

Managing E-Discovery Risks: What You Don't Know Can Hurt You!

Practical Steps for Risk Managers to Gain
Control of Electronically Stored Information
Before and During Litigation

REBEX Conference
October 24, 2008 11:30 a.m.
Fred Travis, Principal
Risk Management Consulting
Fred.travis@riskmanagementconsulting.net

Scope of the ESI Problem

- Thirty-six billion e-mails are sent worldwide on a daily basis; rising by 20% annually
- 93% of information is now held in a digital format
 - Seventy percent of that data is never printed
- Kroll Survey – 4th Qtr. 2007:
 - Only 25 percent of U.S. corporate in-house counsel claimed to be fully up to speed with all case-law developments and regulations relating to ESI
 - About half of the respondents said their organizations had a policy regarding ESI
 - 75 percent state they are losing time and money due to inefficient ESI processes

E-Discovery Challenges

- Locate relevant information;
- Preserve it and prevent it from being destroyed or modified;
- Collect it and convert it into a form that can be reviewed by attorneys;
- Have it reviewed by attorneys for relevance and privilege; and finally,
- Turn it over to opposing counsel, a court or regulator

Each of these steps poses problems and costs

ESI Spoilation & Sanctions

- Courts are holding companies accountable for ESI spoliation, and imposing severe penalties:
 - In 2004, a federal judge punished a company for deleting relevant e-mails by instructing the jury that the contents of the e-mails would have been favorable to the opposing party
- Failure to properly manage ESI can also result in increased litigation costs or regulatory penalties
 - A corporation will not be excused from the duty to preserve electronic evidence merely due to the size, complexity or expense of compliance

ESI Issues & Problems

- Volume of Electronic Communications:
 - Email; Instant Messaging; Web Groups; etc.
- Proliferation of Other Electronic Documents:
 - Personnel records; Scanned documents; Financial Records; etc.
- Inadequate ESI Retention protocols:
 - Category retention & destruction periods
 - Ineffective “Legal Hold” policies & procedures
 - Lack of Auditing, Assessment & Enforcement
- Inefficient ESI storage & retrieval systems
- **Key Issue: Lack of Planning**

Key Risk Management Questions About e-Discovery

- Does your company have full control over ESI in case of litigation?
- Who in your organization is accountable for ESI and e-Discovery? Who is actually working on it?
- Is your company prepared for e-Discovery?
 - Does your company have policies & procedures in place to deal with production of ESI when required?
 - Does your company have the ability to determine whether all relevant ESI has been located & produced?

RM Questions About ESI Controls & Assessments

- Has your company done an electronic data accessibility assessment?
- Is your company ready to answer your outside law firm's questions about ESI retention policies and IT environment?
- Does your company have ESI cost control measures in place?

ESI Risk Management Requirements

- Clear, Concise and Widely Disseminated ESI Strategy, Plans, Policies & Procedures
 - Understood & approved by In-house & Outside Counsel and IT
- Clear Designations of Accountability for ESI
- Regular Assessments & Audits of Compliance
- Periodic Measurement of ESI Volume & Number of Production Requests
- Adequate Budgets for ESI Retention, Retrieval, Compliance, Destruction, Training & Technology

Risk Management Steps for ESI Compliance

1. Develop an ESI compliance strategy NOW -- before litigation makes it necessary

- Select a task force comprising IT, Legal, Risk Management and a selection of key administrative & operations personnel to develop a strategy, policies and specific action plans
- Risk Management should separately work with IT and legal departments to identify potential legal, technical, technological and financial issues
- The strategy, policies and procedures must be communicated to, and approved by, Outside Counsel, Senior Management and/or the Board of Directors

Electronic Document Retention Policies & Procedures

- Company must Prepare for, Implement, Manage and Assess Compliance of Reasonable ESI Retention Policies and Procedures
 - There is no one-size-fits-all approach that will satisfy the needs of every company
 - Unless some legal duty requires an organization to preserve the information, systematic destruction of ESI is both desirable and defensible
 - The key is to recognize when it is necessary to retain ESI and to take the appropriate measures to preserve and produce it

