Enterprise Vault & e-Discovery

Tim Faith
Attorney At Law

Agenda

- Implementing Symantec Enterprise Vault
- Customer Perspective on Use of the Vault
- e-Discovery in Maryland & Enterprise Vault

Bio

- Maryland Attorney, admitted to practice in 2008
- Director of IT department at Chase Brexton
- Worked in IT for over 10 years; implemented a number of enterprise applications for a busy Maryland health center
- http://www.faithatlaw.com
- (p) 410-963-5269, (e) tfaith75@gmail.com

Implementation

- Implemented in 2008 at CBHS for 200 users/ 350 mailboxes on Exchange 2003
- Migrated about 20 GB of .pst files
- Substantially reduced overall mail box size for our key users
- Generally a successful project for our organization

Implementation (2)

- Installed dedicated server for Enterprise Vault in our VM environment; separate virtual disks for data storage and indexing
- Configured policies for mailbox archive, retention periods, schedule
- Also implemented file server archive process, pst migration tool

Customer Perspective

- Enterprise Vault is a reliable information system
- Integrates with Exchange and Outlook so you really can't tell it is in use
- Provides a useful search engine for archived mail, files
- Addresses space problems for Exchange servers

e-Discovery in Maryland

- Maryland Rules were amended in 2008 to address e-discovery
- Maryland Rules follow the more aggressive federal rules for discovery of electronic materials
- Enterprise Vault can help to comply with discovery requests during litigation

Big Picture

- Maryland Rules on e-discovery are broader than just email
- Need to analyze what electronic systems are in use, and how to ensure compliance with potential discovery requests
- Enterprise Vault is part of a solution, but you may need additional tools to produce e-documents

Thought Experiment

- Consider all the information systems in your organization
- Consider the number of computer systems, backup tapes, and other media where information can be stored
- Consider the procedures for backing up data, retaining copies, and the locations of those backup copies

Thought Experiment (2)

- How do you stop the deletion of data that may be relevant to a potential case?
- How do you gather up all the copies of data that might be relevant to a case?
- How will you review this data to determine if relevant?
- How will you extract and provide this data to the other side if requested via discovery?

Discovery in Litigation

- Litigation begins with complaint, but you may need to identify the point in time when you could "reasonably anticipate" that litigation would ensue
- Parties have the right to "discover" information from each other to support claims or defenses
- Discovery can include depositions, interrogatories, and production of documents

Discovery

- Discovery requests need to be honored or you risk sanctions
- A party cannot discover privileged documents, and must show substantial need if seeking "work product"
- Orders by the trial judge on discovery are almost never appealable, so you are at the mercy of the court and should proceed accordingly

Attorney's Role

- Attorneys for the parties may agree at scheduling order what keywords will be searched to identify relevant electronic documents

- Responding attorney to review the relevant documents before turning them over - or - claw back agreement if privileged document turned over unintentionally to other side

- Ensure compliance with discovery requests

"Electronically Stored Information"

- Rule 2-402 allows for discovery of electronically stored information
- Committee note clarifies that this phrase encompasses, without exception, whatever is stored electronically
- 2-402(b)(2) allows for not producing digital documents that would cost substantially more than their value, but tough to win this argument (and if lost, not likely appealable)

Responding to Requests

- Objectives for responding to e-discovery are:
  - ✳return reasonably related documents requested,
  - ✳do not turn over privileged documents,
  - ✳make a good faith effort to respond to discovery requests, and
  - ✳avoid sanctions

"Litigation Hold"

- Know or should have known of potential litigation - point in time to preserve documents
- Litigation hold procedures to prevent the destruction of potentially relevant documents
- Follow-up by counsel to ensure that data not subsequently lost to litigation hold - potentially via a technology solution
- Susceptible to sanctions for not complying

Lessons from Litigation

- Don't certify a discovery response if there are more backup tapes to produce (*Coleman v. Morgan Stanley*)

- No undue burden to retrieve files on active hard drives (*Zubulake v. UBS*)

- Instant messages can be discovered from a non-party IM service provider (*Flagg v. City of Detroit*)

Lessons Learned (2)

- Don't maintain an endless array of backup tapes - have a policy on data retention
- Suspend data retention policy, however, if litigation hold in place for certain users or datasets
- Courts are not sympathetic to the fact that e-discovery can be expensive, but if unduly expensive, may be able to shift costs to other side

Sanctions

- Rule 2-433 provides for serious sanctions for not responding to discovery requests or acting in bad faith
- Includes "game over" on facts or claims, attorney's fees, monetary sanctions