Security in your Practice: Mobile Devices, Firewalls, Using the Cloud

Materials By: Nerino J. Petro, Holmstrom Kennedy P.C., Rockford

Security in your Practice: Mobile Devices, Firewalls, Using the Cloud

Contents

Cover Image sourced from PresenterMedia.com pursuant to subscription and license.

1 RULES OF PROFESSIONAL CONDUCT

The Minnesota Rules of Professional Conduct (MRPC) is the first place that lawyers should look to when considering cloud computing. Unfortunately, as with other modern technologies, many states Rules do not yet specifically address cloud computing. This means that until we have these state only specific resources, we have to interpret the existing Rules pending any updates and changes and the issuance of state specific Ethics Opinions. Until that time we can look to those states that have adopted changes to their rules or issued ethics opinions on use of cloud computing by lawyers and their staff.

As of August 2015, the ABA Law Practice Division Legal Technology Resource Center (check it out at http://bit.ly/18pEDg9) listed ethics opinions from 20 states that have addressed the issue of the use of cloud computing by lawyers with Wisconsin opinion EF-15-01 being the most recent. . The full list of all 20 opinions along with a quick reference, summary of their findings and links to the full decisions are found at http://bit.ly/QBU1dN. The good news is that every one of these 20 opinions all provide that lawyers may use cloud computing in their practices and the standard of care that must be followed is to use "reasonable care" when selecting a cloud service provider. As with many issues regarding interpretation of the Rules of Professional Conduct throughout the United States, the devil lays in the details of each opinion. Specifically, differences exist in these 20 opinions regarding how each addresses the specific requirements as to what comprises "reasonable care" when determining whether a specific cloud computing service is acceptable for use by a lawyer or firm.

MRPC 1.1 requires a lawyer to provide competent representation. In August 2012, the ABA amended the Comment to Rule 1.1. To maintain competence, "a lawyer should keep abreast of changes in the law and its practice, **including the benefits and risks associated with relevant technology**…." A lawyer must act competently to safeguard information protected by MRPC 1.6 from inadvertent or unauthorized disclosure (see comments 17 & 18 to MRPC Rule 1.6) . In addition, a lawyer must act competently to safeguard his or her unrestricted access to data that is stored on servers not owned by the lawyer. Minnesota has adopted this change to MRPC 1.1

1.1 ESTABLISHING A STANDARD OF REASONABLE CARE

1.1.1 The ABA Commission on Ethics 20/20 Working Group on the Implications of New Technologies identified potential confidentiality and access problems involved with cloud computing. These problems included:

a. storage in countries with less legal protection for data,
b. unclear policies regarding data ownership,
c. failure to adequately back up data,
d. unclear policies for notice of data breach,
e. insufficient encryption,
f. unclear data destruction policies,
g. bankruptcy of cloud providers,
h. protocol for a change of cloud providers,
i. disgruntled or dishonest insiders,
j. technical failures,
k. server crashes,
l. viruses,
m. data corruption,
n. data destruction,
o. business interruption (e.g., weather, accident, terrorism), and
p. absolute loss (i.e., natural or man-made disasters that destroy everything).

These identified confidentiality and access problems should alert anyone contemplating the use of cloud services to select a suitable provider, take reasonable precautions to back up data and ensure its accessibility when the user needs it.

1.1.2 As the So what are some of the differences as to the factors which constitute "reasonable care" under these 20 recent ethics opinions? For example, Pennsylvania requires that a service provider provide "the firm with the right to audit the provider's security procedures and to obtain copies of any security audits performed." Alabama requires that lawyers "reasonably ensure that the provider will abide by a confidentiality agreement in handling the data." These requirements are unrealistic in light of the relative bargaining position of a lawyer and a company such as Google. Nerino Petro, Jr., The Ethics of Cloud-based Services, Wisconsin Lawyer, Vol. 85, No. 9, September 2012.

