NJSBA PRACTICEHQ Affinity CONSULTING

BACK IT UP!

By Barron K. Henley, Esq. and Jeffrey Schoenberger, Esq.

DON'T CUT CORNERS HERE

Backup is not an area to cut corners on costs, but there are ways to protect yourself and not spend extravagantly.

BACKUP DEVICE/SYSTEM OPTIONS

We recommend that your primary backup is internet-based, constantly running as a background process on your machines. However, we do NOT recommend relying solely on an Internet backup option. Have a secondary backup system on-site (either external hard drive(s) or network-attached storage (see below)) Here are a few suggestions:

INTERNET BACKUP OPTIONS

This is becoming common as the primary backup method. The biggest advantages of internet-based backups are that they are offsite, someone else handles all hardware issues, and your files are backed-up to highly-secured data centers with redundant power and internet. Top vendors in the field are:

- Backblaze;
- CrashPlan;
- Carbonite; and
- SOS Online Backup.

No matter what you do, you must get a backup system. It is not optional. Losing all your data can cripple your practice and cause you to commit malpractice. The risk is simply not worth it.

EXTERNAL HARD DRIVES

There are external hard drives explicitly designed as backup devices, and this is our recommendation. They hold tons of data and are inexpensive. The annoyance is that you must unplug one of them and take it home with you daily (they need to be rotated so you always have one complete, local backup offsite). On the other hand, they're speedy and reliable. Look for at least 5 TB of storage and a 7,200 rpm drive. If your computer supports USB-C or Thunderbolt, look for drives allowing you to take advantage of the faster speeds those interfaces offer. There are many options.

NETWORK ATTACHED STORAGE ("NAS")

Without getting too technical, NAS is storage (usually an external hard drive) attached directly to your network rather than to an individual PC or server. The benefit is that all computers connected to the network can access the NAS regardless of which computers are on or off. Furthermore, higher-end NAS devices employ RAID (Redundant Array of Independent Disks). RAID is a configuration in which multiple hard drives are arranged to store data across all of them simultaneously. Even though multiple drives are involved, your computer sees the RAID as a single drive letter on the network. RAID gives you better performance (surprisingly), capacity, and reliability than a single large drive. There are several "levels" of RAID, including RAID 1 (straight mirroring when two drives both contain the same data) and RAID 5 (Rotating Parity Array - all data is distributed across all drives, and there are at least 3). For a good explanation of RAID and what the levels mean, see https://en.wikipedia.org/wiki/RAID. It can contain multiple backups of your data, and if RAID is employed in the device, it's improbable that you'll have a simultaneous crash of all the drives contained inside the NAS.

BENEFITS AND DRAWBACKS OF A NAS

NAS devices run the gamut in terms of price and capability. They can be as simple as a hard drive connected to your wired network or as complex as a server that hosts documents, websites, and even virtual machine computers. But, of course, as you add capabilities, you add cost, complexity, and potential security risks.

The primary benefit of a NAS is easy sharing and backing up of documents you do not want to store in a cloud-based sync service. However, except for Tresorit, every major cloud storage vendor can turn over readable data if it is served with a subpoena or lawful warrant. This is true of Apple's iCloud, Dropbox, Google Drive, and Microsoft's OneDrive. Whether you're provided notice and an opportunity to contest depends on the service and its terms of service. It's possible to add your own, known-only-to-you, encryption to these major services, except iCloud, via Cryptomator, but by default, all client data you store in these cloud services has the potential to be produced upon request in a readable fashion.

Files that you store on a NAS are triply protected from this outcome.

- First, the files are stored in a device that you control. If you want the hard drives encrypted with a password only you know, you can do that.
- Second, while it's possible to configure a NAS so that you can access your files from outside your network (*e.g.*, on your smartphone via a mobile app), you don't have to activate that feature, and if you do, the data doesn't live on an intermediary server "in the cloud" somewhere; it still lives on the NAS. Although accessing NAS files over the internet does mean that those files transit through an intermediary server owned and controlled by the NAS vendor, they don't reside there. The vendor's server is a mere bridge, not a filing cabinet or data warehouse.
- Third, the physical NAS device lives in a location you own or control (*e.g.*, your home or office). To access the files, the interested party must gain access to your premises. And, of course, Fourth Amendment search and seizure law is much better developed than interpretive standards for terms of service policies for cloud vendors.

Having presented the "pro" case for NAS devices, one must be aware of the "cons" as well.

- First, a NAS is a computer. Depending on the features you want, like accessing documents over the internet, it is also a server. It runs an operating system and applications. Like your Mac or Windows computer, that operating system and those applications must be kept up-to-date for maximum security. Fortunately, most NAS products are designed to keep themselves updated automatically, much like our smartphones and apps.
- Second, you must practice good security hygiene for a NAS connected to the internet. This means a complex password and, if available, multi-factor authentication for any remote access. Many people never change the username and password combination to their internet router, which is often the same for every device provided by a given cable company or internet service vendor. Don't be the person who loses client files because someone tried the NAS vendor's default username and password successfully to gain access to your NAS.
- Third, although vendors have improved their software markedly in recent years, granting a NAS access to and through your network to the internet harbors the risk of opening a gateway that lets bad people in. If you are uncomfortable making changes to your internet router or have no idea what an IP address is, think twice before going with a NAS.
- Fourth, one of the chief benefits of a NAS, that the device and hence the files are under your physical control, is also a negative because that means the device is as vulnerable to theft, fire, or other disasters as the items in your home or office. If the NAS is your backup and it is destroyed, that's bad news for the business. Fortunately, it is possible to configure a NAS for automatic, unattended backups to the cloud. Those cloud backups can be encrypted with a password you set, so you get the benefits of the NAS and the protection of offsite backup without risking exposure of client information.

If you're interested in further research on a NAS device, here are three major vendors to get you started:

- Buffalo;
- Synology; and
- Western Digital.

RECOMMENDATION REGARDING BACKUP HARDWARE AND SOFTWARE

If you just want to ensure your laptop or desktop is getting backed up, it's hard to beat Carbonite's Personal Plus plan for ~$85/year. Buy any external hard drive and Carbonite will back up your files to their secure cloud servers and make a complete mirror of your internal hard drive on the external drive you connect simultaneously. Further, it works in the background to ensure everything is backed up, and you don't have to remember to do anything.