TEXAS LAWYER

An ALM Publication

texaslawyer.com | October 3, 2016

3 Backup Tips to Protect Your Firm's Data

BY JULIE MACHAL-FULKS

A LAW FIRM'S ELECTRONIC data can be critical to the firm's efficiency. If a firm's electronic information were lost or otherwise unusable, it could hinder or even cripple the firm's ability to successfully represent its clients. To help reduce the risks associated with lost data, many firms have a process for backing up its data. Unfortunately, not all backups are created equally. It is important for attorneys to regularly review and improve their processes related to backups and recommend that their clients do the same.

©iStock/alexsl

1. Review the current backup technology. Law firms are not always on the cutting edge of technology, and many are using outdated methods to back up data. The lawyers in the firm operate believing that the data they might lose can easily be restored.

When using older technology like tape backups, it may actually be difficult or impossible to restore specific data. Lawyers should understand the frequency of the backups, and how often data is overwritten. Often, firms only have the potential ability to restore a few days of data but believe that most data is recoverable.

If an attorney represents a company in a regulated industry, the backup technology could be critical. Some providers that offer cloud backups and storage cannot provide the appropriate safeguards to satisfy regulators in the financial or health services industries.

For those organizations, backups on hard drives, where the regulated entity has the ownership and physical control of the

hard drive, may be the most desirable.

2. Ensure someone is actually making the backups. Due to shrinking budgets and staffing changes, a firm might not be backing up data as regularly as it believes. It is often only after the data is lost that everyone realizes that the backups were never prepared.

A firm's managers may feel more comfortable if it has outsourced the making of its backups to a third-party provider. When a firm outsources backups to consultants, it should ensure that the consultant has appropriate controls in place to ensure that the backups are actually made.

After a data loss, many firms discover that despite an undertaking to make regular backups, no one at the consultant's office is actually performing the task. In that instance, a strongly worded indemnification provision will not help a firm recover data that no longer exists.

3. Understand where the data resides and who is responsible for its loss. One of the biggest challenges with the backup process is where the backed-up data resides, who is responsible for its loss, and what happens if a third party wants to access the data.

Many consultants that agree to assist with data storage and redundancy will not assume any liability if something goes wrong with the data. Lawyers and their clients should always understand exactly what the provider is willing to do in the event of a data loss.

If the data is stored in the cloud, it is also important to know what will happen in the event that a third party tries to access the data. For instance, many companies will comply with all requests from law enforcement for information stored on the companies' hardware. Sometimes, the data will be produced without notice to the data owner.

Some providers are flexible with these protocols and will give the data owner notice that the data will be delivered to law enforcement. Others are not flexible. Due to the sensitive nature of the data lawyers retain, it is advisable to choose a vendor that will provide notice and an opportunity to object before submitting data to any third party, including law enforcement.

In regulated industries, it might be a violation to transfer data outside a specific geographic region. If that is the case, ensure that the provider will notify the customer before transferring the data outside of the identified region.

CONCLUSION

Technology could be advancing the ability to restore and recover lost data, but with those advances come new and different risks. Companies should always understand their approach to backing up critical data, and they should ensure that their processes fit the companies' needs. If outsourcing backups and data storage, understand what potential liability the vendor is willing to assume if something goes wrong.

Julie Machal-Fulks *is a partner in Scott & Scott in Southlake, where she leads a team of attorneys in representing and defending clients in legal matters relating to information technology*