South Carolina Bar
Continuing Legal Education Division

2018 SC BAR CONVENTION

Breakfast Ethics

Sunday, January 21

presented by
The South Carolina Bar
Continuing Legal Education Division

http://www.scbar.org/CLE

SC Supreme Court Commission on CLE Course No. 180813

South Carolina Bar
Continuing Legal Education Division

2018 SC BAR CONVENTION

Breakfast Ethics

Sunday, January 21

Security Is Only As Good As the Weakest Link: Legal Tech Security Measures Every Lawyer Must Take

Barron K. Henley

Digital Security Measures Every Lawyer Must Take

Barron K. Henley, Esq.
bhenley@affinityconsulting.com
Affinity Consulting Group, LLC
1550 Old Henderson Rd., Suite S-150
Columbus, OH 43220
614.340.3444
www.affinityconsulting.com

Digital Security Measures Every Lawyer Must Take
Table of Contents

Digital Security Measures Every Lawyer Must Take

I. **PREMISE OF THIS SEMINAR**: Rule 1.6 requires a lawyer to make "reasonable efforts" to prevent the disclosure of confidential client information. Comment 18 further stipulates that "reasonable precautions" must be taken to prevent client information from falling into the wrong hands. In a digital world, the exact meaning of "reasonable efforts" and "reasonable precautions" may be subject to debate. However, it's hard to argue that doing nothing to protect client data would meet the standard. You don't have to be a security expert or techie to protect yourself and your office. Learn how to cover all the bases of computer, smartphone, tablet, email, wireless and document encryption. We'll also cover the fundamentals of backing up your electronic data. Half of the battle is simply knowing what questions to ask and it's not nearly as complicated as it sounds. Establish best practices in your office and discover the inexpensive or free tools that will make sure your confidential information remains confidential.

II. **DEFINITIONS**: It's important to define what we're talking about here.

A. **Business Disaster**: Generally, any event that makes the continuation of normal functions impossible is considered a disaster. The severity of the disaster is a function of how long it remains impossible for the business to function normally and the severity of the impairment.

B. **Disaster Avoidance**: I really like this discussion and definition of disaster avoidance:

> "When I discuss 'Disaster Recovery Planning' I prefer the phrase 'Disaster Avoidance & Recovery Planning' (DARP). I use DARP because I believe that a disaster is a problem affecting your application availability that is unmitigated. In other words, the problem occurs and you have no repeatable strategy in place to return your operations to normal in a set period of time. Disaster 'Avoidance' in my definition refers to the ability to avoid an outage or provide a controlled and well understood ability to recover systems to normal operations."[1]

Here's the scary thing about business disasters which really underscores the need for planning:

> "According to the Institute for Business and Home Safety, an estimated **25 percent** of businesses do not reopen following a major disaster. You can protect your business by identifying the

[1] Disaster Avoidance and Recovery Planning in a Cloudified World, by Mark Thiele, Jan 5, 2011, see http://tinyurl.com/m396848

> risks associated with natural and man-made disasters, and by creating a plan for action should a disaster strike. By keeping those plans updated, you can help ensure the survival of your business."[2]

III. **CAUSES OF BUSINESS DISASTERS**: Here's a list of things we need to protect against.

A. **Data Loss or Data Disclosure**: The loss of data or access to data can stop a firm in its tracks. Further, the disclosure of confidential client data can result in malpractice actions and may also shut down a firm. There are many reasons why data loss or disclosure occurs:

1. **Human error**.

2. **Hardware failure** - flaw or defect.

3. **Fire or natural disaster**.

4. **Temperature**.

5. **Virus - ransomware - malware**.

6. **Synchronization issues**.

7. **Criminal Acts of Others**. Law firms are often the target of hackers.

> "Hackers broke into the computer networks at some of the country's most prestigious law firms, and federal investigators are exploring whether they stole confidential information for the purpose of insider trading, according to people familiar with the matter. The firms include Cravath Swaine & Moore LLP and Weil Gotshal & Manges LLP, which represent Wall Street banks and Fortune 500 companies in everything from lawsuits to multibillion-dollar merger negotiations. Other law firms also were breached, the people said, and hackers, in postings on the Internet, are threatening to attack more."[3]

8. **Malicious acts of employees**. The biggest example of this is probably the Panama Papers.

---

[2] Disaster Planning, by The U.S. Small Business Administration, see http://www.sba.gov/content/disaster-planning

[3] Hackers Breach Law Firms, Including Cravath and Weil Gotshal, by Nicole Hong and Robin Sidel on March 29, 2016, The Wall Street Journal, see http://tinyurl.com/jbzow32.

> "An attorney spokesman for the law firm of Mossack and Fonseca, the source of the Panama Papers documents, has stated that eight former employees are under investigation by government prosecutors, in an effort to identify who stole more than 11 million documents, which name tax cheats and corrupt officials, from its corporate files. The names of the former employees have not been made public."[4]

B. **Natural Disasters**: This would include tornados, hurricanes, floods, earthquakes, mudslides or anything of that nature. These events often result in constructive eviction from your office space and often, data loss.

C. **Fire**: This may or may not be a "natural" disaster, but the effects are devastating. The water used to put out the fire often causes more damage than the fire itself. Of course, this frequently results in data loss and certainly eviction from your office.

D. **Power Failure**: Of course, lots of things could cause this. The situation most damaging is when power is lost for more than a day. Of course, you can't get work done at the office and probably can't access data on the computers there. So what do you do? As our weather patterns appear to grow more severe for whatever reason, power failure is becoming a bigger issue.

E. **Internet Failure**: Lawyers need Internet access for email, to conduct research, for access to programs and data (if they have hosted servers) and for phone service (if they have a VoIP phone system). Losing that access for any extended period of time could easily constitute a disaster and partially or completely shut down a law firm's ability to work normally.

F. **Death, Disability or Departure of Principal or Key Employee**: The death or disability of a principal can be devastating, particularly if there was no business succession plan in place. A firm can also grind to a halt if a key administrative person leaves or dies and none of what that person did was written down and no one remaining knows how to handle those tasks. Finally, if a key lawyer leaves and takes all of the knowledge regarding a particular practice area (and clients) with them, it can create a serious problem. This is far more common than you may think.

G. **Theft**: We have seen cases in which thieves break into a law office and take the computers, the server and even the backups.

[4] Panama Papers Law Firm Targets Eight Former Employees But Still Alleges System Hack, by Kenneth Rijock, May 14, 2016, Caribbean News Now!, see http://tinyurl.com/z9t8ndv.

IV. **YOUR ETHICAL DUTIES**: I've only reproduced the sections of the rules and comments below which are relevant to this discussion. Further, I've bolded the particularly important text. In 2013, the American Bar Association promulgated amendments to the Model Rules of Professional Conduct which dealt with technology and data security. 28 states have adopted those changes (for a full list, see http://tinyurl.com/yb9jloml). However, as of yet, South Carolina has not adopted the changes. Below, I've shown the relevant South Carolina rules and the ABA rules where they're different. It's obviously impossible to practice law in a technological vacuum so I would expect South Carolina to adopt at least some of the changes below.

A. **SC RULE 1.1 - Competence**: A lawyer shall provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation.

B. **SC RULE 1.1 - Maintaining Competence Comment [6]**: To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, engage in continuing study and education and comply with all continuing legal education requirements to which the lawyer is subject.

C. **ABA MODEL RULE 1.1 - Maintaining Competence Comment [8]**: To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, ***including the benefits and risks associated with relevant technology***, engage in continuing study and education and comply with all continuing legal education requirements to which the lawyer is subject.

D. **SC RULE 1.6 - Confidentiality of Information**:

(a) A lawyer shall not reveal information relating to the representation of a client unless the client gives informed consent, the disclosure is impliedly authorized in order to carry out the representation or the disclosure is permitted by paragraph (b).

…

E. **ABA MODEL RULE 1.6 - Confidentiality of Information**:

(a) A lawyer shall not reveal information relating to the representation of a client unless the client gives informed consent, the disclosure is impliedly authorized in order to carry out the representation or the disclosure is permitted by paragraph (b).

…

(c) **A lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client.**

F. **SC RULE 1.6 - Comment 19**: **A lawyer must act competently to safeguard information relating to the representation of a client** against inadvertent or unauthorized disclosure by the lawyer or other persons who are participating in the representation of the client or who are subject to the lawyer's supervision. See Rules 1.1, 5.1 and 5.3.

G. **ABA MODEL RULE 1.6 Comment 18**: **Paragraph (c) requires a lawyer to act competently to safeguard information** relating to the representation of a client against unauthorized access by third parties and against inadvertent or unauthorized disclosure by the lawyer or other persons who are participating in the representation of the client or who are subject to the lawyer's supervision. See Rules 1.1, 5.1 and 5.3. **The unauthorized access to, or the inadvertent or unauthorized disclosure of, information relating to the representation of a client does not constitute a violation of paragraph (c) if the lawyer has made reasonable efforts to prevent the access or disclosure. Factors to be considered in determining the reasonableness of the lawyer's efforts include, but are not limited to, the sensitivity of the information, the likelihood of disclosure if additional safeguards are not employed, the cost of employing additional safeguards, the difficulty of implementing the safeguards, and the extent to which the safeguards adversely affect the lawyer's ability to represent clients (e.g., by making a device or important piece of software excessively difficult to use). A client may require the lawyer to implement special security measures not required by this Rule or may give informed consent to forgo security measures that would otherwise be required by this Rule.** …

H. **SC RULE 1.6 Comment 20**: When **transmitting a communication** that includes confidences or secrets of a client, the **lawyer must take reasonable precautions to prevent the information from coming into the hands of unintended recipients**. This duty, however, does not require that the lawyer use special security measures **if the method of communication affords a reasonable expectation of privacy**. **Special circumstances, however, may warrant special precautions. Factors to be considered in determining the reasonableness of the lawyer's expectation of confidentiality include the sensitivity of the information and the extent to which the privacy of the communication is protected by law or by a confidentiality agreement. A client may require the lawyer to implement special security measures not required by this Rule.** (nearly identical to the ABA Model Rule 1.6 Comment 19)

I. **SC RULE 5.1 - Responsibilities of partners, managers and supervisory lawyers**:

(a) A partner in a law firm, and a lawyer who individually or together with other lawyers possesses comparable managerial authority in a law firm, **shall make reasonable efforts to ensure that the firm has in effect measures**

giving reasonable assurance that all lawyers in the firm conform to the Rules of Professional Conduct.

(b) **A lawyer having direct supervisory authority over another lawyer, including a suspended lawyer employed pursuant to Rule 34, RLDE, Rule 413, SCACR, shall make reasonable efforts to ensure that the other lawyer conforms to the Rules of Professional Conduct.**

(c) **A lawyer shall be responsible for another lawyer's violation of the Rules of Professional Conduct if**:

(1) **the lawyer orders or, with knowledge of the specific conduct, ratifies the conduct involved**; or

(2) **the lawyer is a partner or has managerial authority in the law firm in which the other lawyer practices, or has direct supervisory authority over the other lawyer, and knows of the conduct at a time when its consequences can be avoided or mitigated but fails to take reasonable remedial action**.

(d) Partners and lawyers with comparable managerial authority who reasonably believe that a lawyer in the law firm may be suffering from a significant impairment of that lawyer's cognitive function shall take action to address the concern with the lawyer and may seek assistance by reporting the circumstances of concern pursuant to Rule 428, SCACR.

J. SC RULE 5.3 - Responsibilities Regarding Nonlawyer Assistants: This rule makes Rule 1.6 apply to everyone that works for the lawyer (not just the lawyers). It further makes the lawyer(s) responsible for the conduct (and mistakes) of nonlawyer assistants.

With respect to a nonlawyer employed by, retained by, or associated with a lawyer:

(a) a partner and a lawyer, who individually or together with other lawyers possess comparable managerial authority in a law firm, shall make reasonable efforts to ensure that the firm has in effect measures giving reasonable assurance that the nonlawyer's conduct is compatible with the professional obligations of the lawyer;

(b) **a lawyer having direct supervisory authority over the nonlawyer, including a suspended lawyer employed pursuant to Rule 34, RLDE, Rule 413, SCACR, shall make reasonable efforts to ensure that the person's conduct is compatible with the professional obligations of the lawyer**; and

(c) **a lawyer shall be responsible for the conduct of a nonlawyer that would be a violation of the Rules of Professional Conduct if engaged in by a lawyer if**:

(1) the lawyer orders or, with the knowledge of the specific conduct, ratifies the conduct involved; or

(2) **the lawyer is a partner or has comparable managerial authority in the law firm in which the person is employed, or has direct supervisory authority over the person, and knows of the conduct at a time when its consequences can be avoided or mitigated but fails to take reasonable remedial action.**

V. **TOOLS AND PROTOCOLS TO PROTECT CLIENT DATA**: Now that you know the rules affecting this issue, here are some tools and techniques to keep your client data safe.

A. **Encryption Defined**: For purposes of this discussion, encryption can be defined as follows.

> "Encryption is the process of converting data to an unrecognizable or 'encrypted' form. It is commonly used to protect sensitive information so that only authorized parties can view it. This includes files and storage devices, as well as data transferred over wireless networks and the Internet.
>
> …
>
> An encrypted file will appear scrambled to anyone who tries to view it. It must be decrypted in order to be recognized. Some encrypted files require a password to open, while others require a private key, which can be used to unlock files associated with the key."[5]

B. **Lawyers Must Encrypt Laptops, Tablets and Phones**:

1. **Duty To Protect**: If you are carrying confidential client data on any of these devices, "reasonable efforts" to maintain confidentiality cannot possibly include doing nothing to protect it.

> "Not properly protected, laptops and portable media can be recipes for a security disaster. One survey reported that 70 percent of data breaches resulted from the loss or theft of off-network equipment (laptops, portable drives, PDAs, and USB drives). Strong security is a must. Encryption is

[5] See http://techterms.com/definition/encryption

> now a standard security measure for protecting laptops and portable devices—and attorneys should be using it."[6]

2. **PC Encryption**: If you've got a notebook computer, there's always the chance that someone will steal it or that you'll misplace or otherwise lose it. If you have confidential client information on the laptop, then it would be prudent for you to encrypt the laptop. Encryption would prevent a thief or finder of your laptop from obtaining any information from the hard drive, even if they remove the hard drive and install it in another computer. There are many choices for this type of software, including the following:

   a. **BitLocker** - included for free with certain versions of Windows Vista, 7, 8 & 10.

   b. **Mac FileVault** - included for free with OSX.

   c. **SecuriKey Pro** - https://www.securikey.com/

   d. **Symantec Drive Encryption** - http://tinyurl.com/39seow

   e. **AlertBoot** - http://tinyurl.com/63h36wt

   f. **Folder Lock** - http://www.newsoftwares.net/folderlock/

   g. **SecureDoc Full Disk Encryption** from Winmagic Data Security - http://tinyurl.com/4vek6ot

3. **Smartphones**: All of the smartphone operating systems have free encryption built in, you must only enable it. Make sure you do this.

4. **Tablets**: Like smartphones, Android and iOS tablets have built-in encryption that you must simply turn on. Windows tablets may also have BitLocker depending upon the version of Windows installed. Of course, any of the Windows encryption options above would also work (besides BitLocker).

C. Email Encryption:

1. **Revisit SC Rule 1.6, Comment 20**: Let's look at that again.

> "When transmitting a communication that includes confidences or secrets of a client, the lawyer must take

[6] Encryption Made Simple for Lawyers, by David G. Ries & John W. Simek, GP Solo, November/December 2012 - see http://tinyurl.com/znh4jqz

> reasonable precautions to prevent the information from coming into the hands of unintended recipients. "

The questions to consider are: What constitutes "reasonable precautions" to protect the client's data; and do you have a reasonable expectation of privacy when you use email? I would argue that reasonable precautions means that you must encrypt your email when sending sensitive documents. Further, although the ethical rules and case law presume that lawyers have a reasonable expectation of privacy when sending an email, common sense has to tell you otherwise.

2. **What The Experts Say**: Here are a couple of quotes to consider.

> "A secure email account that the attorney is assured protects the content of correspondence. No attorney should use Gmail or other free services that in fact admit that they use personal information from email content. They should encrypt their client correspondence. Before sending sensitive correspondence, they should check by phone or text with the client to see what method of delivery is preferred."[7]
>
> "The level of encryption may vary based on practice areas or, more importantly, the firms' clients. At a minimum, emails and attachments that contain confidential data should be encrypted or sent through collaboration tools that send encrypted links rather than plain text data."[8]
>
> "It's all about encryption of the 3 main risk areas for data held: data in transit, at rest and in backups. It doesn't matter if it's email, Instant Messages, case files, discovery or 3rd party expert communications, the principle of encryption is the ONLY way you can really satisfy due diligence requirements."[9]

3. **Email Encryption Services**: There are many ways to encrypt email, but the easiest is to use an encryption service. The options listed below are inexpensive and easy. They encrypt both the emails and any attachments to the email. In most cases, a password must be entered by the recipient to open the email and any attachments.

---

[7] Law Firm Data Security: Experts on How to Protect Legal Clients' Confidential Data, by Nate Lord, DigitalGuardian, October 13, 2015, quoting Robert Ellis Smith. See http://tinyurl.com/h6nzvjb.
[8] ibid., quoting Marco Maggio.
[9] ibid., quoting Steve Santorelli.

a. **Protected Trust**: https://protectedtrust.com/ - this is easily my favorite option.

b. **SenditCertified**: http://www.senditcertified.com/ and note that they offer discounts through several bar associations.

c. **EchoWorx Encrypted Mail**: http://tinyurl.com/h6sm668

d. **Hightail**: https://www.hightail.com/ - this service was formerly known as YouSendIt.com. It's designed for sending enormous attachments, but also offers encryption for those attachments. Incredibly easy to use and inexpensive.

e. **Hushmail**: https://www.hushmail.com/

f. **RMail**: http://www.rmail.com/ - registered email service which can prove delivery + encrypted email

g. **ZixMail**: https://www.zixcorp.com/

h. **ShareFile**: https://www.sharefile.com/

4. **Encrypt Email Attachments**: Word, WordPerfect and every good PDF program including Acrobat offers file encryption. This functionality is built-in so you only have to learn how to use it. With file encryption file simply cannot be opened without a password. You email could unencrypted and simply say "Please see attached." However, the attached file containing the sensitive information would be encrypted on its own.

D. Wireless Encryption:

1. **Home or Work Wireless Connections**: If you rely on a wireless Internet connection at your office or home to work with sensitive client information, it goes without saying that your wireless router or access point should be properly encrypted. If you set it up yourself and aren't sure, then you should immediately secure the assistance of an expert to ensure that your security is properly configured. Sometimes, it's as easy as calling the technical support line for the manufacturer of your router. The big companies that sell wireless routers all have technical support representatives that can walk you through the process over the phone. In case you're wondering, big names in wireless routers include Cisco, Linksys, Netgear, Belkin, TP-Link, D-Link and Asus, among others.

