

UNDERSTANDING DATA RESTORATION IN TODAY'S COMPLEX REGULATORY ENVIRONMENT

BRIEF

CONTENTS

- Establish Policy and Enforce It
- Have a Process for Handling Electronic Discovery
- Courts Don't Care about Technology Complexity
- Dealing with Global Issues
- How to Move Forward

INTRODUCTION

Increasingly, electronically stored information (ESI) has become one of the primary sources of evidence in legal matters both large and small. Despite the fact that we have been storing information on electronic media for decades, the whole area of e-discovery continues to evolve.

While every firm may have variations on how they handle electronic discovery, there are some basic tenets that apply across the board. The challenge is to establish a framework in which electronic discovery disrupts business operations as little as possible, while still answering legal or regulatory requirements.

ESTABLISH POLICY AND ENFORCE IT

The first step is to establish a retention policy for ESI throughout the firm. This will need to be a joint effort between the legal department and the IT department; legal advises on the policy and IT implements the technology to support the policy. The common retention periods for paper documents – 7 to 10 years – also apply to ESI in most cases.

There is no standard for what a retention policy entails, but it needs to be defensible if challenged.

Having a policy that deletes all email older than 90 days is defensible, as long as that policy is enforced for all employees and can be shown to be a standard operating principle. These distinctions are critical to the integrity of a company's ESI policy and first steps need to be made to reach relevant goals.

Policy needs to take into account several questions, typically in this order:

- » What is required by law or regulation?
- » What is common practice for your industry?
- » What is reasonable from a technology and cost perspective?

This last point is the most troublesome, as it is a balancing act between recurring operating costs versus the potential cost of litigation or damages.

In the US, the Federal Rules of Civil Procedure were updated in 2006 to require that companies provide a “map” of how data moves through their organization. This is to be used by counsel to guide discovery and eliminate fishing expeditions for data.

HAVE A PROCESS FOR HANDLING ELECTRONIC DISCOVERY

Too often, companies stop planning after establishing a retention policy, missing the point of what it will take to protect and retrieve data when an electronic discovery event occurs.

Consider two issues. First, a discovery event is highly disruptive to normal IT operations. The same people who manage email, storage, and other IT services will have to stop their normal work to take on the discovery event. They may not have the expertise or facilities to meet the request in a timely fashion. Second, the discovery request may cover data on backup media from obsolete systems. The IT team may no longer have the hardware or software to read the media using normal processes.

A further complication may be that the discovery event requires data from multiple systems with different backup and retention approaches. For example, you may need to retrieve email, documents from file servers, or even information from collaboration systems like SharePoint. It is best to have a coordinating process or team that handles all possible sources of data.

Above all, the process needs to be explainable and defensible in court. Any doubt by opposing counsel or the judge hearing the case will only lead to more discovery and more data having to be produced.

COURTS DON'T CARE ABOUT TECHNOLOGY COMPLEXITY

In the past, technical complexity might have received some sympathy from the court; no longer. One of the most troublesome issues is that technology arrives and then disappears at a much faster rate than the legal requirements for data retention. This means that relevant ESI may be contained on media that can no longer be accessed by conventional means. Unfortunately, the courts are typically not sympathetic to such technical challenges.

DEALING WITH GLOBAL ISSUES

Global organizations have an even more difficult time with policy, process, and technology, given that law can vary from country to country. Too often, US based firms do not understand the limitations that other countries place upon access to data. For example, EU data privacy law has very strict limits on what kind of information can be disclosed or moved across borders. At times, the laws of one country may be in direct conflict with the laws of another, so handling a global discovery event is fraught with peril.

Often, IT services are not provided or managed globally, creating a web of different groups that may have to be involved in handling a discovery event. Differing processes and language can make a difficult process even more complicated.



HOW TO MOVE FORWARD

Given all these issues, how can one be ready to handle data restoration in the simplest way possible? This is an area where using a service from a trusted provider may be of the greatest benefit. The unpredictable nature of discovery events means that your business may not have the expertise or technology needed when those events occur.

A trusted partner will understand chain of custody, defensible processes, and how to assist counsel in meeting their needs. Asking IT to do the same is not their core competency and diverts resources from delivering to all parts of the business.

Technology and discovery will only become more complex in our increasingly electronic world. It makes the most sense to work with a partner who can understand your business and reduce your risk.

Policy needs to take into account several questions, typically in this order:

- » What is required by law or regulation?
- » What is common practice for your industry?
- » What is reasonable from a technology and cost perspective?



ABOUT IRON MOUNTAIN

About Iron Mountain Iron Mountain Incorporated (NYSE: IRM) is a leading provider of storage and information management services. The company's real estate network of over 67 million square feet across more than 1,000 facilities in 36 countries allows it to serve customers around the world. And its solutions for records management, data management, document management, data center management, and secure shredding help organizations to lower storage costs, comply with regulations, recover from disaster, and better use their information. Founded in 1951, Iron Mountain stores and protects billions of information assets, including business documents, backup tapes, electronic files, and medical data. Visit www.ironmountain.com for more information.

© 2015 Iron Mountain Incorporated. All rights reserved. Iron Mountain and the design of the mountain are registered trademarks of Iron Mountain Incorporated in the U.S. and other countries. All other trademarks and registered trademarks are the property of their respective owners.