organization's e-mail and other electronic records.

#4 — Automate the retention process for new discovery data

For collecting new discovery data, use enterprise records management software or services. New services such as Iron Mountain's enterprise e-mail management service collects e-mails and their attachments and archives them in a searchable, web-based repository that can be rapidly implemented — so you can be proactive.

#5 — Document everything

Document all the steps you take to create a more proactive discovery environment. When litigation events occur, log, tag and document everything to guarantee chain of custody. You should also have a formal e-mail policy so that employees understand the proper use of e-mail. This policy needs to be well documented and clearly communicated to all employees.

CONCLUSION

Electronic discovery risks and costs are not going away; in fact, they are very likely to only get worse. There are a number of steps your company can take the short term to react more effectively and over the long term to be more proactive. Iron Mountain can help you all along the way. Iron Mountain's outsourced services are the fastest way to reduce your company's litigation discovery risks and costs. Our full suite of services include:

- Data restoration from thousands of backup tapes delivered in any format you require — fast and with defensible chain of custody
- Data restoration from thousands of backup tapes archived into our searchable web-based Digital Archives platform — so you can respond faster, reduce attorney search and discovery fees and assess your exposure early in the process
- Automatic data collection and archiving of targeted employees e-mail into our searchable web-based Digital Archives service for proactive discovery risk management
- E-mail and electronic records management consulting that can show you how to apply your corporate retention schedule to e-mail and other electronic records — reducing e-mail storage costs and litigation risks

Be Better Prepared for Electronic Discovery — Contact us today.
Iron Mountain Information Management, Inc.

(800) 899 - IRON

digital_archives@ironmountain.com

www.ironmountain.com/digital