Critical ESI Principles

1. An organization cannot keep all information it creates and receives.
2. Purging information on an ad hoc basis can create serious business and legal consequences.
3. Storing information is not the equivalent of managing it.
4. Locally stored electronic mail (PST or NSF) files create technology expense and pose an e-discovery challenge.
5. Information that is not readily accessible is of questionable value.
6. Information that is difficult to access can be a source of significant liability.
7. Disaster recovery is not records retention.
8. Disaster recovery tapes are not an appropriate place for retaining company records.
9. The more information an organization has, the harder it is to find what is needed, when it is needed.
10. Records responsive to discovery requests can be found in e-mail, blogs, instant messaging and voice mail.
11. Records are different than evidence.
12. Non-records or drafts of records may otherwise need to be produced even if they did not need to be retained initially.

ESI Risk Management Steps

2. Develop & Enforce Formal Document Retention Policies and Procedures That Include ESI data
 - The policy should clearly explain what information must be retained, and for how long; and what information must be deleted according to a regularly followed schedule

ESI Preservation

- All relevant ESI **must be preserved upon notice of litigation**
 - An attorney who is representing an opposing party may send a “litigation hold” letter that requires the company to preserve & continue to collect all related documents, including electronic data
- Company must preserve e-mails and other electronic data **when litigation is anticipated**
 - The duty to preserve material evidence arises not only during litigation, but also extends to that period prior to litigation when a company knew, **or reasonably should have known**, that the ESI might be relevant to anticipated litigation

ESI Risk Management Steps

3. Plan & Implement “Legal Hold” Policies & Procedures that:
 - Address information on all relevant systems and devices
 - Assure, to the extent possible and reasonable, that all relevant documents are found and secured
 - Train all affected personnel
 - Assess, review and audit compliance regularly

“Legal Hold” Policy & Procedures

- A “Legal Hold” retention policy must establish processes and procedures for preserving and producing documents, including ESI, relevant to current **and anticipated litigation**
 - At a minimum, the company must identify employees likely to possess relevant information and timely notify them of a “Legal Hold” situation
 - Those employees must be instructed to cease the deletion or destruction of relevant information, and to identify and preserve all relevant documents & records where they can be easily retrieved

“Legal Hold” Policy & Procedures

- Key: All personnel with access to or responsibility for company documents, including ESI, must be identified and provided guidance and training in Legal Hold policies and procedures
- When appropriate, Legal and Management must communicate a Legal Hold to all relevant personnel clearly, forcefully and promptly
 - Failure to do so will likely result in the loss of relevant documents, or the failure to identify all of them
- Risk Management and Legal should regularly review, assess and document the effectiveness of Legal Hold procedures

ESI Risk Management Steps

4. Develop Efficient Processes and Procedures for Complying With e-Discovery Production Requests

- Key: reasonable, defensible transparent process for compliance
- Establish procedures that clearly define where to look and how to look for relevant information
 - Make sure that all possible systems are noted

ESI Risk Management Steps

5. Reduce the ESI document universe:
 - Assure eligible ESI is deleted on schedule
 - Re-inspect existing storage for material that can – and should – be eliminated
 - Catalogue back-up tapes and equipment to assure all copies are purged
 - Audit procedures and processes frequently

ESI Risk Management Steps

6. Leverage existing document collections

- Monitor multiple cases & index discovery requests for similar items.
- Catalogue and reuse prior discovery material.

7. Train & Educate:

- Thoroughly train employees in ESI retention & destruction policies & procedures
- **Particularly emphasize their responsibilities to preserve unmodified all ESI on Legal Hold**

The Bottom Line

- Risk Management Must Take Ownership of This Issue to Create and Manage an ESI Team to:
 - Develop a strategy, policies and procedures
 - Obtain all necessary approvals from senior management and in-house & outside counsel
 - Enforce, assess, review and audit compliance
- Otherwise, your company will find itself at the sharp end of regulation
 - Unnecessarily at a disadvantage in legal proceedings
 - Potentially under threat of severe legal damages
 - Subject to high discovery costs

QUESTIONS?