



# Tossing the Tape?

## Implications of Making the Switch to Disk-Based Backups

**Veeral Gosalia, Antonio Rega, and Matt Shive**

Backup data on tape has usually been deemed inaccessible for e-discovery, with courts ruling that it would be overly burdensome to retrieve. Now that organizations are increasingly using disks, the question of whether backup data remains inaccessible is worth examination.



In the last few years, production of electronically stored information (ESI) for business and other purposes has increased exponentially. As the amount of information that organizations maintain grows, so do the costs and risks associated with effectively managing that data.

Organizations are increasingly moving away from tape and toward disk-based formats as their primary means of backup. While disk options are more scalable, have better indexing, and offer virtual management,

they do introduce e-discovery implications that are not of concern with tape backups.

Records and information management (RIM) professionals should therefore know that when transitioning from tape to disk, more areas may be called into interest for litigation and investigations.

### Case Law

In the last decade, judges have ruled that the amount of work in-

at the plaintiff's effort and expense.

This issue came up again in *Johnson v. Neiman* in 2010, wherein the court ruled with the defendant that electronically stored information residing on backup tapes was not reasonably accessible. The court provided a protective order on the tapes and stated "reasonably accessible" is best defined as whether the electronically stored information is kept in an accessible or inaccessible format (a distinction that corresponds closely to the

it comes to preparing for discovery of backups, regardless of whether they are stored on tape or on disk.

When legal and IT departments forget they have backup tapes from prior years, or when they change their retention policies and fail to enforce those policies on past data, problems such as the ones described below involving the authors' clients can arise.

A client was facing an inquiry that required the review of data from several years. Because the organization

## What's clear is that retention and deletion policies are paramount when it comes to pre

involved in restoring tape backups is overly burdensome, and therefore data on them is considered reasonably inaccessible for e-discovery purposes.

One of the most widely noted and earliest rulings on this matter was *Laura Zubulake v. UBS Warburg*, presided by U.S. District Judge Shira Scheindlin from the Southern District of New York. *Zubulake* centered on a sexual harassment suit filed by a former employee. The employee claimed that to prove her case, she needed e-mails from UBS Warburg that had been stored on tape and later written over by backups.

This issue brought forth case law about the duty to preserve, with exceptions made for data that is retained as part of a backup. This ruling has led to widespread interpretation that if data must be retrieved from backups, the burden of cost must shift to the requesting party.

A ruling in *Kilpatrick v. Breg, Inc.* in 2009 said that backup tapes can be subject to discovery despite being identified as not reasonably accessible. In this matter, the defendant claimed that its tapes could not be produced for the purpose of finding electronic documents of relevance because they were for disaster recovery only. Ultimately, the judge ruled the tapes could be produced to the court, but

expense of production)."

The Federal Rules of Civil Procedure (FRCP) provide further guidance on the matter of backup tapes. Rule 26(b)(2)(B) supports the court actions:

A party need not provide discovery of electronically stored information from sources that the party identifies as not reasonably accessible because of undue burden or cost. On motion to compel discovery or for a protective order, the party from whom discovery is sought must show that the information is not reasonably accessible because of undue burden or cost. If that showing is made, the court may nonetheless order discovery from such sources if the requesting party shows good cause, considering the limitations of Rule 26(b)(2)(C). The court may specify conditions for the discovery. Rule 45 (e) (1) (D) also addresses inaccessibility and echoes this guideline.

### Discovery of Backups

While the cited rulings still leave some gray area about accessibility, what's clear is that retention and deletion policies are paramount when

had a policy that all tapes would be overwritten after 30 days, the investigators initially believed there would be limited historical data. The team at corporate headquarters confirmed this policy, as did the contact at the company's satellite office where collection was to take place.

However, when the forensic examiner was leaving the satellite office after collection, he noticed stacks of tapes – many more than would have been needed for 30 days of backups. It was then revealed that these backup tapes predated the 30-day retention policy. Because the company had not disposed of the existing tapes when it implemented the 30-day retention policy, it had to spend millions of dollars to restore and review the data on them.

As another example, a client that has retained historical backup tapes for a subset of data under legal hold, dating back to 2006, now has to make a subset of its content available for review in a new litigation. Unfortunately, because these tapes weren't indexed, and many were not labeled when created, an extensive process must be undertaken to identify tapes to be indexed, restored, and their content subsequently reviewed. This effort will require an exorbitant amount of time and money to complete.

## Benefits of Using Disk

It is important to note that when much of the case law around tape backups was established, there was little use of disk storage. Now, as disk use increases, there is more discussion of the scope of accessibility of backups on disk.

There are important differences to consider between the tape and disk-based worlds. By better understanding them, RIM, IT, and legal teams can work together to prepare for po-

much data loss is acceptable.

If data must be stored for more than two years, the better approaches are using a combination of tape and disk or simply using tape. Because disks require less storage space, an organization using disk storage can back up an entire data center with just two or three refrigerator-sized storage arrays and will have space for two or three years' worth of data. Using tape, the same data center would require up to eight refrigerator-sized

case law, it will be governed by how readily accessible the data is and if it is too burdensome to discover. Included below are questions to help organizations determine whether disk backups can be considered reasonably inaccessible in e-discovery.

### *How Do Platforms Differ?*

Current typical backup products do not create indices as part of the usual backup process; this is true for tape and disk. Without an index, there

## paring for discovery of backups, regardless of whether they are stored on tape or on disk.

tential discovery of disk backups and to address any burden arguments.