2. **Risk of Using Public WiFi**: First of all, you need to be educated about this subject. For a quick primer, here are two short articles that will bring this

issue into focus: Here's what an eavesdropper sees when you use an unsecured Wi-Fi hotspot by Eric Geier, 6/28/13 (see http://tinyurl.com/ppm3oyc) and What Is A Packet Sniffer? by Andy O'Donnell, 12/15/14 (see http://tinyurl.com/jxvhf92). For an interesting discussion of this in the legal arena, see the now famous California Formal Opinion No. 2010-179 which states:

> "With regard to the use of a public wireless connection, the Committee believes that, due to the lack of security features provided in most public wireless access locations, **Attorney risks violating his duties of confidentiality and competence in using the wireless connection at the coffee shop to work on Client's matter unless he takes appropriate precautions, such as using a combination of file encryption, encryption of wireless transmissions and a personal firewall**. Depending on the sensitivity of the matter, Attorney may need to avoid using the public wireless connection entirely or notify Client of possible risks attendant to his use of the public wireless connection, including potential disclosure of confidential information and possible waiver of attorney-client privilege or work product protections, and seek her informed consent to do so."[10]

3. **How To Protect Yourself**:

   a. **Cellphone WiFi Hotspot**: Rather than connecting to the public WiFi where ever you are, consider using a cellular hotspot or MiFi. Properly configured, these connections are a secure way to connect your notebook or tablet to the Internet via the phone hotspot.

   b. **Consumer VPN Services**: There are many services that allow you to create a Virtual Private Network connection even though you're using a public and otherwise unsecured WiFi connection. "In the simplest terms, a VPN creates a secure, encrypted connection between your computer and the VPN's server. This tunnel makes you part of the company's network as if you are physically sitting in the office, hence the name. While connected to the VPN, all your network traffic passes through this protected tunnel, and no one in between can see what you are up to. A consumer VPN service does the same thing, but extends that

[10] See http://tinyurl.com/3szklcx, emphasis added.

protection to the public."[11] Here are some options for this. Private Internet Access is the one I use personally.

i. **Hide My Ass**: https://www.hidemyass.com/

ii. **Private Internet Access**: https://www.privateinternetaccess.com/

iii. **IPVanish**: https://www.ipvanish.com/

iv. **PureVPN**: https://www.purevpn.com/

v. **Cloak** (Mac only): https://www.getcloak.com/

vi. **CyberGhost**: http://www.cyberghostvpn.com/en_us

vii. **VyprVPN**: https://www.goldenfrog.com/vyprvpn

viii. **NordVPN**: https://nordvpn.com/

ix. **Hotspot Shield Elite**: https://hsselite.com/

x. **Spotflux Premium**: http://spotflux.com/

E. Firewall:

1. **What Is a Firewall**: A firewall is a network security system designed to prevent unauthorized access to or from a private network. Firewalls can be hardware, software, or a combination of both.[12]

2. **Your Obligation**: You need to ensure that a firewall is in place at your office and anywhere you use your computer and connect to the Internet. You can test yourself using services like ShieldsUP![13] or HackerWatch[14]. If you aren't sure if you are being protected, then you should contact a security expert to conduct a penetration test. Penetration testing (also called pen testing) is the practice of testing a computer system, network or Web application to find vulnerabilities that an attacker could exploit.[15]

F. Password Manager: On this subject, also see paragraph V.L.3. below (Secure Password Policy).

---

[11] The Best VPN Services for 2016, by Max Eddy, Fahmida Rashid, 3/9/2016, PCMag - see http://tinyurl.com/njuv7br.
[12] See http://www.webopedia.com/TERM/F/firewall.html
[13] See https://www.grc.com/x/ne.dll?bh0bkyd2
[14] See http://www.hackerwatch.org/probe/
[15] See http://searchsoftwarequality.techtarget.com/definition/penetration-testing

1. **What Is a Password Manager**: A password manager is a program that helps one store, create and organize passwords (and logons and websites, etc.).

2. **Why You Need A Password Manager**: First, it's part of your estate plan. Second, it's a place to keep logons, websites, account numbers and passwords all in one place. I use Dashlane and it will generate and store strong passwords for me (so I don't have to make them up). It will also let me know if my passwords are weak and recommend that I change them. It tells me how many different websites I'm using the same password for (it's not recommended that you use the same password for everything). It also lets me know if there are any reported security breaches for any of the websites it holds passwords for and recommend that you change them. Finally, it will hold all of my credit card information, secure notes about anything I want and personal information like my driver's license, passport, etc.

3. **Good Options**: Top rated password managers include the following (and I strongly recommend the versions you have to pay for - almost all offer a free version that is missing features):

    a. **Dashlane** - https://www.dashlane.com/

    b. **LastPass** - https://www.lastpass.com/

    c. **Sticky Password** - https://www.stickypassword.com/

    d. **LogMeOnce** - https://www.logmeonce.com/

    e. **TrueKey** - https://www.truekey.com

    f. **RoboForm** - https://www.roboform.com/

    g. **Keeper Desktop** - https://keepersecurity.com/

G. Two Factor Authentication: This is also known as 2FA or multi factor authentication.

1. **What Is Two Factor Authentication?** Here's a good definition.

    "Two-factor authentication (2FA), often referred to as two-step verification, is a security process in which the user provides two authentication factors to verify they are who they say they are. 2FA can be contrasted with single-factor authentication (SFA), a security process in which the user provides only one factor -- typically a password.

Two-factor authentication provides an additional layer of security and makes it harder for attackers to gain access to a person's devices and online accounts, because knowing the victim's password alone is not enough to pass the authentication check. Two-factor authentication has long been used to control access to sensitive systems and data, and online services are increasingly introducing 2FA to prevent their users' data from being accessed by hackers who have stolen a password database or used phishing campaigns to obtain users' passwords.

The ways in which someone can be authenticated usually fall into three categories known as the factors of authentication, which include:

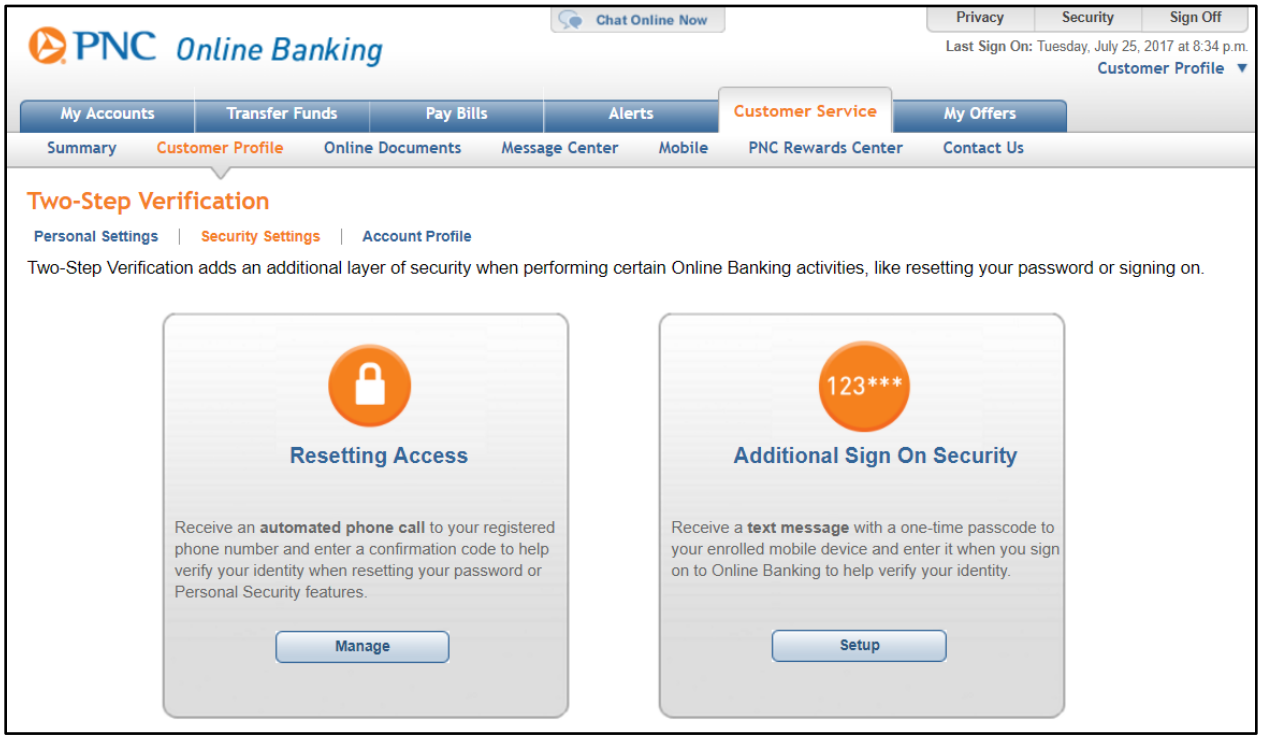
1. **Knowledge factors** -- something the user knows, such as a password, PIN or shared secret.

2. **Possession factors** -- something the user has, such as an ID card, security token or a smartphone.

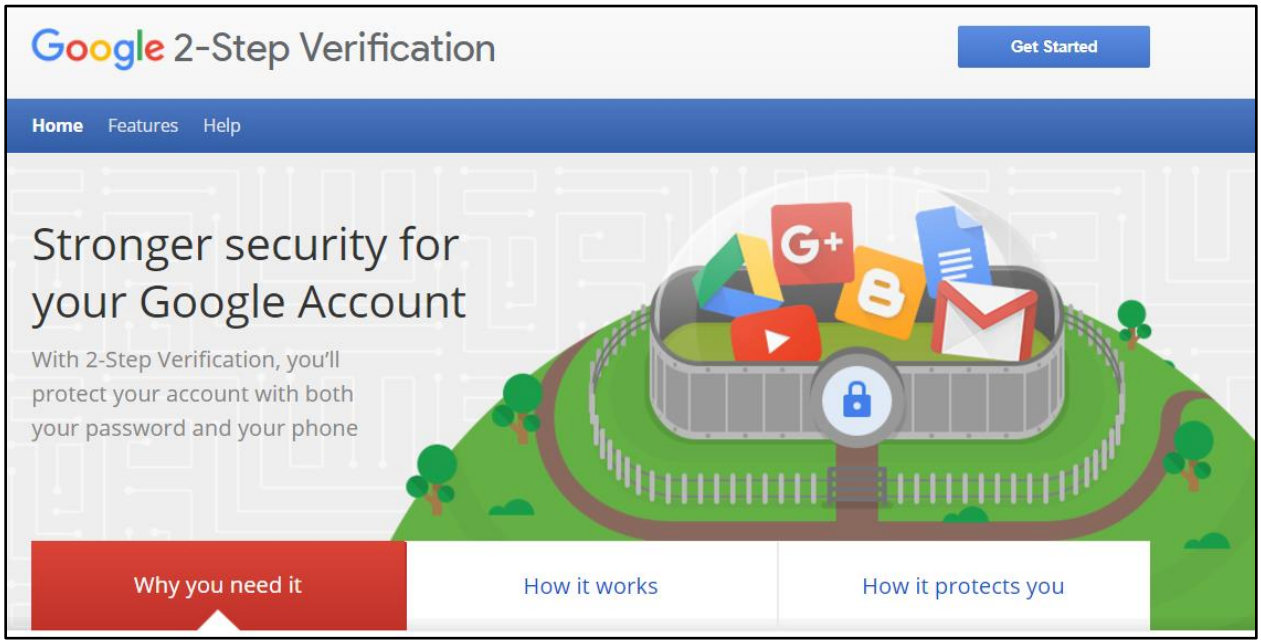
3. **Inherence factors, more commonly called biometrics** -- something the user is. These may be personal attributes mapped from physical characteristics, such as fingerprints, face and voice. It also includes behavioral biometrics, such as keystroke dynamics, gait or speech patterns."[16]

[16] See http://searchsecurity.techtarget.com/definition/two-factor-authentication

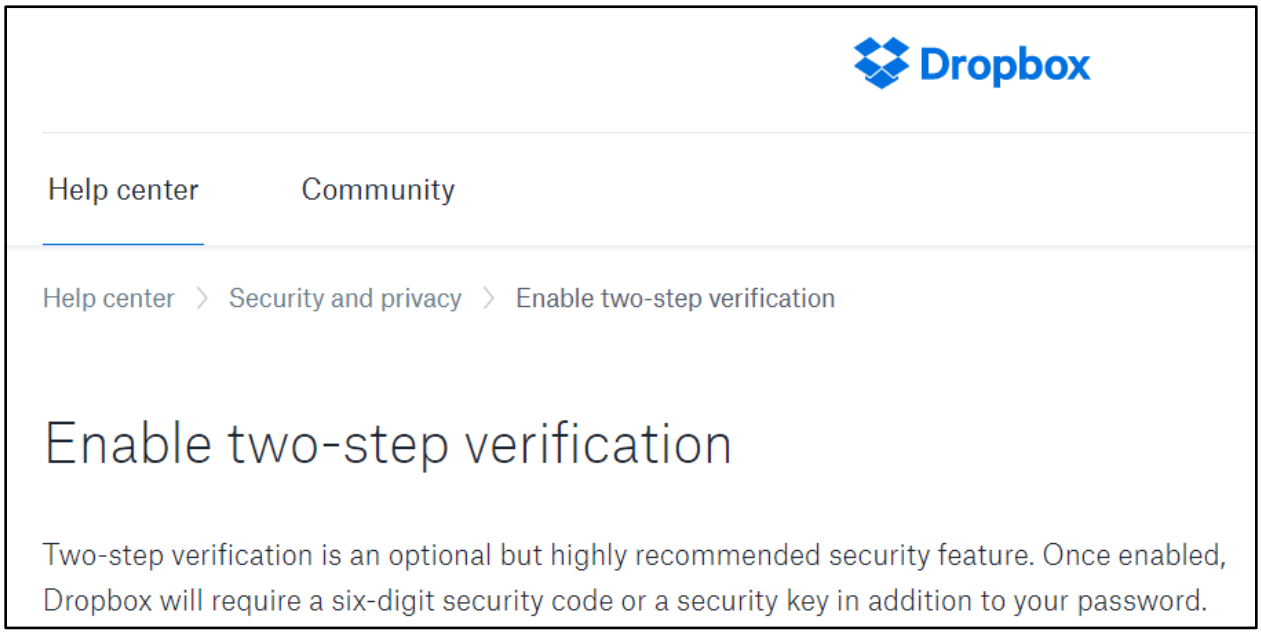
2. **How Do You Get 2FA?** For critical services you access online, check to see if they offer any type of 2FA. Keep in mind that 2FA is ANNOYING, but better security is almost always more annoying. If you want to protect yourself well, be prepared to be slightly annoyed. Anyway, here are some 2FA ideas. Your bank probably offers it:



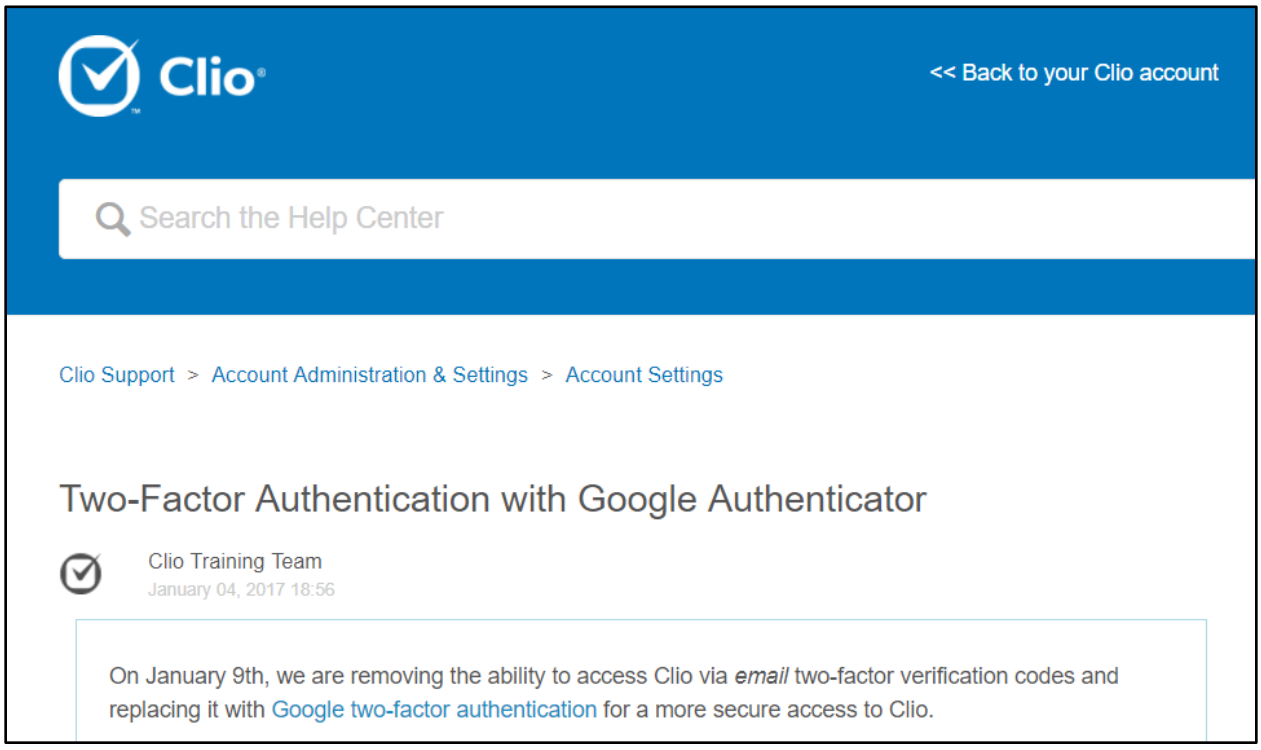
Your email account probably offers it:



Your file sharing service probably offers it:

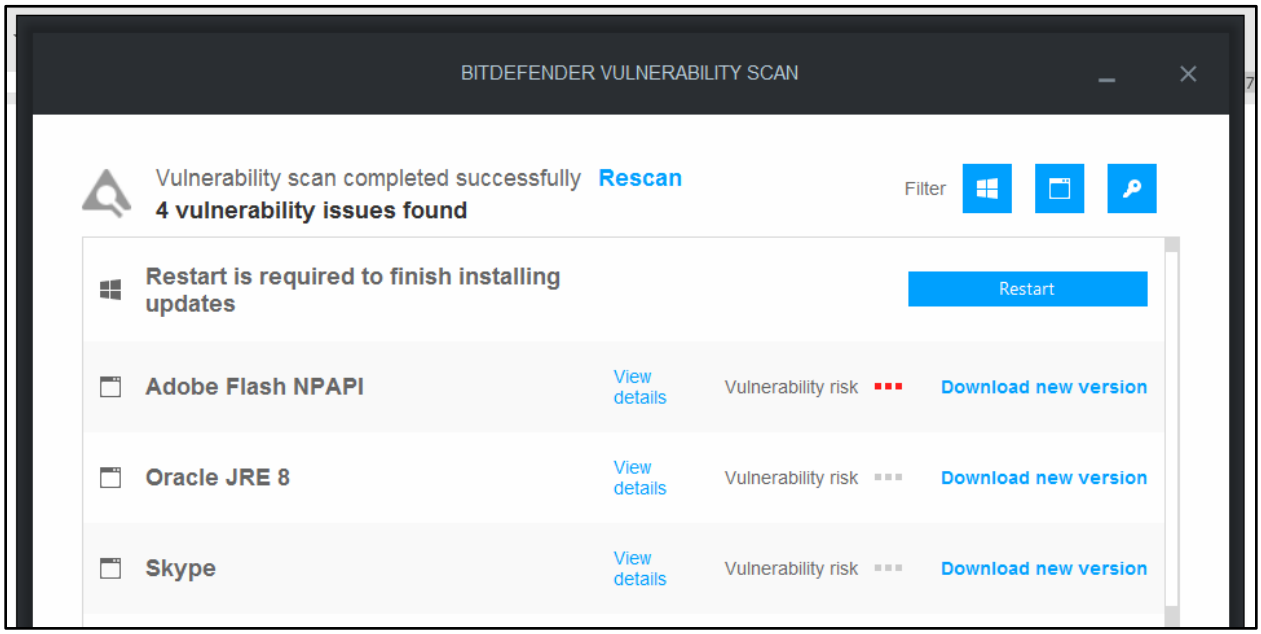


Your case management system probably offers it:



H. **Antivirus/Antimalware Software**: It is fairly common that users think they have protective software running when they actually do not. You should be able to confirm that protective software is running on your computer(s). Again, you may

need to consult an expert. I personally use Bitdefender[17] which I *really* like. Of course, there are many good options available from McAfee, Webroot, Symantec (Norton) and Kaspersky. A good security suite (like Bitdefender Internet Security 2016) provides antivirus, web protection, vulnerability testing (to make sure you have the latest versions of programs that may represent vulnerabilities), a firewall, intrusion detection, antispam and ransomware protection. For example, when I first ran the Bitdefender vulnerability test, it produced the following which not only told me which programs needed to be updated, but also provided links so I could get to them quickly:



I. **Secure File Sharing and Data Rooms**: Make absolutely sure that all file shares have a password required to access them.

