

TBTLA CLE

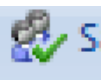
Backup Strategy for Law Offices

Do's and Don'ts of Law Practice Backup

September 14, 2017

  
Reply Reply to All Forward
Respond

   
Delete Move to Folder Create Rule Other Actions
Actions

  Safe Lists
Block Sender Not Junk
Junk E-mail

  
Categorize Follow Up More
Options

From: 
To: Dario Diaz - TBTLA
Cc:
Subject: Re: tbtlA: My CLE Presentation Thursday

Fuck IRMA that worthless bitch



I WAS JUST
WONDERING,
DO WE HAVE A
DISASTER RECOVERY
PLAN?



PROFESSIONAL ETHICS OF THE FLORIDA BAR

OPINION 06-1

April 10, 2006

Lawyers may, but are not required to, store files electronically unless: a statute or rule requires retention of an original document, the original document is the property of the client, or destruction of a paper document adversely affects the client's interests. Files stored electronically must be readily reproducible and protected from inadvertent modification, degradation or destruction.

RPC: 4-1.5(f)(4), 4-1.6, 4-1.8(j), 4-7.7(h), 5-1.2(b)(3), 5-1.2(d)

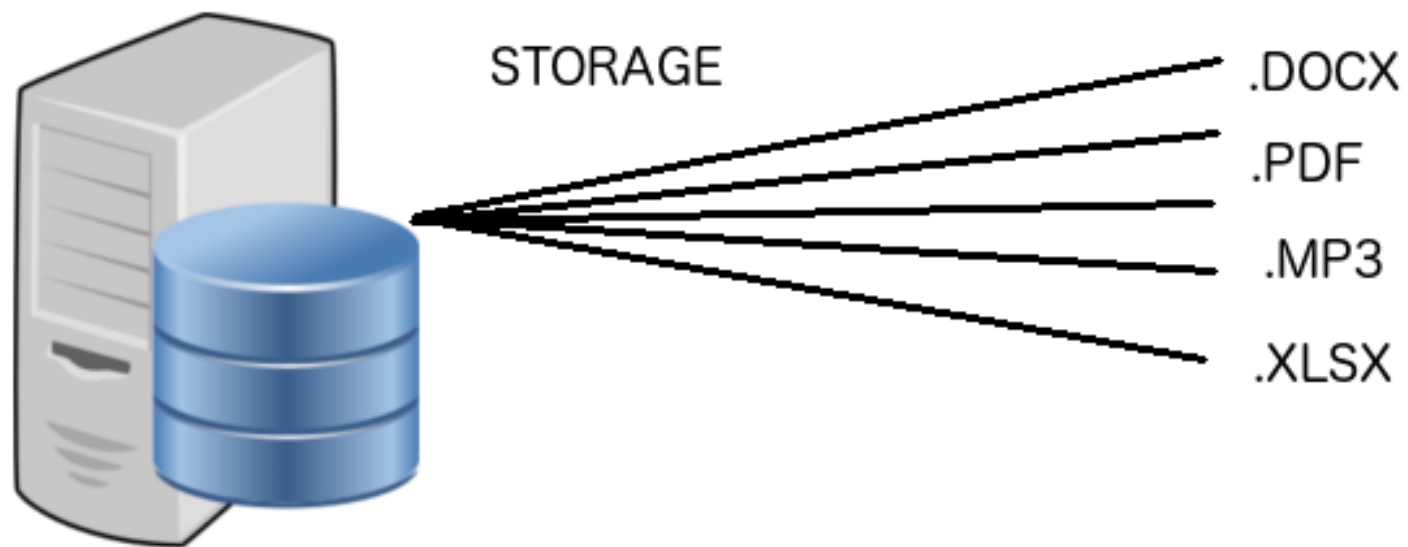
Opinions: 63-3, 71-62, 81-8, 88-11 (Rec.), ABA Informal Ethics Opinion 1127 (1970), New York County Ethics Opinion 725 (1998), New York State Ethics Opinion 680 (1996), North Carolina Ethics Opinion RPC 234 (1996)

~::~

documents be maintained, not necessarily the method by which they are stored. Therefore, a law firm may store files electronically unless: a statute or rule requires retention of an original document, the original document is the property of the client, or destruction of a paper document adversely affects the client's interests.