Among the benefits for moving from tape to disk are the following:

### **Reduced Risk**

Most IT and records management professionals consider disk storage to markedly reduce the risk factor because it doesn't require as much physical handling, which can make tapes more error prone. Backup to tapes is also more likely to fail.

In addition, organizations typically entrust a third party to store their tapes, putting their sensitive data outside their immediate control and potentially at risk. While it's true that organizations often store more data when using disks because they are less cumbersome than tapes and because disk-based backups are often run more than once daily, the reliability of disks makes up for the risks that may come with this increased volume.

### **Reduced Cost**

Cost is often a major factor in deciding to move to disk, but disk storage is not always cheaper. Typically, the metrics organizations use to determine cost include how long the archived data would need to be retained, how much time would be available for its recovery, and how

storage racks, and the volume would grow over time.

### **More Efficiency**

Managing tape is difficult. It should be encrypted when it's shipped to a storage facility. Further, it involves a lot of moving parts: hardware can break, and network resources must be devoted to support the backup process.

Disk storage eliminates these complications. Most disk backup solutions are built on technologies with fewer parts that can fail. Industry statistics show a strategic win for disk use in most cases due to reduced resources needed to maintain the backups.

Additionally, disk backups almost always involve deduplication. While deduplication can be done on tape, the process is less efficient. This is a key differentiator, especially when considering older backup tape methods.

### **Questions for Discussion**

It is critical to understand how disk storage impacts records management from a compliance standpoint and how – if at all – regulations for disk use differ from tape.

As mentioned earlier, there is clear case law concerning how tape backups may be used in e-discovery. If there is a future deviation from

is a significant argument about the discoverability of that data: it needs to be restored, reviewed, and analyzed to find whatever information is being sought.

That being said, backup solutions are changing significantly and rapidly, enabling full indexing that would help limit the amount of data to be restored and addressing issues of deduplication, efficiency, and more. Some platforms include functionality that can aid in e-discovery.

As the burden discussion for disk backups evolves, these features may become more significant, setting a different precedent for this issue. As these types of technologies become available, RIM professionals should evaluate the options to ease future e-discovery burden and cost.

### **Can Backups Be Reasonably Restored?**

With tape, hardware that can physically read the data is required, and those devices can be difficult to find for legacy data. Disk is typically easier to access than tape, but doing so does require some effort.

With disk, the data is usually not encrypted because it does not change hands that often (though disk-based encryption is quickly becoming standard). If the backup is unencrypted, it

is possible to retrieve a single identified item or group of items without restoring the entire backup, making it far superior to tape for finding data. This is yet another reason why information management professionals and counsel must be prepared for the possibility of disk backups coming under the scope of reasonably accessible sources for discovery.

Tape restoration costs can slightly surpass those of disk. Tape requires more resources because it creates contention in the data center's bandwidth as backups are continuing to write simultaneous to the restoration process.

Further, if an organization no longer has the hardware or resources to restore legacy data, it may need to engage an outside provider. While the contention issue goes away with disk use, such restoration still requires a location for the restored data to be written to, such as a disk array or other hardware. Restoring from disk is typically faster than restoring from tape as well.

### ***Does Switching Affect Existing Litigation Holds?***

Switching from tape to disk essentially has no net impact on existing legal holds. The transition affects only the way information is stored; it does not negate any preservation

commitments.

With tape or disk there must be a retention policy in place that takes into account any current litigation hold obligations. During a transition from tape to disk, IT must retain any data that is stored on tape that is under litigation hold. Further, disk use more readily allows for taking more than one backup per day, which creates more points in time to restore or recover from. If some of that data is on legal hold and therefore can't be removed, there could be an increasing cost in the disk environment because more data is being backed up.

When moving to a disk environment, policies may need adjustment to address new retention and backup approaches. As noted in the case examples, enforcing those policies can be difficult, but it must be a priority.

### **Be Proactive**

RIM professionals can make a strategic impact on their organizations by carefully assessing the benefits and challenges of more modern, flexible options for data storage, accessibility, and governance. A thorough audit will give stakeholders the opportunity to take a hard look at how their backup policies need to change.

Legal holds are a critical focal point requiring extra attention dur-

ing these discussions, as well as for and during any subsequent data migrations. RIM professionals should work with the legal team to evaluate the discovery requirements to ensure that retention and deletion policies address retention needs appropriately and that any approaches for managing backup procedures take e-discovery requirements into consideration.

Disk-based storage in particular opens a new door of what may be considered discoverable; in certain circumstances, archived data that may have since been deleted from the "live" environment can be an important consideration to an investigation.

Understanding these sensitivities and being prepared to work with counsel to respond to a discovery matter, either in making a burden argument against restoring the backups or to cooperate in a restoration process if disk backups are deemed accessible by a judge, can be a key difference-maker in the decision-making process. **END**

*Veeral Gosalia can be contacted at [veeral.gosalia@fticonsulting.com](mailto:veeral.gosalia@fticonsulting.com). Antonio Rega can be contacted at [antonio.rega@fticonsulting.com](mailto:antonio.rega@fticonsulting.com). Matt Shive can be contacted at [matt.shive@fticonsulting.com](mailto:matt.shive@fticonsulting.com). See their bios on page 47.*