The Basics of Backup

by Sharon D. Nelson, Esq. and John W. Simek

Protecting Your Practice

Is backup a particularly sexy topic? No, but it sure generates a lot of questions when we lecture. And lawyers have begun to comprehend the significance of backing up wisely – especially after the data catastrophes caused by the natural disasters of 2017. Lawyers are increasingly keen to learn how to backup their data well.

Moreover, lawyers are ethically compelled to protect the confidential data entrusted to them by their clients. That means much more than securing their networks from external attacks and other cybersecurity incidents. Ransomware infections could cripple law practices by encrypting data and rendering it inaccessible. Every lawyer needs to be prepared to recover from a security incident, including those caused by Mother Nature.

Backup

Backup is an essential operation for every law firm – and yet, often poorly understood. Having an adequate backup is implicit in the ABA Model Rules for Professional Conduct and their state counterparts, as any legal ethicist will tell you. One of the lawyer's duties is to competently represent clients. How can you do that if your case files and communications are lost? You could have a hardware failure of your server or a disk crash. What if your cloud provider shut its doors, rendering client data inaccessible? Perhaps your laptop is stolen from your vehicle with client data for a pending matter. There are all kinds of situations where you could lose data or not be able to access it. That is where your backup comes into play. Should you have a catastrophe, you would restore data from your backup and be back in business.

A local backup is also a necessity if you use cloud services and your Internet connection goes down. You could certainly take your laptop to a public open Wi-Fi and get to your data that way, but having a local backup of your data is a good idea too. It gives you a safety net should something catastrophic happen to your cloud provider.

These days, the threat of ransomware is foremost in many attorneys' minds, no doubt because more than half of business surveyed have suffered a ransomware attack. For those that have been living under a rock, ransomware is basically malware that encrypts your data with an encryption key that you **do not** have. You must pay the ransom in order to get the decryption key and hence access to your data. The sad reality is that even though you pay the ransom, you may not get the decryption key. The latest statistics are that you will get a valid decryption key in less than 50% of the cases after paying the ransom. The scary part is that we are beginning to see some forms of ransomware that do not encrypt data, but rather destroy it! There is no option to decrypt the data since it no longer exists. Most lawyers have not heard about this terrifying form of attack but once again, backups may be your salvation.

In order to recover from a ransomware attack, backup is your friend. If you are unlucky enough to contract ransomware, just restore your data back from your backups. Of course this implies that you have good backups and have done test restores to make sure you could actually recover from an attack

or failure. Test restores are crucial to verify that the data is restorable and not corrupted. All too often we hear of law firms that have no backup or the backup is corrupted. One solo practitioner, who used a cloud backup, lost five years of law firm data – he had never done a test restore so he never knew that there was anything wrong with the backup. In such cases, you might sue the service provider – but that doesn't get your data back!

External USB Drives

Many solo and small firm attorneys use external USB drives for their backup. That is a perfectly good solution, but disconnect the drive once the backup is completed. Also, you should have at least two backup drives in case one of them is connected at the same time your computer experiences a ransomware infection. We have dubbed this advice "virgin backup" – you must have a backup which is not connected to your network – therein lies your peace of mind.

Hopefully your computer is equipped with a USB 3.0 port, which will allow for faster backups due to the faster transfer speeds versus a USB 2.0 connection. That means you should be only looking at purchasing an external USB 3.0 hard drive. You may want to consider getting a USB drive with built-in hardware encryption. Hardware encryption will ensure that the data is protected when the device is disconnected and powered off. Some external USB drives also come with backup software for no additional charge.

Tape

At this time, we consider tape backup systems to be obsolete. We have come across some law firms that still use tape, but we wish they would convert to a more economical and dependable hard disk type of system. Tape capacity can't come close to the amount of data you can fit on a hard disk. The data transfer rate to tape is also very slow when compared to disk transfers (even with USB). Tape is fragile as well and doesn't have a long life.

Since backing up to tape is not very reliable, it is a best practice to verify the backup after it completes. Verification further increases the amount of time to backup data. Hopefully we've made the case to abandon tape as backup medium and convert to an alternative method.

Backup Appliance

Another solution is to use a backup appliance that is agent-based. This means that you install a software agent on the computer to be backed up and data is transferred over the network to the appliance by using the agent. Think of it as communication software. The agent gathers the data to be backed up and transfers it to the appliance. This communication connection is not seen as a drive letter or a network share, which makes it impervious to ransomware attacks.

Typically, the backup appliance solution is used to backup local servers. The software is configured to periodically take snapshots of the server and stores the backup data on the appliance. In addition, consider sending an encrypted version of the backup data to the cloud, another best practice. Some appliances have the ability to virtualize the server should the actual server suffer a hardware or software failure. As an example, the backup appliances that we implement can take snapshots every 15 minutes and virtualize a server within a few hours. This has been a lifesaver for some of the law firms we work with.