The committee agrees with other jurisdictions that have noted practical considerations involved in electronic file storage. The committee cautions lawyers that electronic files must be readily reproducible and protected from inadvertent modification, degradation or destruction. The lawyer may charge reasonable copying charges for producing copies of documents for clients as noted in Florida Ethics Opinion 88-11 Reconsideration. Finally, lawyers must take reasonable precautions to ensure confidentiality of client information, particularly if the lawyer relies on third parties to convert and store paper documents to electronic records. Rule 4-1.6, Rules of Professional Conduct.

The committee encourages the use of technology, such as electronic file storage, to facilitate cost-effective and efficient records management. However, the committee is of the opinion that a lawyer is not required to store files electronically, although a lawyer may do so.





- Settings
- Configuration
- Local files
- User Rights
- Programs/Apps
- Outlook, WORD
- License Keys

User Workstation

Workstations have information and are an important part of your backup plan. Being able to restore workstations quickly is an integral part of restoration after a damaging event.



SERVER

- Operating System
- Settings
- Data Files
- Programs/Apps
- Configuration
- File Storage
- Exchange Email

Server is the "central" part of any network. Data files, documents, etc. are generally stored on the server hard drives to be accessed and used by staff. IT IS THE MOST CRITICAL PART OF ANY BACKUP PLAN!



CLOUD BASED

- Off Site
- Secure
- Backup is Backed up
- Redundant
- Cutting Edge



CLOUD BASED

- Off Site
- Secure
- Backup is Backed up
- Redundant
- Cutting Edge

DON'T FORNICATING DO IT!