1.1.3 Unlike the Alabama and Pennsylvania opinions, Massachusetts Bar Association Opinion 12-03 strikes a balance between a lawyer's obligation under the Rules of Professional Conduct and the realities of the commercial market in determining what factors constitute reasonable care. The following recommendations are based on the Massachusetts' opinion list of factors for determining reasonable care.

- Examine the provider's terms of use and written policies and procedures with respect to data privacy and the handling of confidential information.
- Ensure that the provider's terms of use and written policies and procedures prohibit unauthorized access to data stored on the provider's system, including

access by the provider itself for any purpose other than conveying or displaying the data to authorized users.

- Ensure that the provider's terms of use and written policies and procedures, as well as its functional capabilities, give the lawyer reasonable access to, and control over, the data stored on the provider's system in the event that the lawyer's relationship with the provider is interrupted for any reason (e.g., if the storage provider ceases operations or shuts off the lawyer's account, either temporarily or permanently).
- Examine the provider's existing practices (including data encryption, password protection, and system backups) and available service history (including reports of known security breaches or 'holes') to reasonably ensure that data stored on the provider's system actually will remain confidential, and will not be intentionally or inadvertently disclosed or lost.
- Periodically revisit and reexamine the provider's policies and procedures to ensure that they remain compatible with the lawyer's professional obligations to protect confidential client information reflected in Rule 1.6(a).

1.1.4 Moreover, the factors listed in the Massachusetts' opinion are consistent with the August 2012 amendments to the ABA Model Rules of Professional Conduct. A new paragraph was added to Rule 1.6 requiring a lawyer to "make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of the client." Additional language was also added to create Comment [18] to clarify what factors should be considered to determine reasonableness. These factors 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).

1.1.5 Keep in mind that none of the ethics opinions require extraordinary efforts or a guarantee that information will not be inadvertently disclosed. They only require that lawyers use reasonable care in selecting a service provider.

1.1.6 Currently, there is no definitive answer as to whether a lawyer must obtain a client's consent to use a third-party provider for storage of client information. If you think of agreements that you sign for other professional services - such as dental and healthcare - you generally do not find any disclosure regarding cloud based services in them. This is true even though many healthcare providers routinely use cloud services. Many in the legal community take the position that that lawyers are no different than those other professions and if they do not need to disclose, neither do lawyers. Another group believes that the IRPC (and all other versions of the Rules) impose unique obligations on lawyers and that it is prudent to obtain a client's consent. Lawyers should at least, include in their engagement letters a statement that the lawyer uses such a provider, that the lawyer believes the information to be secure, and that invites the client to discuss any concerns with the lawyer.

1.2 Reasonable Care Checklist:

1.2.1 General Precautions

- ❒ Do you regularly back up data to allow the firm to restore data that has been lost, corrupted, or accidentally deleted?
- ❒ Have you installed a firewall to limit access to the firm's network?
- ❒ Do you limit information that is provided to others to what is required, needed, or requested?
- ❒ Do you have procedures in place to avoid inadvertent disclosure of information? (For example, do you have procedures in place to avoid the disclosure of confidential information contained in metadata?)
- ❒ Do you verify the identity of individuals to whom you or your employees provide confidential information?
- ❒ Do you refuse to disclose confidential information to unauthorized individuals (including family members and friends) without client permission?
- ❒ Do you encrypt electronic records (including backups) containing confidential data?
- ❒ Do you have electronic audit trail procedures to monitor who is accessing the data?
- ❒ Do you have procedures in place to address security breaches, including the identification of persons to be notified about any known or suspected security breach involving confidential data?
- ❒ Do you have procedures in place requiring that employees of the firm who use cloud computing receive training on and abide by all end-user security measures, including, but not limited to, the creation of strong passwords and the regular replacement of passwords?
- ❒ Do you have an alternate way to connect to the internet since cloud service is accessed through the internet?
- ❒ Do you protect the ability to represent the client reliably by storing a copy of digital data onsite?

