



Data Retention during Bankruptcy

By Richard Rupp
Director, Repository Services

During bankruptcy, many of the operational demands of Chapter 11 go against formal data retention policies. Normally, corporate backup policies are designed to save the incremental changes within files on certain computers on a daily basis. These backup tapes are retained for a certain period, usually a month, and then re-used. Monthly backup tapes may be kept for a number of years before they are re-used.

There are two major problems with this type of backup strategy when you need to preserve data in Chapter 11:

- By recycling tapes, you are destroying the backed-up information on those tapes. There may be many relevant files or email messages that exist for a few days, and are thus only captured on a few backup tapes. This data will be lost.
- A typical backup copy saves the data that is in the files on the computer. There is additional data in:
 - Deleted files
 - The space between the data in the file, and the end of the disk space allocated to that file
 - Free space on the disk drive that was previously used by deleted files ("emptying the recycle bin")

A "forensic backup" is necessary to save this additional data. It takes more time, and requires special software, hardware and expertise, but it is the only way to fully save ALL information on a computer system. Anytime a forensic backup is taken, it is prudent that two copies of the backup be made. Backup tapes or disks can easily be damaged or go bad. The second copy of the backup should be stored in a physically different location than the first.

Why is data retention in Chapter 11 important?

- Sarbanes-Oxley § 802 places criminal liability on any person who knowingly destroys documents or

Join Us

New ALI-ABA
Course of
Study:
[Electronic
Records
Management &
Digital
Discovery](#)
May 12-13
Chicago

Contact [Paul Neale](#)



for consultation
on your next
case.

[e-News Archive](#)



objects relating to a federal agency or Chapter 11 Bankruptcy.

- Access to relevant data will help with motions, government inquiries, civil and criminal complaints.
- A well-documented data retention plan will also help with motions, government inquiries, civil and criminal complaints.

A company in Chapter 11 must treat all data in accordance with government standards should it be required to produce them as part of the Chapter 11 investigation or possible litigation.

So what do you need to do?

1. Work closely with internal and outside counsel to put together a formal data retention policy. Meet with relevant department heads, compliance personnel and IT staff to review the scope of the data to be retained and identify key employees and organizational units that may become part of the investigation.
2. Communicate this policy to employees. Make sure that they understand what they need to do, what they should not do, and why. Make sure people understand the importance of record retention to the company. Repeat as necessary. Document these communications, and take affirmative steps to make sure that they are understood and being followed. Require confirmation from relevant parties that all necessary actions are being taken.
3. Stop shredding documents. Even if it was part of normal business practices before filing, it may look bad. Box, collect and separately store all documents that were meant to be shredded as a normal course of business.
4. Put together a list of key custodians – people involved in key deals, executives, sales, accounting, finance, etc. Anyone who may have been involved in anything that may be part of a dispute later on. Include, as part of the list, the key events and dates of their involvement. (Much of this data is lost as people leave). Then do a full forensic backup of all computer resources used by these employees.
5. Do a forensic backup of all computer assets related to employees that are leaving the company (both voluntary and involuntary). This should be done if the computer is sold/given to the departing employee, or even if the computer is retained by the corporation. Collect all hardcopy files, CD's, DVD, floppy discs, etc. before the departing employee leaves. Catalog and safely store this information.

6. Before a corporate division is sold, send in a team to make copies of all relevant paper documents. Make backups of all relevant computer systems. When in doubt, be overly precautious.
7. Do a forensic backup of any computer assets that are being sold. These computers should also be professionally erased. (Sensitive corporate data has been documented to have been purchased on hard drives sold on eBay).
8. Before any leased computer equipment is returned, a forensic backup should be done and the computer disks should be professionally erased.
9. Stop recycling backup tapes. This policy deliberately destroys data. Keep all incremental and full backup tapes. There will be an additional expense for new tapes, and storage, but it is a small price to pay compared to a sanction for spoliation (destruction) of evidence.
10. Consider the retention of other data. This includes, but is not limited to:
 - Voice mail
 - Corporate and cell phone bills
 - Log files from email systems, Blackberries, networking and security systems
 - Visitor lists maintained by receptionists
 - Appointment calendars
 - Rolodex and other contact programs
 - Information stored on PDA's
11. Maintain logs of everything that is backed-up, either through hard copies, normal backups or forensic backups. This should include the custodian, dates, and locations of the primary and secondary backup copies.

[Go to top](#)

This document is provided for informational purposes only. The information contained in this document is provided "as is" without warranty of any kind, either express or implied, including but not limited to the implied warranties of merchantability, fitness for a particular purpose and freedom from infringement. The user assumes the entire risk as to the accuracy and the use of this document.

(c)2005 DOAR - All Rights Reserved

□