Hard Drive

- Fast
- Cheap
- Mobile
- Purchase Anywhere
- Tested
- Transferable



Tape Drive

- Trustworthy
- Rock Solid
- Hard to find
- Cheap



USB Drive

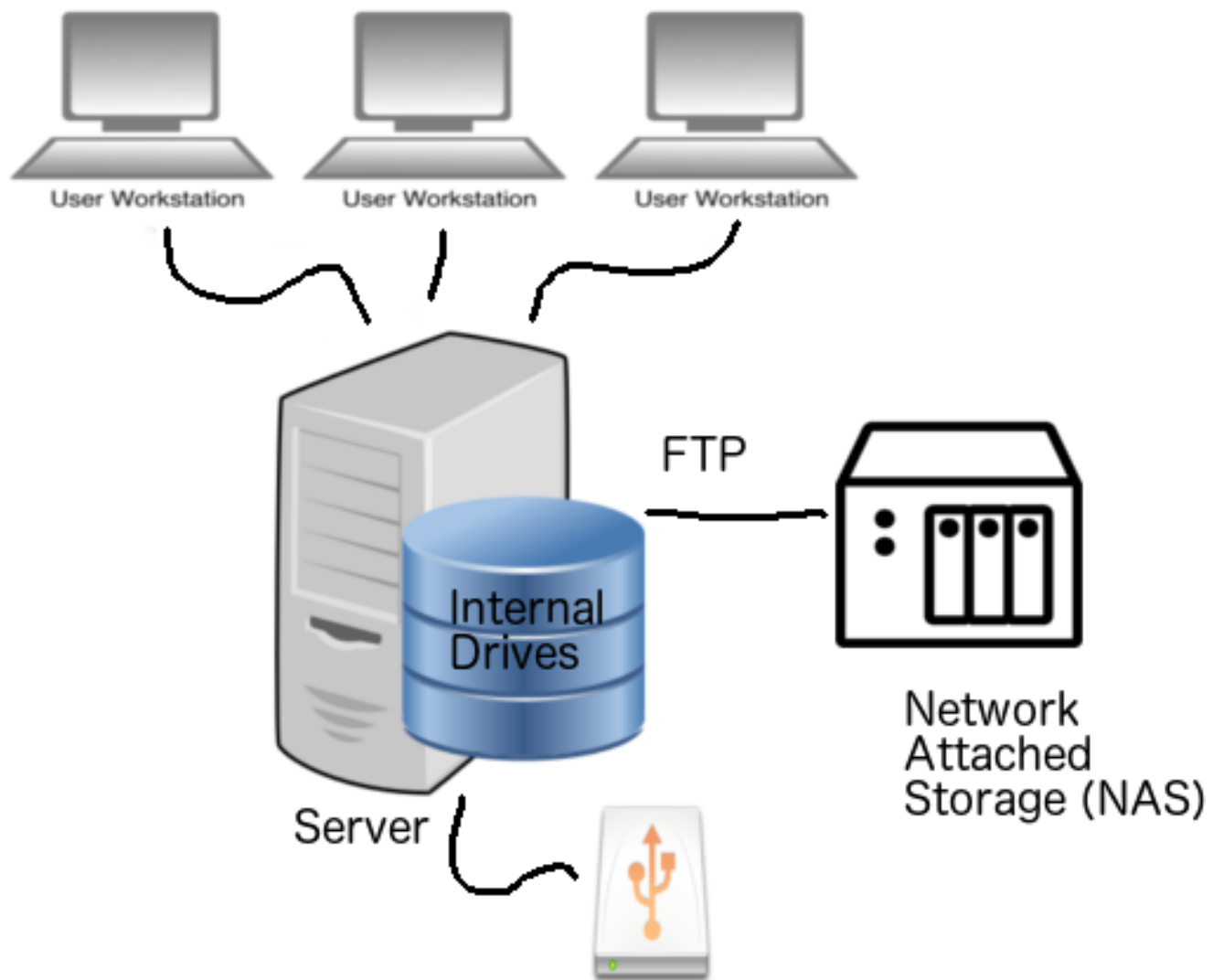
- Fast
- Cheap
- Extremely Mobile
- Purchase Anywhere
- Moderate Speed
- Transferable



Network Attached Storage (NAS)

- Fast
- Not Expensive
- Mobile
- RAID standard
- Hard Drive Speeds
- Set up non-mounted
- Hot Swap

BACKUP STORAGE DEVICES



I. LAW OFFICE DATA CRITICAL

- A. **BACKUP EVERYTHING AND BACKUP OFTEN!**

II. LITIGATION AND DOCUMENT ARCHIVE TAKE YEARS

- A. **BACKUP EVERYTHING AND BACKUP OFTEN!**

- B. Timeline – A case in litigation can take years to get to trial and then possibly years on appeal.

- C. There is even more of a requirement for an attorney to maintain the file (at least the closing statement and contracts) according to the bar rules. *See Rule 4-1.5(f)(4)(C) and (f)(5)*

A copy of the closing statement shall be executed by all participating lawyers, as well as the client, and each shall receive a copy. Each participating lawyer shall retain a copy of the written fee contract and closing statement for 6 years after execution of the closing statement. **Any contingent fee contract and closing statement** shall be available for inspection at reasonable times by the client, by any other person upon judicial order, or by the appropriate disciplinary agency.

- D. And NO, you DO NOT NEED TO KEEP PAPER COPIES! (Ethics Opinion 06-1 states that lawyers may, but are not required to, store files electronically unless: a statute or rule requires retention of an original document, the original document is the property of the client, or destruction of a paper document adversely affects the client's interests. Files stored electronically must be readily reproducible and protected from inadvertent modification, degradation or destruction.)

III. WHAT IS A BACKUP

- A. **BACKUP EVERYTHING AND BACKUP OFTEN!**

- B. Don't confuse "storage" with "backup."

- C. Back up files – Individual files are comprised of .PDF, .DOCX, XLSX (I know nobody used .DOC or .XLS files because those have been deprecated and sunsetted by Microsoft)

- D. Back up system – Saves settings, configurations, bit-by-bit (bare metal) type backup. This backs up EVERYTHING!