1. **ShareFile by Citrix**: https://www.sharefile.com/ - This is a fantastic service that allows you to create virtual "rooms" for others and share documents with them securely. You decide what rights each user has to the collection of documents.

2. **Merrill DataSite Virtual Data Room**: See http://tinyurl.com/laam53o.

3. **Firmex Virtual Data Room**: See https://www.firmex.com/.

4. **SmartRoom Virtual Data Room**: See http://smartroom.com/.

5. **Ansarada Virtual Data Room**: See https://www.ansarada.com/

[17] See http://www.bitdefender.com/

6. **IntraLinks Virtual Data Room**: See http://preview.tinyurl.com/lt6d899.

7. **Microsoft Office 365 or OneDrive for Business**: OneDrive is Microsoft's cloud storage offering and it comes with nearly every Office 365 plan. For only $5/user/month (Business Essentials plan), you get 1 TB of online storage. See this: http://tinyurl.com/h9mdn2v

8. **G Suite by Google Cloud**: The Basic edition is $5/user/month and includes 30 GB of cloud storage; the Business edition is $10/user/month and includes unlimited cloud storage. See your options here: http://tinyurl.com/kkocuto

9. **Dropbox Business Standard or Advanced**: Standard is $12.50/user/month and Advanced is $20/user/month. For an explanation of their business plans, see https://www.dropbox.com/business/plans-comparison.

10. **SpiderOak Professional**: See this for more: https://spideroak.com/business_pricing/

11. **Syncplicity**: See https://www.syncplicity.com/.

12. **Box.com**: https://www.box.com/pricing

13. **TrueShare**: http://www.trueshare.com/

14. **FileGenius**: http://www.filegenius.com/

15. **OneHub**: Secure file sharing - see https://onehub.com.

J. **Encryption Options for Online Sync Programs Like Dropbox, OneDrive, Box and Google Drive**: There are inexpensive and easy-to-use services that will encrypt your files before sync and file-sharing services. These services will effectively eliminate your ability to share files with individuals outside of your office, but they also provide complete protection for your files as they are encrypted before the sync service ever gets your files.

1. **Viivo**: See https://www.viivo.com/

2. **Sookasa**: See https://www.sookasa.com/

3. **BoxCryptor**: See https://www.boxcryptor.com/en

K. **External Hard Drive and Flash Drive Encryption**: If you need to use external hard drives or flash drives, there are many choices for encrypted devices. Of

course, you can also use encryption programs like BitLocker to encrypt external devices as well. In any event, here are some options:

1. **External USB Hard Drives**:

    a. **Apricorn Aegis Padlock 2 TB** USB external hard drive.

    b. **Fantom Drives DSH2000 DataShield 2TB** USB external hard drive.

    c. **Lenovo ThinkPad USB 3.0 Secure** Hard Drive.

2. **Flash Drives**:

    a. **Apricorn Aegis Secure Key** FIPS Validated 4 GB USB 2.0 256-bit AES-CBC Encrypted Flash Drive

    b. **Kingston Digital 8GB Data Traveler** AES Encrypted Vault Privacy 256Bit 3.0 USB Flash Drive

    c. **IronKey S250 8 GB** USB 2.0 Flash Drive

L. **Develop and Follow Policies**: There are many places to find sample policies for the following and a great resource is the SANS Institute. To see their sample policies, just go here: https://www.sans.org/security-resources/policies.

1. **Internet and Email Usage Policy**: There may be (and likely is) a big gap between what you would deem acceptable use of company internet and email and what your employees deem acceptable use of those resources. Thankfully, you can Google "internet usage policy" and find many free examples to start with.

2. **Document and Email Retention Policy**: Lawyers tend to hold onto every document and email forever and this is simply a bad policy. You can end up with so much irrelevant digital clutter that you're unable to find the things you actually need. Your policy should comply with any applicable federal or state laws, the Rule of Professional Conduct and any other relevant regulations. It's also a great idea to contact your malpractice insurer to see what they recommend (they may even have a sample policy you could start with). The ABA has a nice compilation of records and document retention resources (http://tinyurl.com/7z8ksye) and another excellent article to read on the subject is Sample Document-Destruction Policy by Megan Zavieh, 1/21/14, Lawyerist.com (see http://tinyurl.com/hrs3hxy).

3. **Secure Password Policy**:

   a. **Why You Need This**: You need a secure password policy because of the plethora password crackers that are out there.

   b. **Types of Password Hackers**: Here are the main types (there are many more):

      i. **Dictionary attack**: This attack uses a file that contains a list of words that are found in the dictionary. This mode matches different combinations of those words to crack your device open.

      ii. **Brute force attack**: Apart from the dictionary words, brute force attack makes use of non-dictionary words too.

      iii. **Rainbow table attack**: This attack comes along with pre-computed hashes. When user passwords are stored by a service (say www.Target.com), the raw (actual) passwords are converted into a string of random characters by complicated mathematical computations. This conversion process is called hashing. For an extremely interesting article on this technology, see Hacker Lexicon: What Is Password Hashing? by Andy Greenberg, June 8, 2016[18].

   c. **Examples of Password Hackers**: Just so you can appreciate how readily available these are to anyone.

      i. **John The Ripper** - http://www.openwall.com/john/

      ii. **Aircrack-ng** - https://www.aircrack-ng.org/downloads.html

      iii. **RainbowCrack** - http://project-rainbowcrack.com/

      iv. **Crowbar** - https://github.com/galkan/crowbar

      v. **Ophcrack** - http://tinyurl.com/3uyvmy

      vi. **L0phtcrack** - http://www.l0phtcrack.com/#download-form

      vii. **DaveGrohl** - https://github.com/octomagon/davegrohl

[18] See https://www.wired.com/2016/06/hacker-lexicon-password-hashing/

There are many others like Cain and Abel, THC Hydra and HashCat.

d. **Recommended Policy**: I will warn you that a really strong password security policy can be extremely annoying because most of them recommend that you change your password every 30 days, don't repeat old ones and use unique passwords for each logon. While I appreciate the value of those rules, they would drive most people batty in short order. Here are some less annoying rules that will still help ensure your passwords are secure:

- 12 Characters, Minimum: You need to choose a password that's long enough. There's no minimum password length everyone agrees on, but you should generally go for passwords that are a minimum of 12 to 14 characters in length. A longer password would be even better.

- Include Numbers, Symbols, Capital Letters, and Lower-Case Letters: Use a mix of different types of characters to make the password harder to crack.

- No Dictionary Words or Combination of Dictionary Words: Avoid obvious dictionary words and combinations of dictionary words. Any word on its own is bad. Any combination of a few words, especially if they're obvious, is also bad. For example, "Wagon" is a terrible password. "RedWagon" is also very bad.

- Doesn't Rely on Obvious Substitutions: Don't use common substitutions, either — for example, "RedWag0n" isn't strong just because you've replaced an o with 0.[19]

4. **Mobile Device Security Policy**: This policy describes protocols that must be used when using notebooks, tablets or phones to conduct legal work.

5. **Equipment Disposal Policy**: The general rule is that no mobile device, PC or copier should ever be disposed of while it still contains client data.

6. **Litigation Hold Policy**: "If you don't have one, you're asking for trouble. If you know you have been sued or are the subject of a regulatory action, or that either one is likely to occur, you are under a litigation hold and

[19] See How to Create a Strong Password (and Remember It) by Chris Hoffman, 5/29/15, How-To- Geek, see http://tinyurl.com/kx6s7uf.

must proceed expeditiously to preserve the relevant electronically stored information."[20] A couple of good resources to start with are:

- Ten Things to Consider When Establishing a Legal Hold Policy by Stephanie Fox (4/26/2013), Association of Corporate Counsel, see http://tinyurl.com/zspaybw.

- Implementing a Litigation Hold by Nicholas Panarella and Wook Kim, Kelley Drye LLP (2012) Practical Law Publishing Limited and Practical Law Company, Inc., see http://tinyurl.com/hh4kwy2.

M. **Training**: The biggest hole in every organization's security are the users. It is imperative that tools are provided and that training is mandatory.

VI. PAPER REDUCTION STRATEGY:

A. **Disadvantages of Being Paper Dependent**: If all of your case information and the answers you need are on paper, you're at a disaster-avoidance disadvantage. Here are some reasons why moving away from paper dependence should be part of your disaster avoidance plan.

1. **Paper Is Easily Lost or Destroyed**: Water and fire easily destroys paper and most law offices do not maintain parallel, duplicate paper files to protect against this. Unlike digital data, it's almost impossible to create a back-up of paper files. Further, since people must have possession of a paper file in order to work on it, paper files move around a lot. As a result, they are often misplaced or lost.

2. **Paper Dependence Can Mean You're Cut Off from Case Information**: If all of the information you need is in a paper file at the office but you can't get to the office, then you can't get work done. Evacuations, power outages and all manner of natural disaster can prevent you from getting to your office. If that information were electronic, you'd be able to easily make copies of it, access it remotely and/or share it with others.

3. **More Paper Means Limited Lawyer Mobility**: If you have 4 files to take with you somewhere and they're reasonably thick, you're going to need a bag or a cart or a box. This is unwieldy, annoying and difficult.

4. **Managing Paper Files Is Expensive**: Law firms spend a huge amount of non-billable, administrative time looking for paper files and they're rarely easy to find. For example, files might be in a lawyer's office (on the desk, under the desk, on the floor, in a cabinet or on a shelf), in a secretary or

[20] Essential Law Firm Technology Policies and Plans by John W. Simek and Sharon D. Nelson, Law Practice Magazine, March/April 2012, see http://tinyurl.com/8yvvdkq.

paralegal's cube or office, on a counter in a hallway, on a ledge somewhere in the office, in a filing cabinet (imagine that!), in the wrong filing cabinet, in someone's car, at someone's home or in someone's briefcase or bag. That's a lot of places to look. The cost associated with finding files can be very high. Let's say you've got 5 attorneys and they each spend 15 non-billable minutes a day each looking for files which they could otherwise bill at $250/hour. This translates into 6.25 hours per week and at $250/hour, that's $1,562.50/week, $6,250 per month or $75,000 per year.

5. **Creating and Maintaining Paper Files Is Expensive**: Paper, toner, folders, labels and the labor necessary for the care and feeding of a paper-based filing system is incredibly expensive. Another area of savings is postage. Once everything is digital, documents are transmitted and shared electronically which is not only faster, but far less expensive. For example, we have a law firm client in Clearwater, Florida which reduced their annual postage expenditures from $75,000 down to $35,000 by creating and maintaining complete electronic files.

6. **Paper Files Can Only Be In One Place at a Time**: We all know this, but it creates problems. If I find the paper file I've been looking for, then I've "captured" it and no one else can look at it. In other words, the act of removing a file to work on it causes that file to be lost again to everyone else in my office because they don't know where it is. There may have been a few people in the office who actually knew where the file was when I found it. Now that I've taken it, they may be running around the office asking, "who took my file??" By finding and taking the file, I have unwittingly annoyed and stressed those who knew where it was when I found it and are expecting it to still be there when they go looking for it.

7. **Paper Files Are Not Sharable**: You can share a paper file no more easily than you can share a book you're reading.

8. **If You Can't Share, You Can't Collaborate**: We need to collaborate with clients, experts, courts and co-counsel. If you're all paper and you want to share your file, you're spending money on lots of copies, shipping boxes and the whole process is slow.

9. **Difficulty Finding the Document Once You've Found the File**: Once you locate the paper file, now you begin the second search - finding the individual piece of paper within that file.

10. **Paper Files Are Not Searchable**: If a paper files were "searchable," you would be able to instantly locate every document from any file in your office which contains certain words (e.g., "force majeure" or "liquidated

damages") or has certain characteristics (e.g., it is an appellate brief or a Will containing a special needs trust). You obviously can't do that with your paper files. Further, paper files do not contain a table of contents and although they may be have separate sub-parts for correspondence, pleadings and the like, that doesn't mean that people who deposit paper into the file have actually utilized that organizational structure. It also doesn't mean that things are actually clipped into the file, nor that the items in the file are in any kind of chronological order. In other words, the file may be (and often is) a mess. That being the case, now you have to find that ONE piece of paper you're looking for among hundreds, maybe thousands of pages, possibly in no particular order. Depending on the size and organization of the file, you may be faced with a bigger search than finding the file in the first place.

11. **Accessing Data on Paper Is Slow**: We're in the age of instant information. We need it and our clients expect it. If your data and case information is locked up in a paper file, you're at a significant speed disadvantage.

12. **Paper Files Are Rarely Updated in a Timely Manner**: Almost every piece of mail that comes into a firm ends up in a paper file somewhere. Of course, those files must be found first, updated, then re-filed into a cabinet (or more likely stacked on someone's desk or the floor of someone's office). Anyone who has ever been saddled with the task of filing a pile of documents/mail/pleadings into paper files knows how unpleasant it is. If you've never done it yourself, just ask your support staff which aspect of their jobs they find the most mind-numbing, frustrating and distasteful. "Filing" is probably the answer you'll get.

    Human nature dictates that if you give someone a task they detest, they will put it off as long as possible. That is usually what happens with filing. At any given time, the person responsible for filing in your office probably has a nice stack of unfiled documents sitting around somewhere. The time gap between receipt of a document and its ultimate insertion into a file in your office can create problems. During that time, those unfilled documents are effectively lost.

13. **More Paper Means Higher Operating Costs**: Efficiency is the key to maximizing a firm's profitability. Managing fat paper files is labor intensive and reduces a firm's efficiency on all fronts.

14. **Expensive Storage**: Large paper files occupy a lot of space and filing cabinets are expensive and bulky. If you rent office space by the square foot, you're paying for your filing cabinets every month. More importantly, storage for closed files is VERY expensive. Closed storage is

also typically off-site and disorganized. This means that finding and pulling old files is also expensive in terms of time spent.

B. **The Typical Two File Approach**: Most law firms and legal departments maintain two files for every matter or case they handle. One is paper-based; the other is electronic.

1. **Paper File = Primary File**: You are paper dependent if the paper file is the sole reservoir of all information related to that particular matter.

2. **Electronic File = Secondary File**: The electronic file is comprised of documents stored in a folder structure on someone's computer or on a server or documents stored under a client/matter ID in a Document Management System ("DMS"). The electronic file typically contains only the electronic versions of documents generated internally (Word or WordPerfect files). In some cases, there are a few scanned documents in these files as well. Regardless, the electronic file is usually missing documents you received from your client, anything that came from opposing counsel, faxes and the like. Since it contains only a subset of the information in the paper file, the electronic file is usually of limited use.

C. **Creating a Complete Electronic File**: Short of an RFID[21] tag affixed to every file in your office, there may be no perfect way to track them. Since you can't look over everyone's shoulder when they're working on a file, there is probably no way to enforce organizational protocols. But all of those approaches are focusing on the **paper file**. I would argue that it's pointless trying to figure out a magical way to organize, store and retrieve paper files because of their inherent, unavoidable shortcomings outlined above.

Everyone must accept the proposition that banker's boxes and paper file folders are not the future of file management in 21st century law firms. Since we cannot change the nature of a paper file, we propose a solution focusing on the electronic or digital file discussed above. Recall that the paper file is the primary file because it contains everything (incoming and outgoing) while the electronic file typically contains only outgoing materials.

[21] Stands for "Radio-Frequency Identification." RFID is a system used to track objects, people, or animals using tags that respond to radio waves. RFID tags are integrated circuits that include a small antenna. They are typically small enough that they are not easily noticeable and therefore can be placed on many types of objects. Like UPC labels, RFID tags are often used to uniquely identify the object they are attached to. However, unlike UPCs, RFID tags don't need to be scanned directly with a laser scanner. Instead, they can be recorded by simply placing the tag within the range of an RFID radio transmitter. This makes it possible to quickly scan several items or to locate a specific product surrounded by many other items. TechTerms.com - see http://tinyurl.com/nsdoorh.

To be clear, the same folder on a computer or server which currently contains only word processor files can also hold other electronic items such as scanned PDFs and even email (either as MSG or PDF files).

D. **Implementation Steps For A Successful Paper Reduction System**: The approach here is to use a scanner to add incoming documents to your digital file. What you want is an accurate representation of what the original document looked like. However, you also want the scanned documents to be full text searchable. This does not mean that you want to convert your scanned documents into Word or WordPerfect files. You simply want to scan for archival purposes. HOWEVER, you need to be able to find those documents again in the future. The following steps are discussed in greater detail below, but here's the general road-map.

1. Ensure You Have Redundant Backup Systems and Security
2. Acquire Scanners
3. Acquire Scanner Software That Creates Searchable PDFs
4. Acquire Search Program or Document Management System ("DMS")
5. If no DMS, Consolidate Folder Structure and Establish File Naming Conventions
6. Digitize Incoming Documents
7. Store Email Outside of Your Email Application
8. Write Down Your Scanning Protocols
9. Provide Training for all Lawyers and Staff

E. **Redundant Backup And Security**: Before you undertake a paper reduction strategy as outlined herein, you need to make sure you have bullet-proof backups. This is mission critical even if you don't go all digital. No matter what you do, you must get a backup system, it must have redundancy built-in and it is not optional. If you don't take care of this issue, then you're increasing rather than decreasing the likelihood of a disaster. Furthermore, you need to own this issue even if someone else handles all of your computer work. If you lose all of your client data, blaming the IT person won't absolve you from liability under the Rules of Professional Conduct.

