

HOW TO BACK UP YOUR COMPUTER

Despite the dangers, many lawyers fail to have an adequate backup and recovery system in place to protect important information stored on their computers. The information stored on your computer is the lifeline of your practice. Safeguarding that information is critical to your practice's survival, and to meeting ethical obligations you owe your clients.

Ask yourself, if your computer crashed, or was ruined in a disaster, how much downtime would that create for your practice and what would that cost your firm? Even a minor disaster can affect your law practice. Consider the prospect of recreating your documents, forms, time and billing records, calendar entries, contacts, and emails. Scary, isn't it? If you are not yet safeguarding your electronic data on a regular basis, keep reading and learn how to put a system in place. Even if you have the support of an Information Technology (IT) department for your law office, keep reading to ensure you understand what they are doing, and so you can introduce any needed systems in your home office or computer.

Data Backup vs. Disk Imaging

The term "data backup" refers to backing up or making a duplicate copy of selected information stored on your computer. In contrast, "disk imaging" refers to making a duplicate copy of everything on your computer – the operating system, software applications, program customizations, folders, and files – not just data. Disk imaging is a better backup choice. For example, if your computer's hard drive crashes, everything will be gone. To access any backed up copies of your data, you will first need to reinstall your operating system, programs, updates, etc. Only then can you access the saved data. However, if you have a disk image of your computer, your saved programs can help you access data more quickly. Disk imaging programs can be inexpensive and provide easy to use tools that allow you to get up and running more quickly. (For additional information, see the resources listed at the end of this article.)

Choosing a Backup and Recovery System

A good backup and recovery system has three elements: (1) automatic backup software; (2) a reliable storage device that is kept offsite; and (3) verification and procedures to ensure backup is working. A good backup and recovery system will let you sleep easier knowing that your valuable information is protected.

1. **MAKE IT AUTOMATIC:** Backup software must work well for the user, otherwise, the user will not use it. Automatic backup software is the safest choice because you do not have to fit the task of backing up into your day. Instead of a pop-up window interrupting you to ask if you want to back up now or later, a backup is created quickly, quietly, and automatically. The automatic software program you choose should be easy to set up. Typically, once you install the program, an interactive setup allows you to specify what you want backed up, when, and how often. Select a program that has a restore feature, so any archived information can be restored to your computer.
2. **STORAGE DEVICES:** Once you back up all the data and programs on your hard drive, you will need a place to store the initial backup until you back up again. Dedicating an external hard drive to the backup process is preferred to downloading the backup files onto numerous discs. A second removable hard drive or other external storage device is an affordable convenience. It will allow you to make a duplicate backup to be stored offsite, with the original locked in your law office's fireproof safe or file cabinet. When buying an external hard drive, purchase the largest capacity you can reasonably afford. In areas prone to natural disasters, the safest storage of backup information is offsite, preferably in another geographic location. Using Internet-based backup services is one

HOW TO BACK UP YOUR COMPUTER

possible solution. If you choose this option, read and understand [Oregon Formal Opinion No. 2011-188](#), Information Relating to the Representation of a Client: Third-Party Electronic Storage of Client Materials. Also see [Safeguarding Client Information in a Digital World](#), by Helen Hierschbiel, *Oregon State Bar Bulletin* (July 2010), and [Floating in the Cloud: The Ethics of Electronic Client Files](#), by Amber Hollister, *Oregon State Bar Bulletin* (May 2017).

3. **BACKUP POLICIES AND PROCEDURES:** If you choose a disk imaging program, your computer backup and recovery policy is simple – just set the frequency of the backup. How often should you perform backups? The frequency should be dictated by your comfort level with risking any data created or received since your last backup. Most technology advisors recommend that you back up new file information once daily, the full system once weekly, and ship backups out of the geographic area semi-weekly (if living in a disaster-prone area). They also recommend periodic restores semi-weekly or monthly. Your policy may differ, but should designate a frequency, as well as a trusted person responsible for performing the periodic test restores to ensure the backup is working. Part of ensuring the system is working is to check periodically to see whether you can restore a file, and then compare it carefully with the file you backed up. The restored information should be identical to the backed-up information. The time to verify the system is working properly is before disaster strikes.

Selecting Backup Software

When comparing backup software products, look for one that allows you to: (1) recover entire operating systems and/or individual files; (2) schedule backups to occur automatically; (3) customize the timing of backups based on the occurrence of events, such as billing; (4) back up and restore quickly; and (5) test the restoration process. To recover entire operating systems, applications, and data, use disk imaging software.

Resources

For shopping and comparison:

- Cyberguys.com – <https://www.cyberguys.com/>
- PriceGrabber.com – <http://www.pricegrabber.com/>
- Google Shopping - <http://www.google.com/shopping>

For product reviews, articles, and information:

- [Legal Technology Resource Center](#) (LTRC)
- [Law Technology Today](#)
- [Legaltech News](#)
- [PC Mag](#)
- [Backup Review](#)
- [CNET](#)

Backup and Disk Imaging Software:

- [Acronis](#)
- [Norton](#)
- [Paragon Software](#)
- [O&O Software](#)

HOW TO BACK UP YOUR COMPUTER

- Apple/Mac Specific software:
 - [Time Machine](#) (Built into Mac OS, version X or later)
 - [Carbon Copy Cloner](#)
 - [Intego](#)
 - [Drop DMG](#)

Information on Hard Drive Duplicators:

- [Aleratec](#) (Hard Disk Duplicator Buyer's Guide)
- [StarTech.com](#)

Online Data Storage:

- [Carbonite](#)
- [CrashPlan](#)
- [FilesAnywhere](#)
- [Iron Mountain](#)
- [LiveVault](#)
- [SpiderOak](#)
- [SOS Online Backup](#)

NOTE: This information does not constitute an endorsement of or recommendation for a particular product or vendor. Technology changes over time. Attorneys should conduct their own appropriate research before using technology, and continue to review hardware and software over time. Attorneys who choose to use third-party online data storage should also review [Oregon Formal Opinion No. 2011-188](#).

IMPORTANT NOTICES

This material is provided for informational purposes only and does not establish, report, or create the standard of care for attorneys in Oregon, nor does it represent a complete analysis of the topics presented. Readers should conduct their own appropriate legal research. The information presented does not represent legal advice. This information may not be republished, sold, or used in any other form without the written consent of the Oregon State Bar Professional Liability Fund, except that permission is granted for Oregon lawyers to use and modify these materials for use in their own practices. © 2019 OSB Professional Liability Fund