1.3 Cloud Services Provider Checklist

- ❒ Have you investigated the provider's security measures, policies and recovery methods?
- ❒ Have you investigated whether the provider has a third-party audit of security?
- ❒ Have you investigated the provider's system for backing up data?
- ❒ Have you investigated the provider's security of data centers and whether the storage is in multiple centers?
- ❒ Have you investigated the provider's safeguards against disasters, including different server locations?
- ❒ Have you investigated whether the provider has an uptime guarantee and whether failure results in service credits?
- ❒ Have you investigated the provider's history, including how long the provider has been in business, if it has a good operating record, and if it is recommended by other law firms?
- ❒ Have you investigated the provider's funding and stability?
- ❒ Have you investigated whether the data is in a non-proprietary format?
- ❒ Have you investigated the provider's policies for data retrieval upon termination of the relationship and any related charges?
- ❒ Have you investigated the provider's process to comply with data that is subject to a litigation hold?
- ❒ Have you investigated whether the provider's service agreement clearly states that the attorney owns the data?
- ❒ Have you investigated whether the provider's service agreement contains legal restrictions regarding its responsibility or liability, limitation on damages, or choice of law or forum?
- ❒ Does the provider explicitly agree that it has no ownership interest in the data?
- ❒ Does the provider have an enforceable obligation to preserve security?
- ❒ Does the provider have an obligation to notify you if it is requested to produce data to a third party and an obligation to provide you with the ability to respond to the request before it produces the requested information?

- ❒ Does the provider have the technology built to withstand a reasonably foreseeable attempt to infiltrate data, including penetration testing?
- ❒ Does the provider include in its service agreement an agreement about how confidential client information will be handled?
- ❒ Does the provider give you the right to audit its security procedures and to obtain copies of any security audits performed?
- ❒ Does the provider host your data only within a specified geographic area? (Or if, by agreement, the data are hosted outside the United States, does the provider determine whether the hosting jurisdiction has privacy laws, data security laws, and protections against unlawful search and seizure that are as rigorous as those of the United States and the particular state?)
- ❒ Does the provider give you a method of retrieving data if you terminate use of its service, if it goes out of business, or if there is otherwise a break in continuity of service? Does the provider give you the ability to get data "off" its servers or a third-party data hosting company's servers for your own use or in-house backup offline?

2 STEPS TO PROTECT YOUR DIGITAL ASSETS.

2.1 STRONG PASSWORDS ARE A MUST.

Passwords are something that we all need in the modern world but that we all love to hate. Strong passwords are a must, but strong passwords are also difficult to remember. Too often people pick something that is easy to remember or they don't believe that anyone can gain access to say their server so they choose something like passw0rd or pa$$word

2.1.1 Password Best Practices

- 10 or more digits
- Mix of lower case and upper case letters
- Numbers
- Special characters

Here are two examples:
c4RV^6aJ$^ - 10 characters
3q^eDKmBVXn4y – 13 characters

2.1.2 Password Best Worst Practices

Examples of bad passwords:

password	qwerty
Trustno1	Adobe123
123456	123456789
monkey	password1
P@ssw@rd	admin

Go ahead and do an internet search on "worst password" and you will find numerous articles including:

Network World's Top 25 most commonly used and worst passwords of 2014
http://bit.ly/1OHbZfZ

Yahoo Tech's A List of 500 Passwords You Shouldn't Be Using http://yhoo.it/XeH9DN

2.2 USE A PASSWORD MANAGER.

Use a password manager to store your passwords. You only have to remember one strong password that will allow you to access your password repository. You can then create separate passwords for each site and not have to worry about keeping them all straight. Best in class

password managers do more than simply mange your passwords but provide the ability to generate passwords using criteria you set, keep secure notes and some also integrate with additional security products for 2FA/MFA.

There are a number available that provide basic protection for free and business/enterprise level protection for a small annual fee. Best in class solutions include:

LastPass www.lasptass.com

1Password https://agilebits.com/onepassword

KeePass http://keepass.com/ and others

2.3 Use 2FA or MFA

Most cloud services allow you to add an additional layer of security to allow you to further protect access to your online accounts. Many of these services such as Dropbox refer to it as two step verification. In the technology world, this is known as two factor or multifactor authentication; 2FA and MFA respectively.