1. **Backup Rules for a Law Firm or Legal Department**:

a. **No Excuses**: You must be backing up all of your important data every day. Every day, no matter what.

b. **You Own This Issue**: Never just assume that everything is being backed up. Lawyers need to be responsible for ensuring that it is happening every night and you need to be able to verify that it actually occurred without errors. Ask your IT/computer person how the backup system works (generally), how often it backs up data, and exactly what data is being backed up and how you can verify that everything is being backed up (there is often an easy log you can check).

c. **Unattended Is Best**: The best backup methods do not require you to remember to do anything for the backup to occur. Unattended backups are the best for two important reasons. First, if someone has to remember to do it, they'll forget. Second, backups sometimes take a long time and they'll usually bog down your system when they're running. Therefore, they're best run at night when no one is using your network or their computers. This means that you cannot use backup media that is not large enough to backup all of your data.

d. **Backup Everything**: DO NOT backup only the data you've created (i.e., Word or WordPerfect files, etc.). You want to back up the entire drive of the computer you're backing up. Although you may not want to restore a screwed up computer right back to the way it was before a crash, there are lots of things you'll need which aren't in the standard data folders (Internet favorites, Outlook's database of email, contracts, calendar, drivers, some data, etc.).

e. **You MUST Check the Backup Log Every Day**: Most backup devices don't tell you if they worked properly or not. The only way to make certain is to look at the "backup log" which the tape backup software maintains. Someone needs to do this every single day to make sure there were no malfunctions.

f. **Replace Tape Media At Least Annually**: If you're using a tape drive as a backup device, you need to write a "born-on" date on the tape and replace them at their 1 year birthday. Tapes lose their ability to hold data over time and you don't want to take the risk that your successful backup is not restorable due to bad media.

g. **Never Rely Exclusively on Internet or Cloud Backups**: Many lawyers are using online backup options like Mozy Pro (www.mozy.com) or Carbonite (www.carbonite.com). However, these should be secondary backups and definitely not your only backup. The problem is that even if you have a fast Internet connection, it can easily take days to get all of your data back in the event of a crash. We've had law firms take 3 to 4 days to get their data restored and that is frankly unacceptable. If those firms had been using external hard drives or some other of local backup, it would have taken only a few hours to get their data back.

h. **Off-Site Storage**: If you're using tapes, take yesterday's backup home with you every night. If you're using an external hard drive, burn your important data to CD periodically and put it somewhere off-site. You can also use one of several Internet based backup options.

i. **No Incremental Backups**: A pure incremental backup means you're only backing up files that have changed since the last full or incremental backup. You can get quite a chain of these going and hopefully there's a full back up at the beginning of the chain. People typically use this method because it's faster and takes less space. However, incremental backups are NEVER, EVER acceptable for a law firm or legal department. First, trying to restore something when the data is scattered across many incremental backups is a nightmare and takes a very long time. Second, if one of those incremental backups gets screwed up, it may eliminate the possibility that you can restore anything that was backed up subsequently. Finally, incremental backups typically mean that you only have one copy of each file (it over-writes the old version of each file it backs up). So let's say you have an accounting program and the database gets corrupted. If you have an incremental backup then the only copy of the database you have backed up is the corrupted one. By contrast, if you had 5 full, rolling backups for the last 5 days, then you would have a copy of the database backed up before the corrupted occurred.

j. **Run Test Restores At Least Once A Month**: You need to do this to verify that you can restore and also to make sure you know how to do it.

k. **Have a Secondary Backup Method**: Have at least two backup methods. For example, if you've got a tape backup, then add an external hard drive or an on-line backup or burn CDs. You can never have too many copies of your stuff.

2. **AntiVirus Software**: You absolutely must have a good antivirus software program running on your server and all connected computers. The virus definitions must be updated at least weekly and preferably, the updating should be automatic.

3. **Firewall**: A firewall is a specially programmed computer system, hardware appliance or software application that "stands" between an organization's internal network and the Internet. It is a security measure which prevents hackers and other unauthorized users from accessing internal networks.

F. **Acquire Scanners**: I know this point seems obvious, but there are several issues built into it.

1. **One Big Fast Scanner In the Copy Room v. Multiple Smaller Scanners**: Every single law office we've ever worked with that had success in reducing paper relied primarily on small, convenient, desktop scanners rather than a copier. In 19 years, there have been no exceptions to this rule.

a. **High Speed Copier/Scanners**: There are two schools of thought regarding the best way to incorporate imaging into a law office. One method is to buy one really fast scanner, connect it to the network, put it in the copy-room and let everyone use it for scanning. Copier sales/leasing companies are pushing copiers that are also network scanners and printers. Although high speed copiers that also scan are pretty nice and can be extremely fast, there are drawbacks.

In our experience, offices with one, big, fast scanner (and no small desktop scanners) are much less likely to get everyone on board with paper reduction. The fact is, law offices are busy places and time-consuming processes are avoided, generally speaking. A copier/scanner requires that users get up out of their chairs, walk down the hall, stand at a copier, designate where they want the scanned documents to go on the network in advance, scan the documents in, then walk back to their offices and locate the images on the server. If someone is already copying or printing, then the whole annoying process gets delayed and maybe never done. Make someone jump through a lot of hoops to scan, and I

guarantee you that the annoyance factor will quickly nullify any previous enthusiasm the individual may have had for scanning.

b. **Small Desktop Scanners**: The alternative method is to put less expensive, slower scanners on the desks of everyone who will be scanning. If I can sit at my desk, drop a document in a scanner's document feeder on my credenza and direct exactly where the document is going to go with one click, I'll do it and so will most people. Therefore, we recommend desktop (or credenza) scanners within arm's reach for everyone who will be scanning. This is not to say that a big, fast scanner doesn't have a place in your office. Of course, you can also use desktop scanners in addition to a large copier/scanner.

2. **Comparison of Typical Copier to Desktop Scanners**: It is always less expensive to buy separate printers and scanners than to purchase or lease a copier. Here's an example.

   a. **Xerox WorkCentre 5638**:

      i. Print 32 ppm/Scan 38 ppm

      ii. Print/copy/scan

      iii. Typical lease from Xerox for 60 months (no copies included) - $537.90/month for 60 months or **$32,274**

   b. **Fujitsu ScanScap iX500**:

      i. Scans 25/50 ppm (no print or copy)

      ii. $425

      iii. You could buy 75 of these scanners for the price of one Xerox.

3. **Comparison of Leased Copier to Separate Components**: In other words, a Xerox copier can print, copy and scan. If you purchased separate machines to handle each of those functions, what would it cost? Keep in mind that if you scan and print, then you probably don't need a copier because anything scanned can be printed over and over.

   a. **Copier**: Lease payments total for 60 months.

      - **Xerox WorkCentre 5638 (38 ppm): $32,274**

b. **Separate Components**:

- Fujitsu 7180 – (scans 80/160 ppm)..... $1,514
- HP LaserJet M602x (prints 62 ppm/duplex/ network adapter) $1,405
- Stapler/Stacker/Collator for Printer (HP part CE405A) $249
- Toner (enough to print 120,000 pages)..... $1,345
- Unbundled total price:..... $**4,513**

4. **Comparison of Purchased Copier to Five Person Scanning System**: Below, compare what a copier would cost if purchased outright against 5 scanners and a printer.

a. **Copier**:

- **Xerox WorkCentre 5150 Copier** (50 ppm with a few options):..... **$12,000**

b. **Separate Components**:

- Fujitsu 7180 – (scans 80/160 ppm)..... $1,514
- Fujitsu ScanSnap iX500 - 4 of them (scan 25/50 ppm)..... $1,700
- HP LaserJet M602x (prints 62 ppm/ duplex/network adapter) $1,405
- Stapler/Stacker/Collator for Printer (HP part CE405A) $249
- Unbundled total price:..... $**4,868**

G. Recommended Scanners for a Law Office: If the scanner you're considering has the right driver to work with your PDF software or if the scanner comes with the software necessary to create PDFs, then you're probably fine. However, here are a few scanners we particularly like.

1. **Basic Scanners Types**:

a. **Flatbed Scanners**: A flatbed scanner consists of a flat surface on which you lay documents to be scanned. They're very similar to a copier in appearance and they're particularly effective for bound

documents. You can buy flatbed scanners with or without an automatic document feeder ("ADF"). However, buying one without an ADF is a complete waste of money as it will take an inordinately long time to scan any multi-page document. No one will like it and no one will use it. A flatbed scanner with an ADF will allow you to scan regular cut sheets of paper or bound materials. However, they're generally slower and more expensive than their sheet-fed counterparts (see below).

b. **Sheet-Fed Scanners**: Sheet-fed scanners lack the flat glass surface for scanning bound materials; and they only have an automatic document feeder. However, sheet-fed scanners are generally faster and less expensive than flatbed scanners. Of course, if the only type of scanner you have is a sheet-fed scanner and you need to scan bound materials, you could always copy the appropriate pages and then scan them.

2. **Recommended Flatbed Scanners**:

a. **Xerox DocuMate 3220**: Scans 23 ppm, has a 50 sheet ADF and will scan color, b&w, and gray scale. $308 from www.amazon.com - Mnfg. Part #XDM32205M-WU.

b. **Fujitsu fi-6230z Scanner**: Scans b&w one-sided (simplex) at 40 pages per minute or double-sided (duplex) at 80 pages per minute. Also capable of color scanning; and handles letter or legal sized paper. This scanner connects to your computer via USB 2.0. This scanner is small and quiet, handles color, black & white and grayscale. Best of all, it has a 100 sheet automatic document feeder (ADF). Comes with Kofax® VRS® Professional, Adobe® Acrobat® Standard, and ScandAll Pro. Part number PA03630-B555, $1,307 from www.costcentral.com.

c. **Fujitsu fi-6240z Scanner**: Scans b&w one-sided (simplex) at 60 pages per minute or double-sided (duplex) at 120 pages per minute. Also capable of color scanning; and handles letter or legal sized paper. This scanner connects to your computer via USB 2.0. This scanner is small and quiet, handles color, black & white and grayscale. Best of all, it has a 100 sheet automatic document feeder (ADF). Comes with Kofax® VRS® Professional, Adobe® Acrobat® Standard, and ScandAll Pro. Part number PA03630-B505, $1,908 from www.costcentral.com.

3. **Recommended Sheet-Fed Scanners**:

   a. **Fujitsu ScanSnap iX500 Sheet-Fed Scanner**: Sheet-fed, scans 25 ppm simplex, 50 ppm duplex, no TWAIN driver, but comes with Adobe Acrobat X Standard and works fine with it. The US mnfg. part number is PA03656-B005 and it costs $425 from www.pcnation.com. This scanner is both Windows and Mac compatible.

   b. **Epson ES-400 Sheet-Fed Scanner**: Scans 35 ppm/70 ppm, TWAIN compliant, $350 from amazon.com.

   c. **Fujitsu Fi-7160 Sheet-Fed Scanner**: Up to 60 ppm/120 ppm duplex black and white or grayscale. Rapid power up time in less than 4 seconds; large capacity 80 page feeder; plastic and embossed credit card scanning; long document support up to 18.3 feet; scan sticky notes, taped receipts, and labels while securing against multifeeds; innovative acoustic paper protection; Interactive, Multi-Line LCD Panel; Auto rotation, Auto size, Blank page removal, Auto color detection, and Assisted scanning features; TWAIN and ISIS drivers The US part number is (PA03670-B055, and it's $875 from www.amazon.com.

   d. **Fujitsu fi-7180 Sheet-Fed Scanner**: Up to 80 ppm/160 ppm duplex black and white or grayscale. Rapid power up time in less than 4 seconds; large capacity 80 page feeder; plastic and embossed credit card scanning; long document support up to 18.3 feet; scan sticky notes, taped receipts, and labels while securing against multifeeds; innovative acoustic paper protection; Interactive, Multi-Line LCD Panel; Auto rotation, Auto size, Blank page removal, Auto color detection, and Assisted scanning features; TWAIN and ISIS drivers The US part number is (PA03670-B005, and it's $1,514 from www.amazon.com.

H. Acquire Software That Creates Searchable PDFs:

1. **Types of PDFs**: There are two basic types of PDFs – Image Only and Searchable.

   a. **Image Only PDFs**: This type of PDF is visually an exact replica of the original document (whether the original document was electronic or paper-based), but it contains no text which could be searched by Acrobat or any other program. This is usually the type of PDF that you get when you scan a document using a copier, scanner or multifunction machine.

b. **Searchable PDFs**: This type of PDF is also an exact replica of the original document, but it also contains a hidden layer of text so that you can search for any word on any page. PDFs created from other computer programs electronically are searchable by default. In other words, if I create a PDF from a Word or WordPerfect document, an Excel workbook or an email, they are always searchable. PDFs created by scanners can be, but are usually not searchable. The software you're using to scan will determine whether you can create searchable PDFs. So that you can easily find the PDF documents you're looking for, you want to make sure that anything you scan is not just a PDF but a searchable PDF.

2. **Programs You Can Use**: Adobe Acrobat is indefensibly expensive compared to its competitors. Don't be afraid to try any of the following.

   a. **Adobe Acrobat Pro DC**: There are two flavors here: Acrobat DC Pro "with services" which you can only rent; and Acrobat DC Pro desktop which you can buy. You can rent DC Pro with Services for $179.88/year or $24.99/month; and you can buy DC Pro Desktop for $449. Only Pro is available for the Mac. See http://tinyurl.com/ogympca for pricing and product information.

   b. **Adobe Acrobat Standard DC**: There are two flavors here: Acrobat DC Standard "with services" which you can only rent; and Acrobat DC Standard desktop which you can buy. You can rent DC Standard with Services for $155.88/year or $22.99/month; and you can buy DC Standard Desktop for $299. Standard is not available for the Mac. See http://tinyurl.com/ogympca for pricing and product information.

   c. **Foxit PhantomPDF for Business**: Very strong feature match with Acrobat Pro for $129. Also includes a 30 day free trial. For more information, see http://tinyurl.com/7ybcjwu.

   d. **Nitro Pro**: Matches the features of Acrobat Professional. They offer a Nitro Pro+ which is rental only for $7.99/month ($95.88 paid annually - no option to pay monthly) and Nitro Pro (desktop) which is $159.99. You can buy it here: https://www.gonitro.com/pro/for-you.

   e. **Nuance Power PDF Advanced**: Matches features of Acrobat Professional for only $149.99. See http://tinyurl.com/zwy2ym9.

f. **Foxit PhantomPDF Standard**: Strong match with Acrobat Standard for $89. Free trial - for more information, see http://tinyurl.com/p3znuj3.

g. **pdfDocs Pro by DocsCorp**: Very strong feature match with Acrobat Professional and recently completely revamped. A 12 month subscription is the only way to buy it and it's $107 annually. See http://tinyurl.com/htz5s7d for more information.

I. Acquire Search Program Or Document Management System: Even if you've created a good file naming convention, you'll still need help finding some documents. Now that you've created searchable PDFs, you can search through all of them at once, quickly, by searching for particular words. Here is a survey of your options:

1. **Windows Search Options**: Even if you've created a good file naming convention, you'll still need help finding some documents. Now that you've created searchable PDFs, you can search through all of them at once, quickly, by searching for particular words. Here is a survey of your options:

a. **Copernic Desktop Search**: RECOMMENDED - See www.copernic.com. There are three versions of Copernic, Home (FREE), Professional ($49.95) and Corporate ($59.95). Unless you're installing it in a very large firm, you only need the Professional version. You can try the free home version, but one of the limitations of the free version is that it does not search network drives. So unless you're keeping all of your files on the C:\ of the computer you're using (I certainly hope you're not doing this), the Home version will not help you very much. Copernic will search all of your files (Word, Excel, PowerPoint, PDF, HTML, WordPerfect, text and another 150 types of files). It will also search Outlook or Outlook Express email and any attachments to email.

b. **dtSearch**: RECOMMENDED: See www.dtSearch.com - $199 - one of the most sophisticated and fast search engines I've ever seen. It provides the most search options and file types that it can recognize. If you need industrial strength search capability involving enormous numbers of documents, this is your program.

c. **Filehand**: See www.filehand.com - FREE. Instantly search for files on your computer, by content. See the extracts of the files you found, even for PDF files. Scroll through the extracts so you can quickly find the information you're looking for. Find the file you

are looking for, even when many files match, because Filehand Search sorts the results by relevance. Do complex Boolean searches and searches by phrase. Use it all the time because it is so simple to use!

d. **Windows Instant Search** (Windows Vista, 7 & 8): This is free and is included with Windows.

2. **Apple/Mac Search Program Options**:

   a. **HoudahSpot**: $29 - see www.houdah.com/houdahSpot

   b. **Path Finder**: $40 - see http://www.cocoatech.com/pathfinder/

   c. **Spotlight Search (Mac OSX)**: This is included with the Mac OSX operating system. For more information, see http://support.apple.com/kb/HT2531

   d. **EasyFind**: Free - see http://tinyurl.com/d6se856

3. **What Search Programs Do**: Briefly, they read through all of the documents you've created in a word processor or scanned, and they build an index of the text contained therein. Once the index is built, you can search through all of those documents by either file-name OR the words contained inside them. When searching for words contained inside the documents, you can use the standard Boolean logic (and, or, not, etc.).

4. **Document Management System ("DMS") Options**: A DMS is a hardware/software system that automates the process of storing, classifying, searching, sharing, and retrieving electronic documents. A DMS also provides an organization with the tools to create, manage, control, and distribute electronic documents. The main players are:

   a. **Worldox GX**: WORLDOX's unique SQL-free software is installed in more than 2300 companies worldwide, 2000+ of which are law firms and legal departments. It is a “SQL-free” document management system. For the law firm, the total cost of ownership, especially over the long haul, is considerably less. For more information, go to www.worldox.com.

   b. **iManage WorkSite**: Autonomy WorkSite™ is a SQL based integrated application suite that combines document management, collaboration, portal access, knowledge management, workflow and business process automation in a single solution on a highly scalable and secure Internet platform.

From an end-user's perspective (ease of use), this is, by far, the best program available on the market today. Its integration with Microsoft Outlook is fantastic. See http://www.interwoven.com. Interwoven does not disclose pricing information on their web site.

c. **NetDocuments**: NetDocuments provides a document management via the web, so you store your documents on their server and basically pay a monthly fee for the utility of the software. Since you pay by the user, this solution can work for a single lawyer up to thousands of users. For more information, go to www.netdocuments.com.

J. Consolidate Folder Structure: If you don't have a document management system, it is critical that *documents are saved by client/matter, not by user*. Saving documents by user can create lots of problems, such as:

- Docs for one client in more than one folder
- Revision conflicts
- Losing things permanently if staff turns over

Saving documents on users' C:\ drives is a big no-no. Saving documents by client or matter in one central location is a better option. You can create a logical directory layout, find documents easier, it makes backing up your documents simpler, and you can use Windows security to limit access for users. Two main options for file structure:

1. **Saving By Practice Area**: If S:\ is your server drive, you'd create a folder called S:\Documents, and sub-folders for each practice area thereunder:

   - S:\Documents\Corporations
   - S:\Documents\Estate Planning
   - S:\Documents\Miscellaneous
   - S:\Documents\Probate
   - S:\Documents\Real Estate

   Under each practice-area folder, you'll create additional sub-folders for each client name such as:

   - S:\Documents\Real Estate\Smith, John

- S:\Documents\Real Estate\Rosedale, Meredith

If you conduct multiple transactions for a single client in the same area (i.e., you represent an individual in the sale of one house and the purchase of another), you might want to create separate sub-folders for each deal such as:

- S:\Documents\Real Estate\Smith, John\Sale of 123 Maple St
- S:\Documents\Real Estate\Smith, John\Purchase of 400 E Main St

The documents created for each transaction would then be located under the appropriate sub-folder. For example, the path and file-name for the deed might be:

- S:\Documents\Real Estate\Smith, John\Sale of 123 Maple St\2004-09-21 - General Warranty Deed.doc

2. **Saving By Client**: If S:\ is your server drive, you'd create a folder called S:\Documents, and sub-folders for each client thereunder:

   - S:\Documents\Smith, John
   - S:\Documents\Rosedale, Meredith

   If you conduct multiple transactions for a single client in the same area (i.e., you represent an individual in the sale of one house and the purchase of another), you might want to create separate sub-folders for each deal such as:

   - S:\Documents\Smith, John\Real Estate - Sale of 123 Maple St
   - S:\Documents\Smith, John\Real Estate - Purchase of 400 E Main St

   The documents created for each transaction would then be located under the appropriate sub-folder. For example, the path and file-name for the deed might be:

   - S:\Documents\Smith, John\Real Estate - Sale of 123 Maple St\2004-09-21 - General Warranty Deed.doc

3. **File Structures To Avoid**:

   - S:\Jim\Smith, John\Sale of 123 Maple St
   - S:\HRK\Smith, J\Real Est - Sale of House

- S:\Sally\Smith\Real Estate - Sale on 3-4-2002

The foregoing folders are all for the same matter which is being worked on by 3 different people in the same firm. They each have created their own folders for it with different naming conventions and all of them are under the employee's name or initials. This is a very common scenario and the reason that law firms waste so much time trying to find things.

