

## Getting a Handle on Your Backup Data

**By Michael Daniec**

It's a question in-house and law firm lawyers should be asking themselves, and then asking their clients. Yet, few have been: When it comes to your client's archived data, do you have any idea what type of information exists, and how much? Does anyone at the company, or for that matter, at the law firm? Can you be sure that your clients have been backing up their information and can even *find* all their backup tapes? If your client is served with a discovery request or regulatory inquiry tomorrow, how difficult would it be to respond in a timely manner?

Unfortunately for many corporations and law firms, finding out the hard way that they can't answer those questions can be a tedious and extremely expensive process. Once, companies didn't generate nearly as much data as they do today. Then, it was reasonably safe to simply back up everything and store the tapes away somewhere. But the sheer volume of information that must be backed up has grown to a staggering degree, and so have the different places where data can reside—on networks, personal computers and personal digital assistants. At the same time, the importance of properly managing all that information has become more critical.

Several recent events have brought the issue of archived information from out-of-the-way closets to the forefront of corporate concern: requirements of the Sarbanes-Oxley Act and other federal regulations; court decisions in *Zubulake v. UBS Warburg* and *Coleman v. Morgan Stanley*; and devastating natural disasters that have completely wiped out business records.

Many companies hold out hope that they will never be faced with the need to delve into their backup tapes, so they choose to ignore the problem. But that can be a very expensive gamble. Rather than hoping for the best, and then having to react, it's better to be prepared and get backup records in order without the specter of a lawsuit hanging overhead. And while the task may seem momentous, it can be done if the correct steps are taken right away. Failing to do so can be expensive and embarrassing.

### **The Rising Stakes**

Several high-profile court cases have made very clear the danger of inadequately handling e-discovery demands and mishandling backup tapes. In a series of five opinions in *Zubulake*, U.S. District Court Judge Shira A. Scheindlin has ruled on a wide range of issues involving e-discovery. Those rulings have touched on the scope of a party's duty to preserve electronic evidence throughout a lawsuit; lawyer's duty to monitor clients' compliance of preserving and producing electronic data; and imposing sanctions for the spoliation of electronic evidence.

If the ruling in the *Coleman v. Morgan Stanley* case lacks such a history, it more than made up for it with sheer dollar volume. Morgan Stanley was penalized to the tune of more than \$1.5 billion in that case, in part for the way it was perceived they mishandled archived emails. As part of a discovery demand in a case of alleged fraud, Morgan Stanley was required to produce certain emails, including some that had been stored on backup tapes. However, the financial services giant kept finding old emails that had never

been searched, even after a company employee certified that Morgan Stanley had complied with discovery demands.

Stricter federal regulations have also increased corporations' burdens towards maintaining archived information. In response to Sarbanes-Oxley and other measures, companies are storing more and more data. A fear of deleting the wrong information may make it tempting to store everything, rather than following the Sedona Guidelines that describe how "information should be retained as long as it has value to an organization, or is required by law or regulation to be retained." Failing to develop a coherent policy can mean a company drowns in backup data.

Recent natural disasters such as Hurricane Katrina have also made painfully clear how fragile backup records can be. A company can do everything right when it comes to backing up data. But unless backup information is stored safely offsite, or "vaulted," it can be at risk from forces beyond anyone's control.

### **Taking the Right Steps**

So you have convinced your clients they need to get their data in order. With that first step out of the way, there are still others to take when it comes to acquiring and maintaining historical data. But with the proper planning and methods, the task can be achieved.

Among those:

#### ***Step 1: Have a Plan***

Develop a plan for historic information, and then implement it. This may seem like an obvious first step, but it's one that many companies are not adhering to. According to a recent study by Cohasset Associates Inc., only slightly more than half of respondents (57%) have a formal plan to respond to discovery requests for documents.

There are several places to turn for developing a plan, including the Sedona Guidelines. Different industries also have different requirements—heavily regulated industries such as financial and pharmaceutical will need different plans than small retail operations, for example. A multi-disciplinary approach is the best way to develop a plan that is appropriate for your client. Members of the Information Technology, Compliance, Regulatory and Legal departments should all be given the chance to weigh in on the matter. The plan should also involve an educational component: Employees must learn why the plan has been developed and what they need to do to comply with those policies.

#### ***Step 2: Make Sure Backup Data Is Readable***

With a policy towards archiving information in place, it's time to consider the information that has previously been archived. All the historic data should be in one place, integrated into comparable formats and consolidated.

That can be a difficult task. Over time, companies and their IT systems evolve. After numerous technology upgrades, much of the data may no longer be in a format that is easily readable anymore—it could easily have been obsolete for years. Mergers and divestitures may have left different divisions or departments with totally different hardware and software systems. Disparate hardware, software and operating systems often must be merged into compatible systems, a technological challenge when both new and legacy systems are in place.

### ***Step 3: Recover Any Missing Data***

Of course, to begin making sure all the data is compatible, you must have access to the data. That is no easy task, because data can be a fragile thing. Employees quit and don't leave their passwords behind, locking up information on their hard drives. Laptops get dropped. Fires start. More sinister things happen, too; data can be deliberately deleted, as in the case of Martha Stewart's phone records to her broker (although Stewart later had the record restored).

Despite accidents and deliberate sabotage, most data can be recovered. Software programs exist that can help with this task, but many companies lack the resources in-house to attempt complex forensics recovery. In such cases, it may be necessary to bring in vendors that specialize in the field.

### ***Step 4: Cull and Filter the Data***

After all the work that's been done, it will turn out that most of the data on the backup tapes isn't terribly important. There are methods that allow for quickly searching data. If it's possible to establish requirements at the source, companies can save a great deal of time, money and effort when they need to find responsive material.

### ***Step 5: Keeping the Data Safe***

Now that the data is properly archived, readable and searchable, it should be stored in a secure location. For the very smallest of companies, it may be as simple as having employees take turns bringing backup data home after work. But for larger companies with highly sensitive information, online data repositories can be an option. With the data physically distant from corporate facilities, there will be no worries of natural disasters or fires. And online security measures can ensure that the data will not be vulnerable to hackers and others.

Too many companies don't think about their backup data until they have to. Being caught off guard and playing catch-up to find the appropriate historical data on demand is nerve-racking, time-consuming and expensive. When time is of the essence, scrambling to comply with discovery and regulatory demands and needing to dig through veritable needles in haystacks to find the right information will take more time and cost far more than it would have if the company had been prepared ahead of time for the eventuality.

There are numerous steps to take when getting archival information in order. Your clients' ability to handle all this in-house depends on many factors, including their size and scope. In many cases, they may want to consider outsourcing much of the work to a company that specializes in the field.

As their legal advisor and counselor, it is your job to make sure they take whatever steps they need to in order to ensure that their backup data is protected.

**About the Author:** Michael Daniec is CEO of National Data Conversion. NDC helps law firms and corporations deal with data restoration and conversion as it pertains to discovery or corporate compliance. Contact him at [mdaniec@ndci.com](mailto:mdaniec@ndci.com) or 212-463-7511. NDC is on the Web at [www.ndci.com](http://www.ndci.com).