

Reduce the Risk of Sanctions with Effective Media Management

Recent court rulings, such as *Zubulake v. UBS Warburg*, have highlighted the consequences organizations face when they cannot answer the simple question, “Where is my data?”

E-mail server backup tapes were central to this case. UBS said 94 tapes were relevant, but when ordered to produce the information, they were only able to find 87¹. In this case, the defense faced sanctions for spoliation (spoilage of the evidence). UBS Warburg was not able to locate all of the relevant backup tapes when they needed them. These lost tapes ultimately contributed to Ms. Zubulake being awarded \$29 million. As a result, organizations involved in litigation must not only defend their innocence—they must also ensure that lost tapes don’t ruin their defense.

Amendments to the Federal Rules of Civil Procedure

While some cases are extreme examples, organizations are continuously threatened by sanctions for inadvertent destruction of evidence. In response, the Federal Judiciary Committee amended Rule 37 of the FRCP to provide courts and litigators with some guidance regarding relevant sanctions. Rule 37(f) was added such that, **“absent exceptional circumstances, a court may not impose sanctions under these rules on a party for failing to provide electronically stored information lost as a result of the routine, good-faith operation of an electronic information system.”**

Over two years later, companies are still interpreting this amendment in an effort to avoid costly sanctions.

The amendment is not a license to ignore preservation orders, but simply a means of protection in the event that a routine operation opens the door for sanctions. It is now a question of what are “good-faith operations of an electronic information system?” Even under the amended rules, UBS Warburg could have benefited from a more effective media management strategy. CommVault® Simpana® software offers a variety of solutions that improve media management, including the Vault Tracker® feature: an integrated mechanism for tracking tape media through its entire lifecycle of creation, copy, transit, offsite storage, rotation, and ultimate retirement.

A Typical Discovery Scenario

Customer Challenge: An organization needs to produce the e-mail and files for five people for a span of 6 months, 2 years ago. The organization archives monthly full backups for 36 months to an offsite facility.

The Current Way: The organization’s archival retention policy requires that they maintain monthly full backups for three years. At the end of the cycle, the tapes are physically destroyed. Each system is backed up in accordance with the stated retention policy, 1 full copy onsite, and 35 months offsite. At the end of the month, an operator will eject the monthly tapes from libraries, record the media in a spreadsheet, label the container and schedule it to be sent offsite. In response to the discovery request, the operator looks to the spreadsheet and requests the six boxes from two years ago. The operator then sorts through each of the boxes using the spreadsheet to find the relevant tapes. Unfortunately, the spreadsheet only has dates and serial numbers. It does not contain tape content information such as associated servers, databases, mailboxes, etc. It also does not explain why the mail server tapes for January 2005 are not in the container. This organization has documented a policy, created and followed a process, and rigorously documented each of the tapes that were sent offsite. Yet, the restore process is time consuming and error prone and the tapes used in the January 2005 DR tests apparently never made their way back to offsite storage. Is this information lost as a result of the “routine, good-faith operation of an electronic information system?” Only the courts can decide. Wouldn’t you rather eliminate the risk?

The Better Way: CommVault Simpana software provides simple yet holistic data management, from the time the data is backed up to the time it is ultimately destroyed. CommVault Simpana software can:

- Logically group application data into Storage Policies
- Organize copy and retention policies based on business applications vs. server names
- Browse for backup sets regardless of when they were created or where their media is located using the CommVault software’s distributed indexing scheme

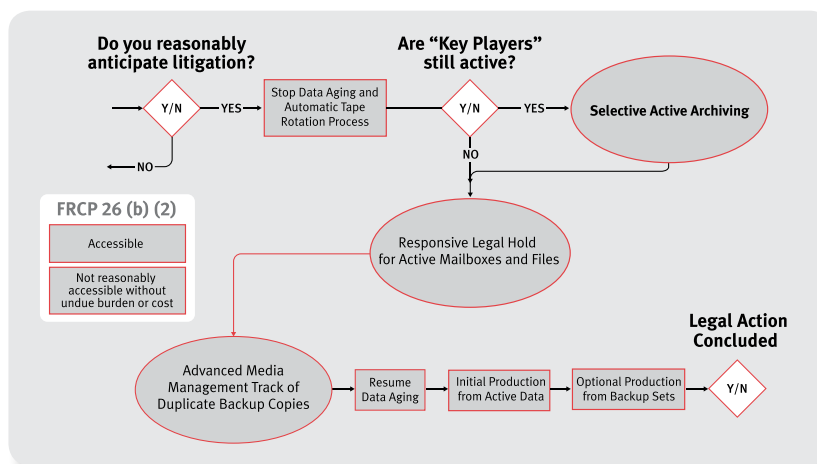
¹. *Zubulake v. UBS Warburg*, (“Zubulake IV”) 220 F.R.D. 212 (S.D.N.Y. 2003).



Rule 37.

Failure to Make Disclosures or Cooperate in Discovery; Sanctions

(f) Electronically stored information. Absent exceptional circumstances, a court may not impose sanctions under these rules on a party for failing to provide electronically stored information lost as a result of the routine, good-faith operation of an electronic information system.



Legal Action Workflow

- **Encrypt sensitive customer information before it is sent offsite**
- **Ensure data integrity through regularly rescheduled data verification processes**
- **Audit and report on the entire process with a powerful, integrated, wizard driven reporting infrastructure**
- **Track the location of removable media, manage library slots for easy media access, prompt for media rotation to ensure compliance with policies, manage foreign tapes, track by container and shelf, report on associated data sets and servers, and automate the rotation of media back on-site for reuse and retirement with Vault Tracker**

In short, CommVault Simpana software automates data protection and tape tracking to eliminate spreadsheets, lower administrative overhead, increase reporting and auditing capabilities and drastically reduce the risk of lost media. Even with the "Safe Harbor" afforded by the additions to FRCP Rule 37, organizations have little room for error. The legal discovery market leads you to believe that success in legal discovery is all about search and review strategies. While these are both critical to reducing costs related to review, they are irrelevant if you cannot find your tapes.

Conclusion

CommVault® Simpana® software is the only product that delivers file, e-mail and document management across replication, backup and archive data as part of a proven and unified data management solution. CommVault software's unique, single architecture reduces the amount of data repositories that need to be searched in response to litigation. From a single console, meet eDiscovery and compliance challenges with powerful search, retrieval and management of all ESI.

For more information on CommVault eDiscovery:

www.commvault.com/ediscovery

Get the facts: http://www.uscourts.gov/rules/EDiscovery_w_Notes.pdf

This information is not intended to be legal advice; customers should consult their own attorneys for an interpretation of the rules and requirements applicable to the subject matter hereof.



www.commvault.com ■ 888.746.3849 ■ E-mail: info@commvault.com

CommVault Worldwide Headquarters ■ 2 Crescent Place ■ Oceanport, NJ 07757 ■ 888-746-3849 ■ Fax: 732-870-4525

CommVault Regional Offices: United States ■ Europe ■ Middle East & Africa ■ Asia-Pacific ■ Latin America & Caribbean ■ Canada ■ India ■ Oceania