K. **Establish File Naming Conventions**: If you don't have a DMS, then you need to establish the rules by which files will be saved and named.

1. **The Old Way**: File naming has become more intuitive since Windows 3.1 (we used to be limited to 8 characters). Document extensions used to identify the type of document (.ltr, .fax, .dep, .pld, .cor, etc.)

2. **The New Way**: You now have 255 characters to name a file or folder in Windows. Therefore:

   - Then: wjcpc01.dep

   - Now: 2004-10-30 - James Smith Perjury Case Deposition 01.doc

3. **Acceptable Characters**: A file name may contain any of the following characters: ^ & ' @ { } [ ] , $ = ! - # ( ) % . + ~ _

4. **Unacceptable Characters**: A file name may not contain any of the following characters: \ / : * ? " < > |

5. **Recommended Protocol**: If you would like everything sorted by date (which is what most lawyers like), simply precede every file name with a date, year first. If you enter the date month/day/year, then all of the January files (for all years) are lumped together, all of the February files are together, etc. Our file naming convention:

   2004-10-30 - Letter to Bill Biviano re billing system.doc

   The date indicates the date the document was mailed out if it's a letter; and the longer description makes it clear what this document contains without even opening it. If you are scanning a document you received, then the date should be the date the particular document was received.

L. **Digitize Incoming Documents**: Some law offices scan all incoming mail which is then forwarded via inter-office email to the recipient (except for obvious things like magazines, etc.). The recipient can then view the mail, save it into the appropriate electronic file, or discard it. The person who scans the mail into the computer system retains the originals for one week and if they're not requested

by the recipient, they are shredded. In the alternative, let everyone scan in their own mail and that way time won't be wasted scanning things that would have been thrown away anyway. If everyone has a desktop scanner, this is easy.

M. Store Email Outside Of Your Email Application:

1. **Problems Caused By Storing Email Only in Webmail or Email Application**: A significant problem most law firms struggle with (if they do not own a document management system) is saving and finding matter-specific email. Why? Because people (1) keep them in their individual inboxes (which no one else can see), or (2) save them in subfolders within their own inbox (which no one else has access to), or (3) delete the email altogether. Email is valuable correspondence that in most circumstances should be saved. However, in a law firm or legal department, it should not be saved exclusively within one's own individual inbox.

2. **Stop Printing Email**: Because people understand that email sitting in their inbox is difficult for anyone else to find, they start printing it. However, stuffing your paper files with printed email accomplishes little, if anything, useful. It makes your files fatter and makes it even more difficult to locate the particular documents you're looking for once you find the file. Instead, you need to capture email electronically by creating files from them.

3. **Create Files from Your Email**: Because an email is just a record in a database (not a file like an MS Word file) and can't easily be shared or found by anyone else in your office, it is necessary to create files from those emails. The files created should be stored with all other documents related to a matter. They can be segregated out into an email folder under each matter or many people prefer to lump them in with all correspondence. Here are some of your options:

    a. **Webmail**: If you access your email exclusively via a website (like Gmail), then your options are limited to creating a PDF from your email one at a time. Of course, you'll need a program which allows you to create PDFs in the first place such as Acrobat (not free) or Primo PDF[22] (free).

    As a side note, we strongly recommend that you get an email application to store and organize your email rather than relying on a website like Gmail or Yahoo. In our opinion, webmail is not a

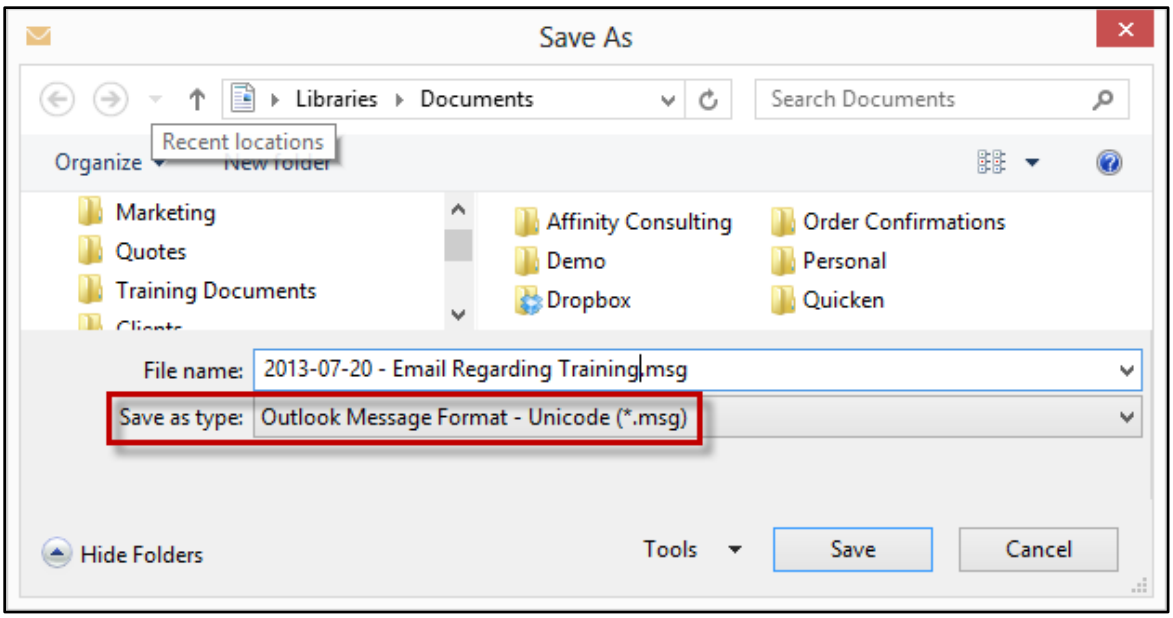
[22] See http://www.primopdf.com/

good idea for lawyers because it is often hacked[23], it's not accessible when you're offline, it doesn't integrate with other programs, it can't be saved as a file (only printed to PDF) and it is difficult to organize by matter. If you don't want to use Microsoft Outlook, then consider a free email application like Mozilla Thunderbird[24] which will run on a Windows or Mac PC. Email programs like Outlook or Thunderbird can easily be set up to routinely download the email from your webmail account and you typically have the option of leaving the downloaded email on the web or deleting it as soon as it is downloaded. It is not difficult to set up an email program like Outlook to work with your existing webmail account. Most email providers have the instructions right on their website. For example, if you use Gmail, then just see this: http://tinyurl.com/d96lc6k. If you have an option between POP and IMAP as email connection methods, choose IMAP. Gmail allows you to pull its email into an email program for free. Some webmail providers charge you for this privilege such as Yahoo. With Yahoo, you have to upgrade your free account to a paid one ($19.99/year for Mail Plus) and then you can pull it into an email program.

b. **Save Outlook Email As MSG Files**: You can save email much like you save a Microsoft Word document clicking the File menu ➔ Save As (Outlook 2003, 2010 & 2013) OR Office Button ➔ Save As (Outlook 2007). We recommend that you save as **Outlook Message Format - Unicode (*.msg)**. If you're using Outlook 2003, it will default to HTML but you can switch to MSG. If you're using Outlook 2007 or 2010, it will default to MSG.

   A huge benefit to saving MSG files is that it also captures the attachments to the email you're saving *inside* the MSG file. So if you forgot to separately save the attachments, it won't matter because when you open an MSG file, they're right there. Furthermore, MSG files are still email files (even though they're no longer stored in Outlook) so you can open one you saved previously and forward it, reply to it or anything else you could do with an email you open in Outlook.

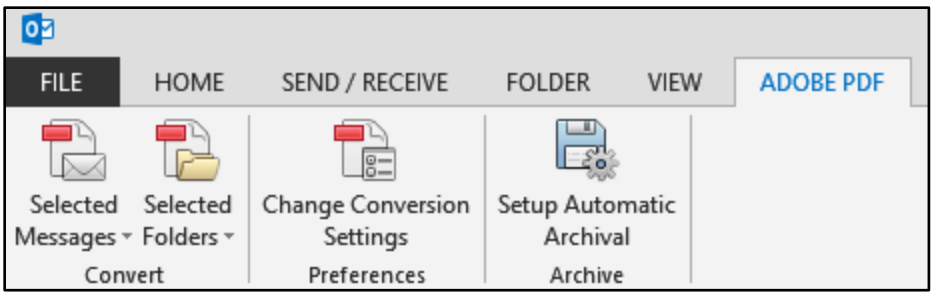
[23] Just conduct an Internet search on the terms "gmail hacked" and you'll see what I mean.
[24] See http://www.mozilla.org/en-US/thunderbird/ for more information.



You may notice that you have a choice of Outlook Message Format and Outlook Message Format - Unicode. The Unicode format is the current standard for Outlook and holds support for international characters. The non-Unicode one saves msg-files in the ANSI format. The ANSI format is the only format that Outlook 2002 and previous can read. Outlook 2003 and later can read ANSI formatted and Unicode formatted msg-files. Dragging and dropping messages out of Outlook into an Explorer folder will by default save it in the Unicode format.

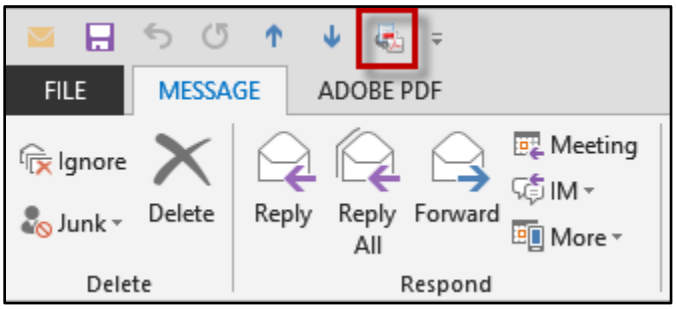
You can also save email as **Text Only** although you'll lose any formatting that was in the email. Saving as an MSG file will retain the original formatting, look and feel of the email.

c. **Save Outlook Email As PDF Files**: This is made infinitely easier if you use Acrobat Standard or Pro and take advantage of the integration between Outlook and Acrobat. By using the ribbon shown below, you can make PDFs of single email, multiple emails at once or even entire folders at once. You can also set up Automatic Archival so any email that ends up in a particular folder is automatically archived into a PDF without you doing anything.

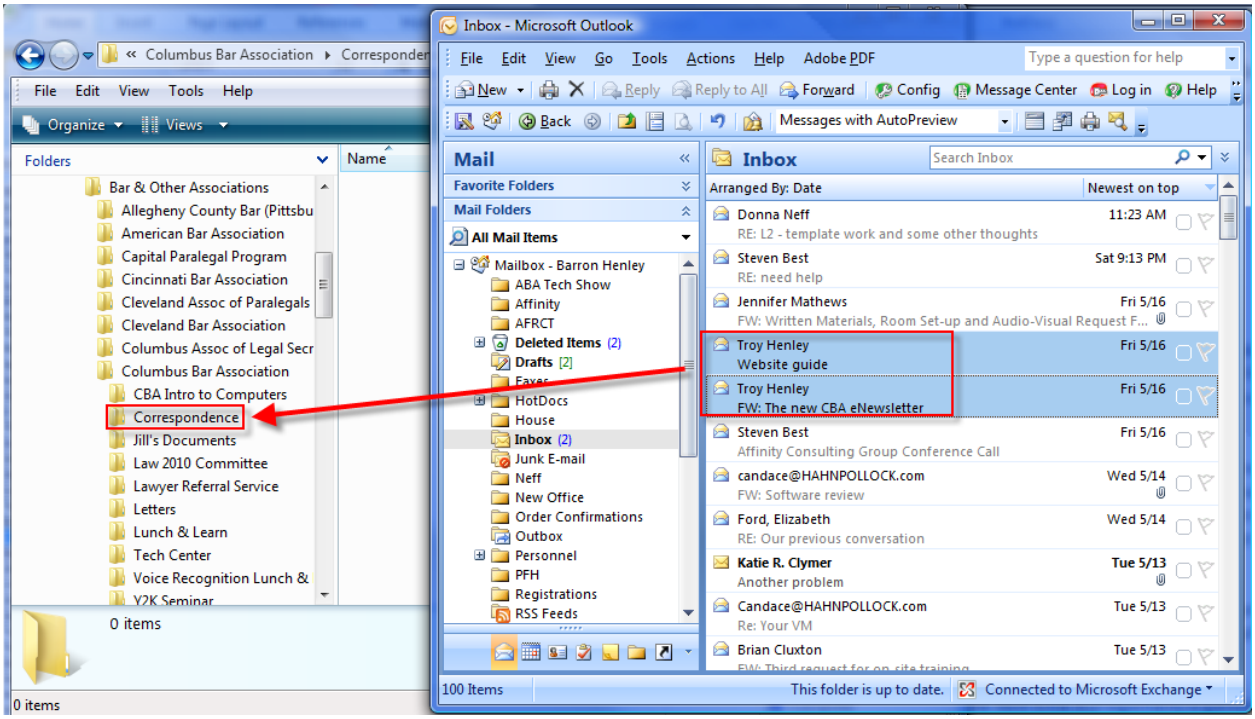


Using the Acrobat integration also captures attachments inside the PDFs you create from email automatically (same as MSG files). Another benefit of creating PDF files from your email is that PDFs are viewable on just about any device. MSG files, on the other hand, can only be viewed in Outlook, Thunderbird and a few other programs. So from a future-file-access perspective, PDF is much safer than MSG.

In addition to the foregoing, Acrobat also allows you to add a button to the Outlook Quick Access Toolbar called Convert to Adobe PDF so that you can open any email and click a single button within the email to convert it to PDF. This method also saves the attachments inside the PDF just like using the ribbon mentioned above. Below is a screenshot of my Quick Access Toolbar in Outlook 2013 with my PDF button highlighted.



d. **Save Outlook Email By Dragging Into a Folder**: You can clean out your inbox or subfolders under your inbox by cascading the windows and simply dragging and dropping all of them into the desired folder. This will COPY the emails over into that folder, saving them automatically as MSG files, which preserves the metadata and all attachments.



N. **Write Down Your Scanning Protocols**: Have meetings, experiment, and develop protocols which include what to scan and who will scan it. If you're using a DMS, determine how scanned documents will be saved and profiled into the system. If you're not using a DMS, determine folder organization and file naming conventions. Once you get your system all ironed out, conduct training (see next step).

O. **Provide Training For All Staff**: This is the most important aspect of the entire project. Ideally, you'll have someone conduct the training for you at your office using your new equipment and software. Even people who don't think they'll be scanning or who have said they don't want to should be included in the training. The reality is that once resistant individuals see how easy and constructive it is to scan, many of them will change their minds. Seeing it work first hand is pretty inspiring.

P. **Additional Recommendations**:

1. **Make Your Electronic File Mirror Your Paper File and Run Them Parallel To One Another**: The documents you've created in-house are probably already in your electronic file. We propose that you simply add everything else in your paper file to it as well. In other words, if you receive a fax, scan it into your electronic file and put the hard copy of the fax in your paper file (like you've always done). If you receive a document in the mail from opposing counsel, scan it into the electronic file and deposit the original in the paper file. If you aren't happy only

retaining the original Word or WordPerfect files, then after the letters are printed and signed, scan copies of them before you put them in the envelope. You can continue at this stage for as long as you'd like. This way, the paper addicts in your office will be appeased, but you'll still reap a lot of the benefits of an electronic file. When you're ready, move to the next step.

2. **When Possible, Destroy The Items You Scan**: We're not talking about the elimination of the paper file. Instead, we're suggesting that you could store a lot of your paper in digital form only and there is no penalty. For example, if someone sends you a fax, do you need to retain the original fax? Since a paper fax is not evidence of anything other than the death of a tree and could be modified imperceptibly with a cheap scanner and software, it's unlikely that you need to keep it in paper form. Therefore, faxes are great candidates for scanning and shredding. If you ever need to print the fax, of course you can do so from the scanned image. By starting this policy, you'll see that your paper files start becoming a lot thinner, easier to search and easier to manage. If you are paranoid about losing your paper file, then you can certainly keep stuffing it with everything that comes in or goes out; but I'd respectfully submit that you're missing out on an enormous benefit of going digital.

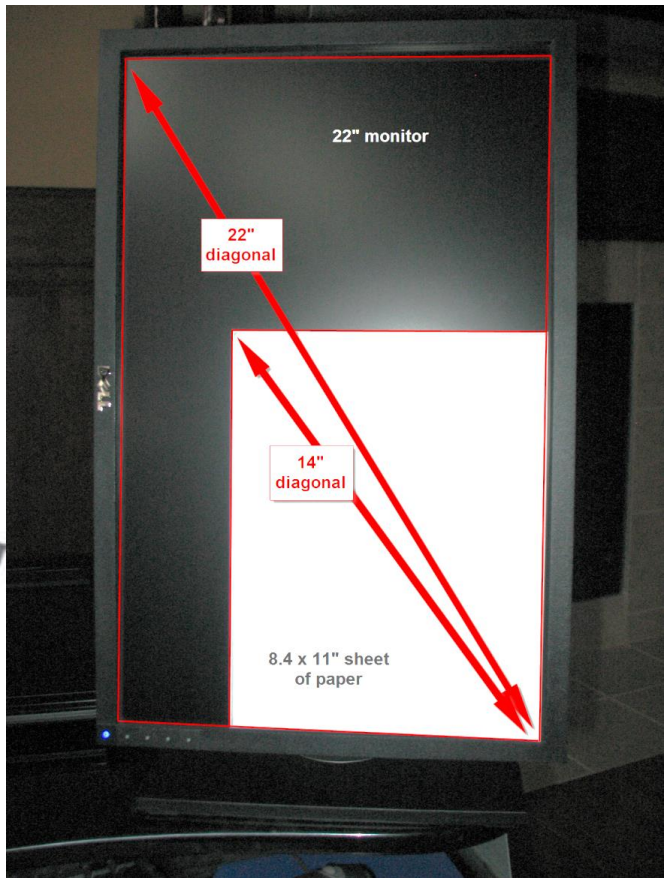
3. **Pick A Date By Which You Will Stop Saving Every Piece of Paper**: Most law offices initially keep all of the paper just like they always did. However, if you're scanning AND filing all of the paper into paper files, then you're actually creating extra work for yourself. If you follow the roadmap I've laid out, you'll realize at some point that keeping all of the paper isn't serving any useful purpose. However, in my experience, that doesn't mean you'll stop keeping all of the paper. People tend to keep doing what they've always done even when intellectually, it no longer makes sense. So that you don't fall into this trap, pick a date in the future - say six (6) months after you start scanning in earnest - and decide that if everything is going well, you're going to stop keeping every single piece of paper after it is scanned.