2.3.1 2FA requires something you know, like your password plus at least one of the following:
Something you have, such as a authentication code or security dongle; or

Something you are, such as a fingerprint or retina scan.

2.3.2 Some good articles to read to learn more include:
c|net's article Two-factor authentication: What you need to know http://cnet.co/1r6NjlP

lifehacker's article Here's Everywhere You Should Enable Two-Factor Authentication Right Now http://bit.ly/XeYlsM

2.3.3 There are also apps for smart devices to generate the authentication code. For desktop systems and business/enterprise class solutions there are also items such as the Yubikey which works in conjunction with LastPass and other verification technologies. You will find a Yubikey product comparison at
http://www.yubico.com/products/comparison/features/

2.3.4 For larger firms or firms that need even stronger authentication capabilities, take a look at:
Fortinet TimeBased one Time Password tokens at http://bit.ly/Xf1xog or
Safenet eToken key at http://bit.ly/Xf1xog .

2.4 Encryption

According to Microsoft:

Encryption is a way to enhance the security of a message or file by scrambling the contents so that it can be read only by someone who has the right encryption key to unscramble it.

2.4.1 There are 2 types of encryption for computers and smart devices:

- Asymmetric AKA public-key encryption that uses a public key know by everyone and a private key known only to the recipient ; and
- Symmetric encryption where you use the same key to encrypt and decrypt the information. An example of symmetric encryption would be the, which uses the same key to encrypt and decrypt a user's data.

2.4.2 Encryption on data in the cloud, on portable devices such as tablets and laptops and even portable USB flash drives, is important due to the majority of states now having in place data breach lass that require firms to notify clients if data is stolen or lost. If you are in NV and MA, the law requires that you encrypt personal information if it is taken from the office.

2.4.3 While most cloud storage services provide encryption, THEY control the encryption key. The downside to the provider controlling the encryption key includes:

- Provider "controls" the encryption key;
- Provider's staff can decrypt your data if required by court or other government order;
- Provider's staff could decrypt data on their own; and
- Encryption key and data can be stored on the same servers making it much easier for a hacker to gain access to your data as they only need to gain access to one systems, not two if the data and the encryption keys are stored on different network and servers.

The upside to the provider controlling the encryption key includes:

- You never have to worry about losing or forgetting the encryption key;
- They have policies and procedures in place to protect your privacy;
- They generally provide better network security than you can in your own office; and
- They often times store your data in geographically different data centers to provide redundancy.

2.4.4 Not all services control the encryption key. For example SpiderOak allows you to control the encryption key as well as several other services. Generally however, services like SpiderOak are not as user friendly as Dropbox or Box.com.

2.4.5 Many in the legal technology world believe that the concerns over a provider controlling the encryption key is overblown: lawyers have entrusted their files to couriers and offsite storage providers for years, and this is much the same as we rely on others to protect our data.

2.4.6 When it comes to desktop tools, the best solutions encrypt the entire hard drive on a desktop or laptop computer. While there are a number of products that will encrypt files or folders, encrypting the entire drive means you don't have to worry about whether or not you protected a file if your computer is lost or stolen. Even if your device is lost or stolen, if the entire storage drive is encrypted they can't simply bypass the operating system and still get at the data. For desktop and laptop computers, take a look at:
Windows 7 Ultimate & Enterprise include Bitlocker
Windows 8.1 Pro & Enterprise include Bitlocker
FileVault and FileVault2 forOS X
Symantec Encryption Desktop (formerly PGP Whole Disk Encryption).
Truecrypt open source – no longer in development which ceased in summer of 2014 although it still work with Windows XP, 7 and 8.

2.4.7 When it comes to cloud based storage service such as Dropbox, Google Drive, Box.com and others there are a number of tools that may be able to provide encryption using an encryption key that you control. This is in addition to the encryption provided by the provider such as Dropbox.