- E. Server vs. Workstation – Why you should have both. Workstation has software with keys, installations, user settings, user permissions, local data files.

IV. WHY DO YOU NEED TO BACKUP

- A. **BACK UP EVERYTHING AND BACKUP OFTEN!**

- B. Your system will fail, period. Count on it. Nothing is sure but death, taxes, and hard drive failure. It's not IF but WHEN it will fail.

- C. Even if your system does not, "fail" it can be compromised by ransomware, virus, disgruntled employee, or simple error. For example, an employee deleted an entire folder from a network drive by accident.

V. BUILT IN BACKUP (SHADOW COPY)

- A. **BACKUP EVERYTHING AND BACKUP OFTEN!**
- B. How often does data change? Some cases daily, in some cases never.
 - 1) Shadow Copy is built right into the Windows O/S. Shadow copy keeps a version of files right in the system itself. You can recover certain files directly from the system without the need for any, “backup.”
 - 2) The in/famous “trash can” recovery method.

VI. BACKUP PLAN

- A. **BACKUP EVERYTHING AND BACKUP OFTEN!**
- B. 3-2-1 backup approach — store your data in three places, on two types of storage, with one copy stored off-site.
- C. Time – How quickly do you need to recover the data.
- D. Who is responsible?
- E. Off-Site Disaster Recovery – How do you get your data from the off-site location?
- F. History (something gets deleted a year ago)
- G. Backup Types – Full; Incremental; Differential
 - 1) Full – Backup everything (settings, configurations, system files)
 - a. Complete and safe, takes longer, any errors result in no backup
 - b. MUST be done at least once a week.
 - 2) Differential – Backs up everything since the last FULL backup. Small and fast. But must have a copy of the last FULL backup.
 - 3) Incremental – Backs up any changes since last backup; FULL or DIFFERENTIAL. Very small and very fast, but requires each backup since the last FULL backup.

VII. EQUIPMENT (HARDWARE & SOFTWARE)

- A. **BACKUP EVERYTHING AND BACKUP OFTEN!**
- B. Speed, capacity, cost – How fast, how much, how...um...much.
- C. Tape – Oldest technology, still used. Slow and somewhat expensive.
- D. Hard Drive – Fast, inexpensive, scalable.
- E. Network Attached Storage (NAS) – Fully configurable, redundant, fast
- F. RAID – Cascade protection, requires additional hardware, fast.
- G. Cloud (Carbonite) – Stored offsite, protected...but SLOW to recover.

VIII. CONSIDERATIONS

- A. **BACKUP EVERYTHING AND BACKUP OFTEN!**
- B. Ransomware – DON'T BACKUP TO A MOUNTED DRIVE!
- C. Virus -
- D. Encryption
- E. Time (wait longer, lose more data)

IX. TESTING

- A. Fail your system manually at least once a year – This means that you actually get your main drive, remove it from your server, and do a complete install from the ground up.
- B. It's a great way to test your process, get a good backup copy of your system (because you are removing your old drives), and keep your equipment new by performing preventive maintenance.



THE FLORIDA BAR

651 EAST JEFFERSON STREET
TALLAHASSEE, FL 32399-2300

JOHN F. HARKNESS, JR.
EXECUTIVE DIRECTOR

850/561-5600
WWW.FLORIDABAR.ORG

Certificate of Accreditation for Continuing Legal Education

227809
Tampa Bay Trial Lawyers Association
Margaret S. Peavler
PO Box 1913
Dunedin, FL 34697-1913

June 9, 2017

Reference Number: 1704403N
Title: Backup Strategies, the Do's & Don'ts of Law Practi
Level: Advanced
Approval Period: 09/14/2017 - 03/14/2019

CLE Credits

General	2.5
Technology	2.5

Certification Credits

Please provide the attendees the above reference number so they may go online to www.floridabar.org to report their completion of this program.