4. **Stop Injecting Paper Into Your Workflow**: This is something you need to start thinking about all the time. People habitually print things and make copies so it can be difficult to break the habit.

5. **Stop Making Copies of Everything You Send Out and Putting Them In The Paper File**: There are unquestionably a lot of paper documents in your files that you don't actually need in paper form if electronic copies of them are on your server. Out of paranoia, lawyers like to "paper the file" and create "paper trails" of everything they do so their work is "well

documented." Those terms, as they relate to paper, were used in the practice of law 100 years ago and frankly, they're losing their relevance today. The objectives those terms represent can all be accomplished electronically and much more efficiently. Furthermore, a paper copy of something is no longer evidence of anything since anyone can alter a paper copy with a $50 scanner and make the alteration undetectable. Since most firms only keep paper copies of documents they send out so they can easily determine WHEN they were sent out, simply include the date in the name of the file (i.e., 2003-01-04 - Doe, John letter.doc).

6. **Buy Monitors That Rotate to Portrait**: Many lawyers print documents in order to review them because they find it difficult to review documents on a computer screen. This difficult typically arises out of the fact that when viewing a document on a typical monitor, one can only see a few paragraphs of each page because the monitor is landscape (wide) and the document is portrait (tall). To remedy this problem, we recommend buying monitors that rotate to portrait (see screen shot below). Monitors with this capability usually only cost a few dollars more than those without it and it is completely worth the extra money. As you can see below, a standard 22" monitor rotated to portrait not only allows a user to see an entire page of text at once, but it makes it nearly twice as big as it would appear if you printed it on 8.5 x 11" paper.



7. **Buy Dual Monitors**: This concept simply allows you to spread out and not spend so much time minimizing and maximizing applications you're working with in order to switch between them. The reason you'd want to go with two monitors rather than one larger one is that it is far less expensive to do so. For example, two 23" monitors can easily cost $400 for both ($200 each); however, a 30" monitor can easily cost $1,200 for one of them. New desktop computers can be configured to include two monitor ports for this purpose. Many laptops also come with two monitor ports on the docking stations (Dell Latitude laptops, for example). If you have an existing desktop computer, you can buy upgraded video adapters which provide dual video output ports. Finally, you can buy USB to VGA adapters which are designed to allow you to add additional monitors via the USB port on your computer.

8. **Don't Shred - Recycle Instead**: Shredders are expensive, noisy, make a mess and jam. You're much better off finding a recycling company to pick up your paper and destroy it confidentially for you. Companies providing this service are easy to find. For example, if I google "paper shredding Columbus Ohio," I get a long list of companies that offer this service locally. Obviously, you want to choose a company that guarantees that

the paper will be confidentially destroyed. We use a company called Iron Mountain which has offices all over the U.S.

9. **Scan Non Client Related Items First**: For example, you probably have a lot accounting records stuffing filing cabinets (bills paid, bank statements, etc.) that would be excellent candidates for scanning. Try those first as they are great candidates.

10. **Consider a Press Release or Marketing Materials About What You've Done**: By reducing paper, you're reducing your firm's carbon footprint, reducing landfill waste, helping the environment *and* saving money. This is something to crow about. Many firms incorporate these facts into marketing materials, their web site, etc.

VII. CLOUD STRATEGY:

A. Why The Cloud Is Important For Disaster Avoidance: Any hardware or software you have on-site is at risk to crashes, power and Internet interruptions, natural disasters, sabotage and theft. Whether you rent a software application (like a case management program) or you rent server access (aka hosted servers), the computers you're accessing are in data centers with Fort Knox security, redundant/backup power, redundant Internet access and fault tolerance few law firms in the world could afford to build in-house. In fact, a Tier IV (highest) rated data center provides guaranteed 99.995% uptime.

If your servers and/or software are accessible via the Internet and some disaster befalls your office, you just have to get somewhere with power and an Internet connection to regain access to everything. Due to the fault tolerance of data centers, you're not likely to lose access otherwise due to power, Internet, sabotage or theft.

Here's another opinion on this subject from a Chicago-based lawyer:

> "Here is my outlook. It's simple. I am not a data expert. I am not a tech expert. I am not a security expert. Given this information, I refuse to keep client data on premises, in our systems, etc.. I practice law. But that in no way makes me suitable to make decisions about my clients' data. Perhaps the easiest thing law firms can do is to put data in the hands of experts (and understanding that those experts are not attorneys). Offsite servers that are encrypted, protected and have teams of people

ensuring their security are any law firm's best friend. In my opinion, they are underutilized in the industry."[25]

B. Definitions Related to Cloud Computing:

1. **SaaS or Software As A Service**: Rather than purchasing and installing software on a computer or server, SaaS is simply accessed via a web browser. Your data is stored in the vendor's servers in a data center (see paragraph 6 below) rather than in your office. There are a ridiculous number of definitions of SaaS, but I think this one sums it up succinctly without using 15 more acronyms requiring definitions:

> "Generally speaking, it's software that's developed and hosted by the SaaS vendor and which the end user customer accesses over the Internet. Unlike traditional packaged applications that users install on their computers or servers, the SaaS vendor owns the software and runs it on computers in its data center. The customer does not own the software but effectively rents it, usually for a monthly fee. SaaS is sometimes also known as hosted software or by its more marketing-friendly cousin, 'on-demand.'"[26]

To be clear, this means that you do *not* have the software installed on your computer - it is accessible only via a browser on the Internet. Further, your data and/or documents are located on the vendor's servers and not on your computer or server.

2. **PaaS or Platform As a Service**: PaaS is a derivation of SaaS that allows users to *rent* hardware, operating systems, storage, and network capacity over the Internet access. Salesforce.com is a great example of this with their Customer Relationship Management (CRM) product. Salesforce's platform allows outside developers to create add-on applications that integrate into the main application and are "hosted" on the company's infrastructure. For example, Advologix[27] is a legal case management system that was built on the Salesforce.com platform.

3. **IaaS or Infrastructure as a Service**: In most cases, this means renting access to a server located in a data center (see paragraph 6 below). The server provides processing power and electronic storage, both of which

[25] Law Firm Data Security: Experts on How to Protect Legal Clients' Confidential Data, by Nate Lord, DigitalGuardian, October 13, 2015, quoting Jared Staver. See http://tinyurl.com/h6nzvjb.
[26] Software as a Service (SaaS) Definition and Solutions, by Meridith Levinson on May 15, 2007, www.cio.com, see http://tinyurl.com/24cofbx for full article.
[27] See www.advologix.com

are accessed via the Internet. The server is available on-demand and the provider is usually responsible for maintaining the server, providing backup and technical support.

4. **Hybrid Approaches**: Of course, there are slight variations on these ideas. With pure SaaS, you don't own anything except your data. However, services like Hosted Exchange[28] are a little different. In that case, you can own the application necessary to view the data (Outlook), it's installed on your computer, you own the data, and you can access/view the data offline regardless of whether you continue to subscribe to the service. You are necessarily also renting a server with Hosted Exchange so it has aspects of SaaS and IaaS.

5. **Colocation**: You can also buy your *own* server and install it in a data center (see paragraph 6 below).

6. **Data Center**: Here's a good definition from www.cio.com:

> "Known as the server farm or the computer room, the data center is where the majority of an enterprise servers and storage are located, operated and managed. There are four primary components to a data center:
>
> > White space: This typically refers to the usable raised floor environment measured in square feet (anywhere from a few hundred to a hundred thousand square feet). For data centers that don't use a raised floor environment, the term "white space" may still be used to show usable square footage.
> >
> > Support infrastructure: This refers to the additional space and equipment required to support data center operations — including power transformers, your uninterruptible power source (UPS), generators, computer room air conditioners (CRACs), remote transmission units (RTUs), chillers, air distribution systems, etc. In a high-density, Tier 3 class data center (i.e. a concurrently maintainable facility), this support infrastructure can consume 4-6 times more space than the white space and must be accounted for in data center planning.

[28] Microsoft Exchange is Microsoft's server application for backing up and sharing email, contacts, calendars, tasks and other information in Microsoft Outlook. It provides centralized data storage, sharing abilities, plus synchronization with various phones and other devices. Hosted Exchange is essentially renting this service by paying a monthly fee per user.

> IT equipment: This includes the racks, cabling, servers, storage, management systems and network gear required to deliver computing services to the organization.
>
> Operations: The operations staff assures that the systems (both IT and infrastructure) are properly operated, maintained, upgraded and repaired when necessary. In most companies, there is a division of responsibility between the Technical Operations group in IT and the staff responsible for the facilities support systems."[29]

In plain English, a data center is a secure physical facility which houses the computers of one or more enterprises. Depending upon what "Tier" a data center is rated for, it may have redundant components, backup generators and multiple uplinks (internet connections). There are 4 Tiers and Tier 4 guarantees 99.995% uptime.

C. Is Going to the Cloud All or Nothing? Absolutely not. For example, I could be using hosted Exchange (with Outlook) while running Word, Excel & PowerPoint locally. If you rent a cloud server, programs like Citrix XenApp[30] provide a delivery mechanism so that regular shrink-wrapped software you own can be delivered to you through the Internet. So I could run my accounting software from a cloud server via Citrix XenApp, while every other program I use is running locally.

D. Ethical Issues Presented By Moving To The Cloud:

1. **Applicable Rules of Professional Conduct**: These are discussed in paragraph IV. on page 4 above.

2. **Other Authorities**:

   a. **Ohio State Bar Association Informal Advisory Opinion 2013-03**:

      i. **Summary:** "You have requested the opinion of the Ohio State Bar Association Professionalism Committee on whether your law firm may use a third-party vendor to store client data in 'the cloud.' As you describe it, your firm currently backs up its computer files, including client documents and data, on a server located on site. You are considering a third-party vendor that is offering a program that would use 'a major software provider to securely store your data off site,' which your law firm would be able

[29] See http://www.cio.com/article/499671/Data_Center_Definition_and_Solutions
[30] See http://tinyurl.com/dv3jx for more information about XenApp.

to access via the Internet. You indicate that the data would be encrypted before it left the law firm and would remain encrypted at the offsite data center, located in Atlanta.

The Committee's opinion is that storing client data in 'the cloud' is a permutation on traditional ways of storing client data, and requires lawyers to follow the ethics rules that apply to client information in whatever form. With due regard for these rules and related Ohio ethics opinions, the Committee advises that the Ohio Rules of Professional Conduct do not prohibit storing client data in 'the cloud.'"[31]

ii. **Key Points**: "…[T]here are four main issues to consider in applying the Ohio Rules of Professional Conduct to cloud storage of client data: competently selecting an appropriate vendor; preserving confidentiality and safeguarding the client's data; supervising cloud storage vendors; and communicating with the client."

iii. **Competently Selecting an Appropriate Vendor**: The opinion outlines several considerations including:

- What safeguards does the vendor have to prevent confidentiality breaches?
- Does the agreement create a legally enforceable obligation on the vendor's part to safeguard the confidentiality of the data?
- Do the terms of the agreement purport to give "ownership" of the data to the vendor, or is the data merely subject to the vendor's license?
- How may the vendor respond to government or judicial attempts to obtain disclosure of your client data?
- What is the vendor's policy regarding returning your client data at the termination of its relationship with your firm?

[31] OSBA Informal Advisory Opinion 2013-03, July 25, 2013.

- What plans and procedures does the vendor have in case of natural disaster, electric power interruption or other catastrophic events?

- Where is the server located (particularly if the vendor itself does not actually host the data, and uses a data center located elsewhere)? Is the relationship subject to international law?

iv. **Supervising Cloud Vendors**: "… [U]nder Rule 5.3(a)-(b), lawyers who contract with a cloud-storage vendor must make reasonable efforts to ensure that the vendor's conduct is compatible with the lawyer's own professional obligations. While the extent of supervision needed is a matter of professional judgment for the lawyer, the lawyer must exercise due diligence in ascertaining whether the vendor will be capable of conduct consistent with the lawyer's own obligations."

v. **Communicating With the Client**: "We do not conclude that storing client data in 'the cloud' always requires prior client consultation, because we interpret the language 'reasonably consult' as indicating that the lawyer must use judgment in order to determine if the circumstances call for consultation.

…

In exercising judgment about whether to consult with the client about storing client data in 'the cloud,' the lawyer should consider, among other things, the sensitivity of the client's data."

b. **American Bar Association's Standing Committee on Legal Ethics and Professional Responsibility Forma Opinion 95-398**:

"…[I]n this era of rapidly developing technology, lawyers frequently use outside agencies for numerous functions such as accounting, data processing, photocopying, computer servicing, storage and paper disposal and that lawyers retaining such outside service providers are required to make reasonable efforts to prevent unauthorized disclosures of client information."

"A lawyer who gives a computer maintenance company access to information in client files must make reasonable efforts to ensure

that the company has in place, or will establish, reasonable procedures to protect the confidentiality of client information. Should a significant breach of confidentiality occur, the lawyer may be obligated to disclose it to the client."

c. **American Bar Association's Standing Committee on Legal Ethics and Professional Responsibility Forma Opinion 08-451**: "A lawyer may outsource legal or nonlegal support services provided the lawyer remains ultimately responsible for rendering competent legal services to the client under Model Rule 1.1. In complying with her Rule 1.1 obligations, a lawyer who engages lawyers or nonlawyers to provide outsourced legal or nonlegal services is required to comply with Rules 5.1 and 5.3. She should make reasonable efforts to ensure that the conduct of the lawyers or nonlawyers to whom tasks are outsourced is compatible with her own professional obligations as a lawyer with "direct supervisory authority" over them. In addition, appropriate disclosures should be made to the client regarding the use of lawyers or nonlawyers outside of the lawyer's firm, and client consent should be obtained if those lawyers or nonlawyers will be receiving information protected by Rule 1.6."[32]

d. **State Opinions on Cloud Computing**: All of the following permit cloud services and impose a reasonable care standard. However, the specific duties imposed on lawyers varies from opinion to opinion.

   i. Alabama Ethics Opinion 2010-02

   ii. Arizona Opinion 09-04

   iii. California Opinion 2010-179

   iv. Iowa Opinion 11-01

   v. Maine Opinions 194 and 207

   vi. Massachusetts Opinion 12-03

   vii. New Jersey Opinion 701

   viii. New York Opinion 842

   ix. Nevada Opinion 33

[32] See http://tinyurl.com/celuw4g for the full text of the opinion.

x. North Carolina 2011 Formal Ethics Opinion 6

xi. Oregon Opinion 2011-188

xii. Pennsylvania Opinion 2011-200

xiii. Vermont Opinion 2010-6

3. **Sample State Opinions**:

a. **Nevada Formal Opinion 33**:

"The previous ABA opinions and the new comments to Rule 1.6 clearly evidence the ABA's policy to treat electronic client communications and information according to existing rules and not to hold an attorney responsible for a breach of client confidentiality, or for storing client information in such a manner that the breach is possible, so long as the attorney:

1. Exercises reasonable care in the selection of the third party contractor, such that the contractor can be reasonably relied upon to keep the information confidential; and

2. Has a reasonable expectation that the information will be kept confidential; and

3. Instructs and requires the third party contractor to keep the information confidential and inaccessible."[33]

b. **Arizona Opinion 05-04**: Arizona Rules of Professional conduct "require that an attorney act competently to safeguard client information and confidences. It is not unethical to store such electronic information on computer systems whether or not those same systems are used to connect to the internet. However, to comply with these ethical rules as they relate to the client's electronic files or communications, an attorney or law firm is obligated to take competent and reasonable steps to assure that the client's confidences are not disclosed to third parties through theft or inadvertence. In addition, an attorney or law firm is obligated to take reasonable and competent steps to assure that the client's electronic information is not lost or destroyed. In order to do that, an attorney must either have the competence to evaluate the nature of the potential threat to the client's

[33] State Bar Of Nevada Standing Committee On Ethics And Professional Responsibility Formal Opinion No. 33, February 9, 2006. See http://tinyurl.com/9tt3ljn.

electronic files and to evaluate and deploy appropriate computer hardware and software to accomplish that end, or if the attorney lacks or cannot reasonably obtain that competence, to retain an expert consultant who does have such competence."[34]

4. **Meeting the Reasonable Care Standard**: In exercising reasonable care, the following are some questions and considerations you need to address before deciding to use any particular service.

   a. Where is your data stored? If it is to be moved, do you have the right to approve the transfer if it is going to be moved to another state or country?

   b. What is the provider's disaster-recovery or avoidance plan?

   c. How often are backups of the data made, where are they stored, and are multiple past versions maintained or only the most recent versions of your data?

   d. Who (if anyone) from the provider has access to your data? What level of access does each person have? You need to make sure that the provider understands that the data is to be kept confidential and I would recommend a written instruction to that effect.

   e. Is the data encrypted (not readable) when it is being transferred to the vendor and when you're accessing it from the vendor?

   f. Be sure that the vendor is not claiming any ownership rights in your data.

   g. What Tier is the datacenter where you data is being stored certified for? You want your data hosted in a Tier 4 certified data center. An explanation of the data center tier system can be found here: http://tinyurl.com/8rvrzou.

   h. Is the cloud vendor contractually obligated to notify you in the event of a security breach?

   i. Can you download your data at any time? If you decide to stop using the service, are they obligated to provide your data to you? If so, in what format and within how many days?

[34] State Bar of Arizona Ethics Opinions, 05-04: Electronic Storage; Confidentiality 7/2005. See http://tinyurl.com/qg6nrhh.

j. How long has the provider been in business and what is its financial health? What happens if the provider closes down? How will you get your data?

VIII. **MOBILE COMMUNICATIONS STRATEGY**: Of course, the ubiquity of cell phones allows lawyers to stay connected from anywhere. However, if there's more than one person involved in your firm's operation, an office phone system is pretty important. Even if it's just you, most lawyers don't want all of their clients calling their personal cell phone number because they're often be unable to answer it. From a disaster avoidance perspective, all law offices need an office communication system that is fault-tolerant and mobile. If something happens to your office or you unexpectedly can't get to your office for a period of time, your phones must continue to ring. Further, everyone in your office should still be able to answer and place calls from anywhere, even if your physical office no longer exists.

A. **VoIP Office Phone Systems**: I'm not a phone consultant, but you definitely need to understand VoIP[35] technology, what it is and the benefits of it over a standard POTS[36] system. "Hosted" versions of VoIP office phone systems generally don't require that you have any phone hardware in your wiring closet. All you need is an Internet connection and VoIP phones. If you choose to, you can even use a headset plugged into your computer as your phone (as opposed to a traditional office phone with a handset).

B. **What Is VoIP**: Voice Over Internet Protocol simply refers to a telephone system that uses the Internet to transmit phone calls. In a physical office, your office phone plugs into a network jack (just like your computer) rather than a telephone jack. In a home office, the office phone plugs into your wired or wireless Internet router. Nothing extra is needed. For example, I can take a VoIP phone home, plug it into my home wireless router, and I'm instantly connected to our office phone system. I can also plug a phone headset directly into my computer to make and receive calls (using software that gives me a “softphone” option). VoIP gives you a dial-tone just like a POTS system and the phones work exactly the same way. However, you do need to acquire special VoIP phones if you don’t want to use a softphone option. They're no more expensive than POTS phones and this link will take you to a good list of models and prices: http://tinyurl.com/5qybbb. However, VoIP providers typically have proscribed phones for use with their system which you can buy directly from the provider.