2.4.8 Users do need to check carefully before using one of these cloud based tools as some of them only work with Dropbox while others work with Dropbox, Google Drive, OneDrive and Box.com. Also, some are free while others have commercial versions.

2.4.9 For other encryption ideas for the desktop, portable drives and the cloud, you may wish to read:
http://www.gfi.com/blog/the-top-24-free-tools-for-data-encryption/
http://www.techsupportalert.com/best-free-encryption-utility-for-cloud-storage
http://www.fiftyfiveandfive.com/office-365/cloud-storage-encryption/
http://lifehacker.com/the-best-cloud-storage-services-that-protect-your-priva-729639300

2.5 CHECK YOUR 6.

You also need to watch your back or "Check your 6" as they say in the military. When you connect a device or an app to Dropbox and other services, it keeps a record of connected devices that you can review and disconnect. You should check allowed or connected devices on a semi-regular basis to see if anyone is accessing your accounts from a device you do not recognize. If so you should disconnect any of these devices and immediately change your password.

In Dropbox for example, you should check your security tab to see what devices are linked to your account regularly

2.6 BACKUP YOUR DATA!

There is absolutely no reason you are not backing up your computer since you can do it for free using Windows System Image backup. Check out how to do this at: http://bit.ly/1o6SgoY

2.6.1 There are also free third party tools such as EasUS ToDo backup http://bit.ly/GM04bm , Clonezilla http://clonezilla.org/, and Comodo Backup http://backup.comodo.com/backup-features.php for WIndows PCs and Super Duper

2.6.2 For more information on backing up check out "The absurdly simple guide to backing up your PC" at http://bit.ly/1o6SQTH

2.6.3 Mac OS X users can also use Time Machine which is part of OS X http://abt.cm/1oQy117 for backing up your Mac.

2.6.4 There are also free third party tools such as SuperDuper! http://bit.ly/1oQxNXX , Carbon Copy Cloner http://bit.ly/1oQyzEk and CrashPlan http://bit.ly/1jjHyyK for your Mac as well.

2.6.5 There are also backup apps and services for your smart devices. For example, Apple allows you to backup your iPad to iCloud.

3 SHARING FILES WITH OTHERS SAFELY

With our reliance on email, electronic files and digital communications, lawyers and their staff find the need to collaborate on documents and share information with others continuing to grow. While sharing documents by email works with smaller files, limitations in your own email service as well as limitations on the recipients email service regarding attachments and size limitations on attachments often prevent sharing documents easily. Too often, we try to send a

file and receive an error message that it was able to be received or that have been rejected because the attachment exceeded the file size limit. Luckily, lawyers and their staff have many options today for online file storage and sharing that helps mitigate or eliminate these issues.

3.1.1 USING THE CLOUD TO STORE AND SHARE FILES.

Just like general society, the legal profession is becoming more and more mobile with the need to access documents on the go was necessary. The ability to share the information as stated above is also becoming more critical to the daily operation of a technologically oriented law office. The ability to review files and correspondence during client meetings, the ability to pull up a client file as needed or to share information in electronic format quickly and easily have all become a critical part of a modern legal practice. These services go beyond simply storing and sharing files will become an integral part of your workflow allowing you to improve quality of service as well as your efficiency and effectiveness in serving your clients.

Modern cloud-based technologies mean that lawyers no longer need to store all the information on an expensive on-site server (that needs to be replaced on a regular basis or that makes it difficult to access that information when they're out of the office). While there are any number of cloud-based storage and sharing services, they are not all created equal: some are easier to use but are less secure while others are more secure but not as user-friendly. As with any cloud-based or on premise technology, lawyers need to understand the locations of using this technology in their practice. This includes understanding the security features available and how best to use them to meet their obligations under the rules professional conduct and other regulations or laws pertaining to the safekeeping of personally identifiable or confidential information. Bottom line, just as with any other service lawyers must do their due diligence in selecting a cloud-based file storage and sharing service to ensure avoiding the risk of ethical violations and malpractice claims.