Since the appliance is essentially a server customized for backup, expect to pay up to a few thousand dollars for the initial investment. A lot of the backup appliance providers provide the agents on a monthly subscription basis. The cost may be per agent or based on the amount of data (size of server) that is being backed up. Off-site storage may also be included in the cost or priced on a per terabyte basis. Expect to pay on average somewhere around $100 a month per server being backed up. It could be as low as $50/month or up to $200/month depending on how the provider bases its charge (per device or by size volume). Off-site storage should run around $150-$200 per terabyte per month.

Cloud Backup

Using a cloud-based backup solution will also allow you to restore data following a ransomware attack. Just like the external USB drives, make sure you have at least two backup sets in the cloud.

There are many good backup solutions using the cloud. If possible, you should look to a cloud provider that allows you to control the encryption key used to encrypt the data. Carbonite is a good backup cloud provider that has that capability. A best practice would be to have multiple versions of the backup data in the cloud. That way if one gets corrupted or suffers a ransomware infection, you'll have alternate backup sets to restore from. Another highly reviewed backup provider is Backblaze.

Target Data

Selecting the appropriate technology is just one piece of the backup puzzle. The first thing you need to do is determine what you will back up. If you are looking for a disaster recovery option (total loss of equipment or service), you'll need a method that will allow you to recover quickly and preserve not just the data, but possibly applications as well. You'll probably end up with some sort of backup appliance if disaster recovery is your goal.

Risk Assessment

Once you have determined what needs to be protected, the next analysis is to determine the likelihood of data loss or inaccessibility. How likely is there to be a hardware failure? Perhaps your risk is fairly low if you have new hardware. However, failures can occur beyond hardware issues. Data could become corrupted. Someone could inadvertently delete a file. You could overwrite a file with the wrong version thereby destroying the original contents and of course, ransomware could render data inaccessible.

No matter what the scenario, you should perform a risk assessment and determine action steps to mitigate that risk.

Data Location

Another consideration is data location. Where is your important data being held? Many lawyers still have on premise equipment and keep their data on local storage devices. They just don't trust losing control of the data by putting it in the hands of a third party. Others are using cloud services and confidential client data is out of the lawyer's direct control. Different methods are needed if you have direct access to the data or it resides on some external service.

No matter where the data resides, the challenge is to find it all. You would be surprised at all the places law firm data ends up. Employees take data home. It exists on flash drives. It may be sent as attachments to a personal web-based e-mail account. Spend a little time to inventory all or the data sources. You can't back it up if you don't know you have it. "Dark data" – data a law firm doesn't know it

has – has grown by leaps and bounds in recent years. It presents all kinds of risks – you can't protect that data, you can't back it up and if you don't know you have it, you may fail to disclose it when required to do so by laws and regulations or in litigation.

What about personal devices such as smartphones? You'll have to decide if the information on a personal device is at risk of being lost and should be backed up. This may be a good time to rethink your BYOD (Bring Your Own Device) policy and what devices can access firm data. If you do decide that smartphone information needs to be backed up, there are software solutions to accomplish this. Should you leave the process up to each individual or should you invest in a MDM (Mobile Device Management) system?

How Much?

Finally, how much data do you need to back up? That can radically impact your backup strategy. Hard drive space is fairly cheap these days, but you can't defy the laws of physics. Transfer times are only so fast. You can't make the electrons move any faster. Network speeds will limit the amount of data transfer as well. Perhaps now is a good time to upgrade your network cabling and hardware. If you are only backing up to the cloud, hard drive space is not an issue. However, you will need to know the data volume in order to determine how much the off-site storage is going to cost.

Last words

We worry about backup for lots of reasons. The natural disasters of 2017 were a great reminder of the need for having backups, as many lawyers painfully discovered.

Beyond that, ransomware has been on a wild roller-coaster ride, causing havoc everywhere, including in law firms. Ransomware really is a global epidemic today. The "bad guys" are constantly updating code and discovering new vulnerabilities to exploit. We hope you never have to experience a ransomware event or a system failure. But if you do, make sure you have properly engineered your backup so you can get back in business with minimal effort and pain. Engineering a good backup system is one of the smartest things any law firm can do to protect its confidential data.

Backups are one piece of the cybersecurity toolkit, but oh boy, there are lots of others. The Futures Conference of the College of Law Practice Management is holding a conference entitled "Cybersecurity: This Way There Be Dragons." The conference will take place October 25-26, 2018 in Boston at the Suffolk University Law School. It is sure to sell out quickly. You can find out more about the conference at http://collegeoflpm.org/.

The authors are the President and Vice President of Sensei Enterprises, Inc., a legal technology, cybersecurity and digital forensics firm based in Fairfax, VA. 703-359-0700 (phone) www.senseient.com