I use a headset attached to my computer (wirelessly, of course) from Plantronics that looks like this (and costs about $160).

[35] VoIP stands for Voice Over Internet Protocol.

[36] POTS stands for Plain Old Telephone Service (not trying to be cute here, this is really the acronym the industry uses for referring to standard land-line phone systems)

C. **Why Businesses Are Switching to VoIP**: Rather than give you a bunch of marketing blather, I'll just explain the benefits that drove our own office to switch and why we would never go back to POTS.

1. **Less Expensive**: VoIP plans typically include all long distance calls and every feature. So you just pay a flat fee per month, per phone and that's it.

2. **Amazing List of Features**: Most VoIP services include every phone system feature you've ever heard of as their standard offering. In most cases, you can't think of a feature that isn't standard.

3. **Easy to Use**: Each user can control their own system from a web page or application which shows their "dashboard." For example, I can login and I control anything I want about my phone. This means we don't have to call the "phone guy" every time we want to change something. For example, if I wanted to move an employee from one office to another, it used to take 3 days (for the phone guy to show up) and cost me $150 for the service call. Now, we just move the employee's phone to the new office and plug it in. That's it. There's no complicated configuration that needs to occur for their direct dial and phone set up to follow their phone - it just does.

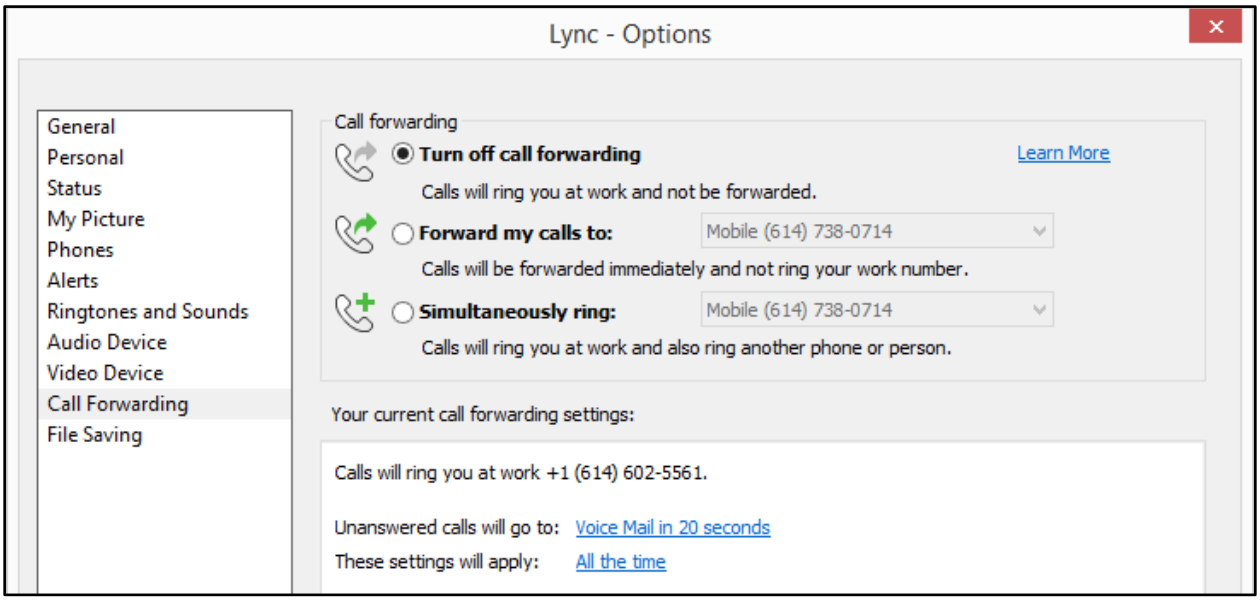
4. **Voice Mail from Anywhere**: I love this feature - all voice mails are automatically emailed to me as attachments. I can also retrieve voice mail from the Internet (any computer connected) or my phone. Now I never have to go through the annoying process of "dialing in" to retrieve my messages when I'm on the road.

5. **My Phone Can Travel With Me**: If I want to work from home, I can take a regular VoIP phone home and plug it into my home Internet router and I'm hooked into the office instantly. With my wireless headset, anywhere I have an Internet connection with my laptop connects me to my office

phone system. With either connection method, direct calls ring where ever I happen to be, people can transfer calls to me and everything works just as it does when I'm physically in the office. I can also use my computer as my phone or forward all of my office calls to my cell. When I'm on the road, it's great to be able to relax in the hotel room with my VoIP headset and handle phone calls without having to risk a bad connection on my cell phone.

6. **You Can Easily Have Multiple Offices On The Same System**: Since it all works through the Internet, it doesn't matter where your co-workers are physically located.

7. **Easy Call Forwarding**: I'm often out of the office for extended periods of time and prefer my office phone to auto-forward to my cell phone. Our old phone system allowed this, but I had to get out the manual and hit about 25 buttons on my phone to finally get it done. This is typical and so complicated that no one does it. With VoIP, it's just 2 clicks:



8. **Call Logs**: This doesn't sound like a big deal, but I find it extremely valuable that the VoIP system keeps a full log of all of my incoming and outgoing calls. I never lose a number thanks to this feature.

D. VoIP Options: Here are some options (there are many more than this):

1. **RingCentral** - http://www.ringcentral.com/solutions/small-business.html
2. **Vonage Business** - https://my.vonagebusiness.com/adminv2/
3. **Hover Networks** - http://www.hovernetworks.com/

4. **Proximiti** - http://www.proximiti.com/

5. **Jive** - http://jive.com/

6. **ShoreTel Connect** - https://www.shoretel.com/

7. **8 x 8, Inc.** - https://www.8x8.com/

8. **Fonality** - https://www.fonality.com/

9. **AVAD Technologies** - http://avadtechnologies.com/

E. **Microsoft Skype for Business**: This is "Microsoft's system for unified communications in the enterprise. It includes instant messaging (IM), voice and video calling and Web conferencing both within the organization and externally."[37]

This can be purchased or rented. There are many providers of hosted Skype for Business including Intermedia (www.intermedia.net) and Workspace Communications (http://tinyurl.com/ller9wx) among others.

Some people in our office have regular desk phones, but 90% of our people use wireless headsets that plug directly into our computers. For a list of Lync certified headsets, see http://tinyurl.com/jcqq4rb.

IX. MOBILE HARDWARE STRATEGY:

A. **No Desktop Computers**: Desktop computers are a bit less expensive than laptops, but their lack of portability makes them a liability in a disaster avoidance plan. If your employees have laptops and take them home every day and something happens at the office over-night (or over the weekend), everyone will still have their primary work tools with them. If you're going to invest in laptops, then you should insist that people take them home. Of course, this increases the possibility that they may be lost or stolen. However, it's not difficult to encrypt the laptops so that only authorized users can use them (see next paragraph).

An additional benefit of having laptops is that it creates the opportunity for additional productivity. They allow people to work in circumstances they would otherwise have been unable to work. For example, let's say one of your employees wakes up on a Monday morning and her daughter is sick and can't go to school. Now your employee may have to stay home to take care of her daughter. She may WANT to work but can't come into the office. If she took her laptop home over the weekend, then when her daughter goes back to bed, she can work if she wants to. That's what I mean by creating the *opportunity* for

[37] PCMagazine.com Encyclopedia - see http://tinyurl.com/n7pszov

someone to work if they want to. Sometimes, employees are coughing (for example) but don't otherwise feel bad. However, they may not want to come to the office and possibly get someone sick or annoy people with their coughing. So they have to stay home, but they still feel fine to work. Having a laptop might make that possible. If this kind of thing happens just once a year, you've easily cost-justified the additional amount a laptop costs over a desktop.

B. **VoIP Phone Systems**: See Article VIII above. For total mobility, consider avoiding desk phones and instead using USB connected wireless headsets because they're completely portable.

C. **Portable Scanners**: If you need to scan on the go, consider something like the Fujitsu ScanSnap S1300i or ScanSnap iX100.

D. **Portable Printers**: You will not be surprised to know that you also have portable printer options. For example:

1. **Hewlett Packard OfficeJet 100 Mobile Printer** - $160 - 6.9 x 13.7 x 3.3 inches and weighs 5.1 pounds. Prints 22 pages per minute.

2. **Canon Pixma iP100** - $160 for battery - 12.7"(W) x 2.4"(H) x 7.2"(D), 4.4 lbs.

3. **Epson WorkForce WF-100 Wireless Mobile Printer** - $200 - 5.1 x 15.1 x 10.2 inches, 4.6 lbs.

X. **ELECTRONIC DOCKETING AND TASK MANAGEMENT STRATEGY**: You need as many copies of your calendar and the firm calendar as possible to minimize the possibility of losing them. As we all know, missing a deadline in a legal practice can carry heavy consequences.

A. **Elements of an Effective Calendaring System**: Keys to an effective calendaring system that won't let you down are:

1. **Ease of Use**: A good docketing system shouldn't require a lot of training and explanation.

2. **Redundancy**: You need multiple copies of your calendar.

3. **Security**: At least one copy of your calendar should be off-site in the event of a fire or other disaster.

4. **Audit Trail**: Ideally, there should be some way of ascertaining who many any particular entry on a calendar.

5. **Cross-Checking**: Someone must be responsible for ensuring that the backup calendars are in sync with the calendars in use.

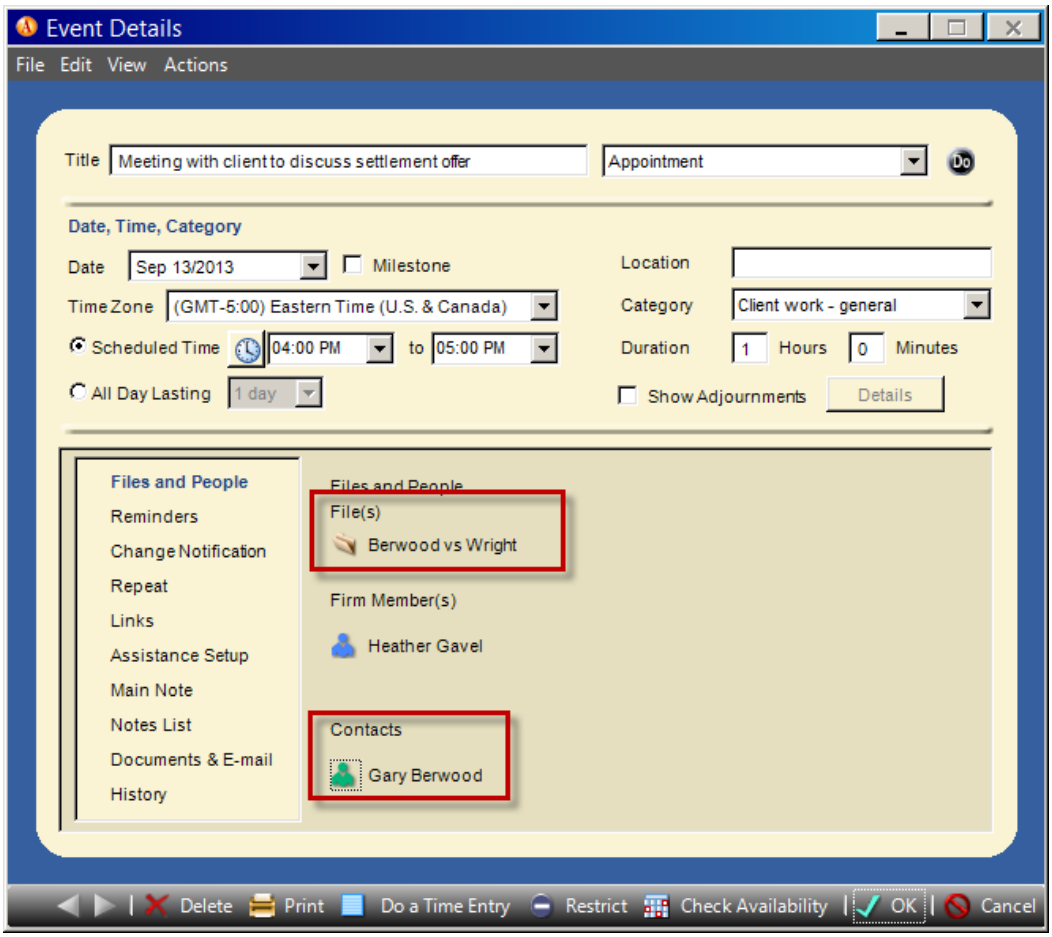
6. **Follow Up Tickler System**: There must be some means of ensuring that there is a follow-up date for every active matter. Some lawyers refer to these as "come-back" dates, but it's important there is a "next thing to do" on a calendar or task list for every active matter.

7. **Accountability**: Everyone (attorneys and support staff) must be accountable for proper docketing. In other words, it's everyone's job.

B. **Inadequacy of Paper and Programs Like Outlook**: Individuals who attempt to accomplish the foregoing goals with paper-based systems often find the process painful and waste large amounts of time entering, erasing and duplicating entries by hand. As a result, many have partially or completely abandoned paper in favor of Personal Information Manager ("PIMs") programs. PIMs keep track of calendars, tasks, names, addresses and phone numbers, among other things (Microsoft Outlook, Novell GroupWise, and Lotus Notes are good examples). While these programs do a fine job of managing a calendar, tasks and phone numbers, they're not designed specifically for a lawyer. For example, Outlook would be as useful to a maître d' or school teacher as it would to a lawyer because it has no special features which would specifically benefit any of them. Since PIMs do not address the information needs and work flow required by lawyers, they can definitely be improved upon. By contrast, practice management programs (aka matter management or case management programs) are designed specifically for lawyers, and meet their practice management and calendaring needs far better than any generic PIM. Having said that, a PIM like Outlook is much better than a paper-based system. The point is that there are better solutions than Outlook (specifically, practice management programs).

C. **How Practice Management Programs Help With Docketing**: The foundational elements of practice management are 1) People (contacts), 2) Events (appointments & tasks), 3) Files (client/matters) and 4) Time (billable time records). PIMs like Outlook only help with people and events and without the other two, they cannot provide a true practice management solution, no matter how they're customized. Here's how practice management programs are generally better than Outlook and other PIMs:

1. **Linking Events To Matters**: Every time you set up an appointment or task in a case management program, you can link it to a matter. Below is a new appointment dialog from a case management program and as you can see, the appointment is linked to a file (matter) and a contact (the client in this case).



As a result of the foregoing, this appointment will show up in the Berwood v Wright matter and in Gary Berwood's electronic contact card. By simply browsing to the electronic matter in a PMP, you'll see *every* appointment and task related to that matter, pulled directly from the calendars and task lists of everyone in your office. With PIMs, you cannot view all the events (appointments or tasks) related to a particular matter because there's no way to link them to a specific matter.

2. **Linking Events Together**: This is best illustrated through an example. Let's say you have a real estate closing scheduled for two weeks from now and you have two tasks you need to take care of 3 days before the closing: 1) review the title work, and 2) review the pro-forma closing statement. A PMP would allow you to link those tasks to the closing on your calendar. As a result, if the closing is moved back a week, the tasks would move with them automatically. In other words, moving the appointment on your PMP calendar simultaneously moves the two related tasks. Furthermore, if those tasks fell on a weekend or holiday, they would automatically re-schedule themselves to the first preceding business day. If the closing were canceled, the dependent events would

automatically be deleted with the closing. Secondly, if that sequence of events (closing + attendant reminders) is something you commonly set up for similar matters, you can save them as a block or precedent. By doing this, you can easily drop that sequence of events into future matters and the only thing you'd have to enter would be the closing date and time. Outlook, for example, has no means of accomplishing this.

3. **Redundancy**: Most PMPs will synchronize with Outlook or Google Apps (Google's web-based calendar, contacts, task list, etc.) and this is one very important way of achieving calendar redundancy. For example, if you're using a PMP that syncs with Outlook and you have Microsoft Exchange, your calendar in the case management can be replicated in Outlook, synced to your smartphone and iPad or Android tablet. This simple combination could easily give you 4 additional copies of your electronic calendar. Further, if you are using a server-based PMP, then you're hopefully getting a daily backup of all of the data on that server. If you're using a web-based PMP, then constant backup of all data stored in the program is normally included in the basic service.

4. **Audit Trails**: Any PMP worth its salt can easily track which user made any particular entry on a calendar or task list. Of course, this becomes more important when calendars and/or task lists can be shared electronically. For example, I have given several people in my office electronic authorization to add items to my calendar. If a new appointment shows up on my calendar that I didn't create, then it's easy to determine who put it there because our case management program records the author of ever event in the properties of the event itself.

5. **Cross-Checking**: If you have an electronic calendar that is syncing across multiple devices and programs, then the necessity of manually cross-checking one calendar against another disappears. You really have only one calendar even though it's accessible from many devices (computer, tablet, phone, etc.).

6. **File Follow Up**: This functionality is built into every PMP I've ever used or tested.

7. **Security**: First of all, a paper calendar can easily be lost and anyone who picks it up can read it and alter it. As such, a paper calendar has almost no security at all. Electronic calendars can be locked down and every PMP requires that one have a logon and password in order to gain access to the program in the first place. Further, you can restrict access to your calendar within a PMP so that even fellow users can't see and/or alter your calendar.

8. **Accountability**: A paper calendar can only be edited and maintained by the person in possession of it. With electronic calendars, everyone in your office can be involved.

D. Practice Management Programs Worth Considering: There are actually many more options than this, but here are some significant players in this area.

1. **Shrink-Wrapped options**:

- AbacusLaw by Abacus Data Systems, Inc. - 800.726.3339; www.abacuslaw.com
- Amicus Attorney by Gavel & Gown Software, Inc. - 800.472.2289; www.amicusattorney.com
- Case & Point by Corporate Legal Solutions - 800.597.4361; www.caseandpoint.com
- Case Management Groupware by Legal Files Software, Inc. - 800.500.0537; www.legalfiles.com
- CaseTrack by Economy Analysis Group, Ltd. - 207.367.2950; www.case-track.com
- Client Profiles by Client Profiles, Inc. - 866.720.5005; www.clientprofiles.com
- CLS/Summit by Computer Law Systems, Inc. (now merged into RainMaker Software, Inc.) - 800.328.1913; www.clssummit.com
- EsqWare Case Management by EsqWare, Inc. - 800.568.7996; www.esqware.com
- Law Base by Synaptec Software, Inc. - 800.569.3377; www.lawbase.com
- Legal Edge Law Firm Suite by Legal Edge Software - 610.975.5888; www.legaledge.com
- Needles by Chesapeake Interlink Ltd. - 410.363.1976; www.needleslaw.com
- Perfect Law by Perfect Law - 800.749.6200; www.perfectlaw.com
- Perfect Practice Case Management by ADC Legal Systems - 407.843.8992; www.adclegal.com

- PracticeMaster by Software Technology, Inc. - 402.423.1440; www.stilegal.com
- Prevail by Practice Technology, Inc. - 407.228.4400; www.prevail.net
- ProLaw Ready by Thompson/West - 800.977.6529; www.prolaw.com
- RealLegal Practice Manager by law.com - 888.584.9988; www.reallegal.com
- Time Matters by LexisNexis - 800.328.2898; www.Time Matters.com
- Trial De Novo by De Novo Systems - 800.755.9744; www.denovosys.com
- TrialWorks by Lawex - 800.377.5844; www.trialworks.com

2. **Web Based Options**:

- ActionStep: www.actionstep.com
- AdvologixPM: www.advologix.com
- Amicus Attorney Cloud Edition: www.amicus-cloud.com
- Clio: www.goclio.com
- Credenza: www.credenzasoft.com
- Houdini Esq: http://houdiniesq.com/esq.html
- LawRD: www.lawrd.com
- Rocket Matter: www.rocketmatter.com
- Total Attorneys: www.totalattorneys.com

E. Practice Management Programs Are Designed To Manage Tasks: Generally speaking, PMPs make sense when a lawyer has a high volume of cases and/or the lawyer simply desires a high degree of organization. Within a PMP, every future task on a case is set up as a task related to the case. As such, you can go to any particular case and see what has to be done next. Further, you can run reports which show you the next thing to be done on every single active matter. Finally, most PMPs don't show you a task until you need to deal with it. In other words, you won't see a big list of every future task, you'll only see the ones which are due.