3.1.2 WHAT TO LOOK FOR IN CLOUD STORAGE AND FILE SHARING SERVICES.

There are a number of factors to consider when evaluating potential candidates for cloud storage and file sharing. From a lawyer's perspective, most critical should be security of the service and the documents stored in it. Too often, lawyers focus on services that are the easiest to use without considering what this means to the security implications of their information. Generally, there is a trade-off between ease-of-use and security: each lawyer must weigh the trade-offs that are presented between ease-of-use and security of the different services available. Here are some of things you need to consider when it comes to security for cloud-based storage and file sharing services:

- Is the data encrypted while on the services servers (commonly referred to as "data at rest") and is it encrypted while being transferred between their servers and your computer or anyone else's (commonly referred to as "data in transit")?

- Does this service use 256 bit encryption both for data at rest and data in transit?
- Does the service offer what is commonly known as “zero knowledge” security wherein you the user control the encryption key without which no one else can decrypt your data?
- Is your data encrypted before it leaves your device?
- If the company does not provide for zero knowledge security, are the encryption keys and your data stored on separate servers?
- Does the service provider have a policy in place regarding who has access to your data and when it may be accessed?
- Does the service provider provide you with the ability to remotely delete your information from any device attached to your account?
- When sharing files with others, can you add an additional level of protection through the use of a password without which they cannot access the file?
- In order to access the information you wish to securely share, does the service require the recipient to sign up for an account in order to access the information?
- Does the service provide for auditing of who accesses the service and your files?

3.1.3 While the ideal service would meet all of the above criteria, the reality is that we don't live in a perfect world and we often must weigh the potential risks and benefits in selecting a service. An example of this is widespread adoption use of Dropbox by lawyers and their staff.

3.1.4 Dropbox is one of the most popular document storage and sharing services because it is one of the easiest to use. Dropbox allows you to synchronize files across multiple devices and platforms and just plain works. The downside to Dropbox is that you have no control over the encryption key and your options for sharing files securely are limited. The encryption key used to encrypt your data is controlled by Dropbox which potentially means that their staff can decrypt your data pursuant to lawful authority or in the event an employee with access goes rogue. In all fairness to Dropbox, and other services that control the encryption key, it does allow the company to help you decrypt your files in the event you forget your account access password. Where you control the encryption key, if you forget that encryption key no one, including the company, can help you decrypt those files. Furthermore,, many in the legal technology world believe that the concerns over a provider controlling the encryption key is overblown: lawyers have entrusted their files to couriers and offsite storage providers for years, and this is much the same as we rely on others to protect our data.

3.1.5 In reality, I recommend that you not use Dropbox without additional encryption tools to store and share your confidential or privileged information; you do not want to appear in your local newspaper as the lawyer whose data was breached because you focused on a service that was the least expensive rather than the one that provided sufficient security to protect your information. Tools such as Sookasa (www.sookasa.com), Viivo (www.viivo.com), Boxcryptor (www.boxcryptor.com), CloudFogger (www.cloudfogger.com) and SafeMonk (www.safemonk.com) work with Dropbox as well as other less secure online storage and sharing services such as Google Drive and Microsoft OneDrive. These tools all offer varying levels of ease-of-use and security when sharing files and you should check and see if they provide sufficient controls that you are comfortable using them to communicate information with others. For example, with Sookasa, you can share a link with an outside user which expires after 15 minutes after they click the email.

3.1.6 Other services such as Citrix ShareFile (www.sharefile.com), SpiderOak (www.spideroak.com), , Hightail (www.hightail.com), and Egnyte (www.egnyte.com), to name just a few, provide higher levels of security for storage and for file sharing and may also include zero knowledge capabilities. For a comparison of a number of online file sharing and storage services, check out the 2015 Best Online File Sharing Services Review at (http://bit.ly/1KFspzD) and The Best Cloud Storage Services for 2015 at (http://bit.ly/1KFsDXj), for non-exclusive lists and reviews.