F. **Task Management**: Unfortunately, there's no panacea when it comes to task management. What works for one person doesn't work for the next. However, there are some principles that everyone can put to use.

1. **Read Getting Things Done**: Getting Things Done: The Art of Stress-Free Productivity by David Allen is $9 on amazon.com. Mr. Allen is not a techie, but his ideas can be translated to any analog or digital approach for tracking tasks. In terms of task management, the concepts are solid.

2. **Remember the Hit By A Bus Rule**: It's a little morbid, but the hit-by-a-bus rule dictates that if you disappear tomorrow, others in your office should be able to figure out what is on your task list so balls aren't dropped and malpractice claims done ensue. I've talked to lawyers who track their tasks by "how they arrange things on their desks" and lawyers who use random sticky notes, cryptic hand-written notes in their Day Planner or who send themselves emails to remind themselves about things to do. These techniques will convey little useful information to anyone else and should be abandoned in favor of task management techniques that reasonable people can decipher. Whatever system you use, at least one other person in your office should be able to translate it. PMPs can make this a lot easier on everyone involved because they standardize the methods by which tasks are tracked.

3. **Your Inbox Is Not a To Do List**: Unfortunately, lots of people feel that their inbox is a way of reminding them of things they need to do. The problem is that the subject line of an email often has nothing to do with the underlying task. Secondly, if you have a lot of email, you can only see a certain number of them on the screen at once. If an email gets pushed off the bottom of the screen and you can't see it, then it can't remind you of anything. In view of these things, it's important that you NOT use your inbox as a to-do list.

G. **File Follow Ups**: Here's the rule: every active matter should have a follow up date or a "next task to be completed." Failing to adhere to this rule is exactly how balls get dropped. The problem is, how does one track this? Manual systems can actually work well to solve this problem if users are diligent and have some means of setting files for future follow-up. On the other hand, PMPs all have a means of handling file follow-up. Not only can you typically set up a task that reminds you of files that need attention, but there is often a report solution to the issue. In many PMPs, there is a report called something similar to the "Last/Next Report." You can select all active matters to run it and it will display the last thing that was done and the next thing that needs to be done. Obviously, if you run a Last/Next Report on all active matters and the "next thing to be done" column is empty for any active matter, that would be a red flag.

XI. **CLIENT DATA BACKUP STRATEGY**: This subject is an entire seminar by itself. So I'm not going to go into great detail about this, but I'm going to give you some general rules and principles to follow in order to keep your data safe.

A. The Backup Rules:

1. **You Own This**: You cannot just *assume* that your data is being backed up. Trust but verify. You need to know how to confirm that your data is backed up every day and someone in your office needs to be responsible for it. If you lose all of your client data, you won't be able to blame the person who handles your computer work or anyone else. It's on you.

2. **Every Day, No Excuses**: You must be backing up all of your important data every day.

3. **Unattended Is Best**: The best backup methods do not require you to remember to do anything for the backup to occur. Unattended backups are the best for two important reasons. First, if someone has to remember to do it, they'll forget. Second, backups sometimes take a long time and they'll usually bog down your system when they're running. Therefore, they're best run at night when no one is using your network or their computers. This means that you cannot use backup media that is not large enough to backup all of your data. Therefore, CDs, DVDs and flash drives are eliminated because unless you have hardly any data, it's not going to fit on a single CD or flash drive and that means you'll have to baby-sit the backup and feed it additional media when the first one is full.

4. **Backup Everything**: DO NOT backup only the data you've created (i.e., Word or WordPerfect files, etc.). You want to back up the entire drive of the computer you're backing up. When you restore, you want the operating system back the way it was, you want all of your printer drives installed, your video driver installed, your network adapter driver installed, etc. Trying to install all of your programs from CD and getting your settings back to the way they were pre-crash can literally take months.

5. **You MUST Check the Backup Log Every Day**: Most backup devices don't tell you if they worked properly or not. The only way to make certain is to look at the "backup log" which the tape backup software maintains. Someone needs to do this every single day to make sure there were no malfunctions.

6. **Replace Tape Media At Least Annually**: If you're using a tape drive as a backup device, you need to write a "born-on" date on the tape and replace them at their 1 year birthday. Tapes lose their ability to hold data

over time and you don't want to take the risk that your successful backup is not restorable due to bad media.

7. **Off-Site Storage**: If you're using tapes, take yesterday's backup home with you every night. If you're using an external hard drive, burn your important data to CD periodically and put it somewhere off-site. You can also use one of the Internet based backup options I'll mention later.

8. **Do Not Rely On Incremental Backups**: An incremental backup means you're only backing up files that have changed since the last full or incremental backup. You can get quite a chain of these going and hopefully there's a full back up at the beginning of the chain. People have used this method because it's faster and takes less space. Incremental backups are NEVER, acceptable. First, trying to restore something when the data is scattered across many incremental backups is a nightmare and takes a very long time. Second, if one of those incremental backups gets screwed up, it may eliminate the possibility that you can restore anything that was backed up subsequently. You want to do a full backup of everything, every night.

9. **Run Test Restores At Least Once A Month**: You need to do this to verify that you *can* restore and also to make sure you know how to do it.

10. **Have a Secondary Backup**: If you're using a tape drive, get an external hard drive as a secondary backup or use one of the online backup options. Just make sure you have an extra copy of your stuff.

B. **Backup Device/System Options**: Here's an area where you cannot cut corners, regardless of your budget. You don't have to spend a ton of money to make sure your data is secure, but it is catastrophically expensive to lose all of your electronic information.

1. **Tape Drives**: High end tape drives used to be the best and most reliable option for servers, but many computer consultants are moving away from them due to the emergence of better options - primarily multiple internal or external hard drives. Good tape drives are rather expensive. They're also typically slow, the media has to be replaced annually and the drives wear out. For those reasons, we no longer recommend them for individual PCs or servers.

2. **External Hard Drives**: There are external hard drives designed specifically as backup devices and this is our recommendation. They can hold an incredible amount of data and are very inexpensive. The annoyance is that you have to unplug one of them and take it home with you every day (they need to be rotated so you always have one full backup offsite).

Other than that, they're very fast and reliable. Look for at least 1 TB of storage and a 7,200 rpm drive. If your computer supports USB 3.0, Thunderbolt or FireWire, look for drives that will allow you to take advantage of the faster speeds those interfaces offer. There are many options.

3. **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 an configuration in which multiple hard drives are arranged so that data is stored 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 a number of different "levels" of RAID, including RAID 1 (straight mirroring when two drives both containing 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 http://tinyurl.com/mmqrf. The main drawback of a NAS device is that you cannot really take it off-site. However, it can contain multiple backups of your data and if RAID is employed in the device, it's extremely unlikely that you'll have a simultaneous crash of all of the drives contained inside the NAS.

   There are new NAS devices that also provide total cloud access to the data they hold which is pretty amazing. Check out the WD My Cloud EX4 8 TB as an example of this.

4. **Internet Backup Options**: This is becoming more and more common as a ***secondary*** backup method. Some use it as a primary backup but we recommend against this because internet connections frequently go down.

   - Carbonite - http://www.carbonite.com/ (my favorite)
   - Mozy Pro - http://mozy.com/product/mozy/business
   - Mozy Home - https://mozy.com/product/mozy/personal
   - iBackup: https://www.ibackup.com/index.html
   - CrashPlan - https://www.code42.com/crashplan/

- SOS Online Backup - http://www.sosonlinebackup.com/

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

C. Recommendations Regarding Backup Hardware and Software: For a small firm, consider something like this:

1. **Server**: There are simply too many options out there and you should rely on your network expert for this. Ultimately, you can pay more and more for fault tolerance and quick recovery. When you've reached a point of diminishing returns in terms of what you've spent is hard to tell. Just remember the rules: You want everything backed up daily and you need at least one copy on-site and one copy off-site.

2. **Personal Desktop or Laptop**: I would recommend that you buy an external hard drive (2 TB or larger) and use a Carbonite Personal Plus plan for $100/year. You get unlimited online storage and the ability to mirror your computer's entire internal hard drive to the external drive simultaneously.

XII. OTHER COMPONENTS OF YOUR DISASTER AVOIDANCE STRATEGY:

A. Preventative Maintenance for On-Site Servers:

1. **Managed IT Services**: Managed IT Services use a technology framework designed exclusively for monitoring, maintaining and supporting business networks - remotely, securely and proactively. This allows the provider to manage your network securely across the Internet without the need for VPN connections or opening ports on your existing firewall. This approach minimizes downtime and increases productivity at your office because the managed services provider is often able to fix problems before anyone in your office even realizes there is a problem and the preventative maintenance is done in the middle of the night. Furthermore, most of these services also include “help desk” - software support for all users via phone, email and web meeting.

2. **Find a Good Computer Geek**: Server specialists can monitor your backups and event logs on your server for you. Many bad events can be predicted by checking these things. Tell your computer person that you want them to be pro-active in helping you avoid data loss. If they don't know what to do, find another computer person. Computer companies that know what they're doing are not going to be the cheapest option out there. If

the lowest price is your primary determinant in choosing IT support, you're likely going to regret it.

B. Power Protection for Your Computers:

1. **Surge Suppressor/Uninterruptible Power Supply ("UPS")**: Without exception, every computer on the network (workstations or servers) should be plugged in to a UPS. Most units have both plugs that are supported by the battery in an outage, and plugs that just have surge suppression (for your laser printer). But even more important than outage issues are the effect brownouts can have on your computer equipment. A UPS will supply extra voltage to your computer equipment when the voltage from the wall falls below a certain level. How is this a crisis? Power issues can cause component failure, such as bad hard drives, bad motherboards, bad RAM, etc. Bottom line, having proper protection from electrical issues is like having insurance. You have to do it. Don't forget to protect all the other things that plug into your network, such as printers, speakers, scanners, hubs, switches, routers, modems, etc. Most laser printers draw too much power to be plugged into the battery backup outlets of a UPS unit, so make sure they are plugged into the surge suppression-only outlets.

2. **Get UPSs or Surge Suppressors on Everything Connected To Your Network**: Spikes can come in via any connected device. Get your switch/hub on a surge suppressor (recommend a UPS), make sure all of your printers and everything else connected to your computer is at least plugged into a surge suppressor.

3. **Plain Surge Suppressors**: You can get plain surge suppressors that are good (such as the Tripp Lite Isobar4 (part #ISOBAR4ULTRA). However, they cost as much ($41) as many UPSs but can't keep your PC running in the event of a black-out or brown-out. Be advised that the cheapo power strips are just extension cords and aren't going to help you avoid problems. If you bought your surge suppressors in a 3 pack for $9.95 at Wal-Mart, you've wasted your money.

4. **Warning About VA Ratings**: Make sure the VA rating of your UPS is high enough to support the equipment you're plugging in. To determine a UPS's VA rating, then calculate the VA ratings (wattage) of what you're plugging in (amps x 120 volts). We had a client who had a Tripp Lite SmartUPS 1050 - ($347 – only 705 VA). He plugged in the following:

   - Dell Optiplex – 720 watts
   - Dell monitor – 180 watts
   - Printer – 936 watts

The first time the power went out, he fried his Tripp Lite and it wouldn't even work again. Since he exceeded the VA rating, his warranty was void. Sadly, the Dell representative he bought the foregoing equipment from was the one who recommended this particular UPS. Since the computer alone exceeded the VA rating for the UPS, he obviously didn't know about this little issue either.

5. **Our Recommendation**: We recommend a 1500 VA UPS for a desktop computer and a 500 VA UPS for a laptop.

C. **Router/Firewall/Switch**: If you're going to have a network or you're going to have high speed Internet access, you must have one of these. We've had clients who were "hacked" the result of which was that confidential client information was compromised. It is malpractice per se if you leave yourself open to this possibility. Talk with your IT professional about how your network is protected against hackers and make sure you have the appropriate hardware and/or software in place.

D. **Antivirus Software**: This obviously isn't hardware, but you must have antivirus on every computer and your server(s) and their definitions must be automatically updated weekly. Anything less, and you leave yourself open for attack.

E. **Protect and Change Your Passwords**: Stop writing your passwords on sticky notes on your monitor. You need to change them periodically and keep them in a place where others aren't likely to find them. They should also be "strong" passwords which is a mix of numbers and letters (and usually one symbol like $ or %). No one should know your logon and password except you. The same goes for your server. **On the other hand**, you must require that every employee provide you with their current logon and password. Employees shouldn't be able to keep you out of *your* computers because you don't know the password. If you want to see how long it would take a hacker to break your password with a "brute force" password hacking program, go to www.howsecureismypassword.net and enter some of your passwords.

F. **Don't Leave Your Computer On and Logged In**: When you leave the office for anything, either log off or lock the workstation. Locking the workstation is easily done by holding down on the Windows key on your keyboard (see picture to the right) while striking the L key. This will not exit your programs or cause your computer to re-boot. However, no one can access the computer unless they know your password (which they hopefully don't). Turn your computer off when you leave the office. If you have to leave it on because you're accessing it remotely via www.gotomypc.com or www.logmein.com, then at least log off and

turn the monitor off. You'll still be able to log in remotely using either of those services.

G. **Stop Waiting For Computers to Die Before Replacing Them!** Replacement through attrition is the most expensive, disruptive and time wasting method of handling that task. In spite of that, most law firms only replace computer hardware when it finally dies. The useful life of a computer is 3 years, if you didn't buy a bargain, low-end computer in the first place. If you buy behind the curve and get a discontinued or under-powered computer, you've just handicapped your efficiency and shortened the useful life of the computer. Here's why you need to schedule the replacement of hardware before the hardware actually stops working:

1. **Data Loss**: Unless you're backing everything up on every computer, every day, then you're likely to lose something that was stored on the computer that stopped working or crashed.

2. **Pay Too Much**: You have no time to research, plan, or find the best price from the best vendor. You have to run out and buy a new computer, printer, etc. as quickly as you can. This will cost you lots of money because you're going to get the worst deal possible simply because you can't wait.

3. **Inappropriate Configurations**: Most bricks and mortar computer sellers cater mostly to the home market for computers. Their selection of business-oriented computers will be limited and they'll likely have very little good advice regarding what you should buy. Instead of getting Microsoft Office included with the new computer, you'll end up with games. Instead of Windows Vista Business, you'll get Windows Vista Home. Instead of an smaller hard drive appropriate for an office computer, you'll pay extra for a 500 GB drive you'll never even fill 10% of. Instead of simple speakers, you'll pay extra for 3D Surround Sound with a powered sub-woofer. You get the idea.

4. **Down Time**: It is very expensive for you or any of your employees to sit at their desks, unable to work. If your computers don't work, then you don't work.

5. **Charitable Deductions**: If your old computer actually works, then you could donate it to charity and take a legitimate tax deduction. If it doesn't work, then it'll probably set in your computer graveyard closet until you finally have to pay someone to take it away.

H. **Write Your Own Cookbook!** Firms can come to a screeching halt when a long-time administrative employee leaves or dies. This is the person who knows

everything about your firm; and they are usually the *only* one who knows everything about your firm. When this person is gone, you can't find anything – not even paper towels! Typically this person is the only one who bills, the only one who writes checks, the only one who knows how you have always done things.

How do you get away from this dangerous situation? Create what we call a firm cookbook. Now, I know that sounds overwhelming and you think there is no possible way you could do that, but think again. Why do we call it a cookbook? Because you're going to add recipes to it, all broken down into steps. One recipe might be "How to Restore a File From Backup." It would tell you how to log onto the server, how to access the backup software, what to click on to see the list of files you can restore, and how to restore them. Another recipe might be "How To Run Invoices." It would explain in great detail how to run invoices from the fees and expenses entered into your accounting system.

Have each key employee take the time to carefully document every step they take in accomplishing all important tasks assigned to them. Yes, it can be time consuming, but if you don't do it now, it will never get done. Include everything from how you want your phones answered, to how you want prospective client calls handled, to billing processes, to supply ordering, and everything in between.

I. **Get a Business Succession Plan in Place**: If you have a successor in mind or partners who will carry on in the event of your death, get a plan in place to make sure the transition is as smooth as it can be.

J. **Know Your Options - Lost Data Can Often Be Recovered For a Price**: There are many companies that specialize in recovering data from crashed hard drives, regardless of the cause. They are expensive, but not getting your data back may be even more expensive. Some options:

- Disk Doctors - www.diskdoctors.com
- Ontrack Data Recovery - www.ontrackdatarecovery.com
- DriveSavers - www.drivesavers.com
- ESS Data Recovery - www.essdatarecovery.com
- IntelliRecovery - www.intellirecovery.com
- ADR Data Recovery - www.americandatarecoveryinc.com

K. **On-Site Servers Need Redundancy**: True file servers have the ability to protect against hardware failure. For example, servers should have the following characteristics:

1. **RAID (Redundant Array of Independent Disks)**: Without getting too technical, this is an arrangement in which multiple hard drives are arranged so that data is stored across all of them simultaneously. This gives you better performance, capacity and reliability than a single large drive. There are 5 levels of RAID, from RAID 1 (straight mirroring when two drives both containing the same data) to 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 http://tinyurl.com/cpm2c6h.

2. **Redundant Network Adapters**: This is common because they are inexpensive and they fail.

3. **Redundant Power Supplies**: Again, if the one in use goes bad, the back-up power supply kicks in immediately without even shutting down the server.

L. **Contact List**: It's a good idea to maintain an electronic list of every employee's cell phone numbers, home phone numbers and numbers of relative they would contact in an emergency. That way, you can all find each other after a disaster.

M. **Bank Records**: Put together a kit that contains with blank checks, operating payroll and trust account information. It would be a good idea to make sure your bank's computers aren't located in a potential disaster area.

N. **Have a Pre-Determined Place to Go**: Find a hotel, executive office suite location or friend's office you could all head to in the event of a disaster. Have directions and phone numbers.

O. **Have Evacuation Plan for Your On-Site Servers**: Make someone responsible for packing them up and taking them to the predetermined location. Make sure the person responsible knows how to shut them down properly, what to pack up and what can be left behind.

P. **Consider Business Interruption Insurance**: This may keep you going financially.

By Barron K. Henley, Esq.
bhenley@affinityconsulting.com
Affinity Consulting Group
1550 Old Henderson Road, Suite S-150
Columbus, Ohio 43220
Phone: 614.340.3444
Fax: 614.340.3443
Web: www.affinityconsulting.com