3.1.7 The reality is that as with any cloud service technology, lawyers must do their due diligence to ensure compliance with the applicable rules of professional conduct.

4 SOME THINGS DON'T BELONG IN THE CLOUD!

If you have information, images or other data that would cause you extreme embarrassment, loss of standing in the community, loss of business or even criminal prosecution if it you saw it on the front page of the local newspaper, it sure doesn't belong on the web without additional steps taken to secure it. And there is some information that just shouldn't be put on the web at all. You will not find KFC's Secret Recipe or the formula to Coca Cola stored in the web and for good reason – security is always an issue on the web even if you have taken steps to protect the information. And let's face it, embarrassing or nude photos of you and others shouldn't be on your iPhone, tablet or put up in the cloud unless you are willing to have them distributed to thousands of strangers if they are leaked, hacked or even inadvertently posted to a public area on the web by you.

5 FIREWALLS

Firewalls are not an option but a requirement, whether you are running a single computer or a network. Firewalls monitor and protect your network from Internet traffic. Generally, firewalls can be divided between those that are software-based and those that are hardware-based.

5.1 SOFTWARE BASED FIREWALLS

Windows includes a basic firewall which monitors incoming traffic to your net. While this is better than not using firewall at all, it is limited as only monitors inbound traffic and a traffic it might originate inside your network. This is important in the event that you are infected, and outbound firewall can protect infection from spreading to others and also alert you to the issue itself.

5.1.1 There are number of free, third party firewalls available from, Comodo http://bit.ly/1OHg5Vo, PrivateFirewall http://bit.ly/1OHggQp and ZoneAlarm http://bit.ly/1OHgo2c to name just a few. Unlike the Windows built-in firewall, these third party firewalls provide both inbound and outbound protection and have a stronger feature set. For good explanation of the features of free software firewalls, check out gizmo's freeware website article Best Free Firewall Protection at http://bit.ly/1OHgwyS and techradar's The Best Free Firewall Software of 2015: Stop malware before it gets you at http://bit.ly/1Ktsrdo .

5.1.2 For commercial software based firewalls, checkout TopTenReviews PERSONAL FIREWALL SOFTWARE REVIEW at http://bit.ly/1Ktsyps .

5.2 Hardware Based Firewalls

Hardware firewalls traditionally have been a stand-alone product in the office environment, many home routers today include the hardware-based firewall. Hardware firewalls are sometimes referred to as "gateway devices". That is because they serve as the gateway to your computers and network from the outside Internet.

5.2.1 Home Routers with Firewalls

These devices usually use a combination of NAT (Network Address Translation http://bit.ly/1KtthHb) which take short public Internet addressing creates private addresses for your internal network from with one or both of SPI (Stateful Packet Inspection http://bit.ly/1Kttdad) or SPF (Static Packet Filtering http://bit.ly/1Kttjif) which examines bits of the packets of information that traverse between the Internet and your network. Examples of these types of multipurpose devices include D-link Wireless N300 Soho VPN Router http://amzn.to/1Kttvy1, TP-LINK TL-ER604W SafeStream Wireless N300 Gigabit Broadband VPN Router http://amzn.to/1KttytM and NETGEAR Nighthawk AC1900 Dual Band Wi-Fi Gigabit Router http://amzn.to/1KttJFs .

5.2.2 Standalone firewalls

There are number of standalone firewall products suitable for a size office. Some of these products will even run on hardware that you provide is basically an older computer that can be repurposed for this task. Untangle NG Firewall (http://bit.ly/1KttY3h) is a software-based gateway federal product that can be installed on your own hardware or purchase compliance directly from Untangle. The free version gives you basic content filtering up a version gives you UTM (Unified Threat Management) capabilities. UTM combines firewall, anti-malware, antivirus and other security features and a unified package. pfSense is a free and open source software that is designed to be used as a firewall and router. You can use it on your own hardware you can buy it in appliance from pfSense (https://www.pfsense.org/).

5.2.3 For those that wish to purchase commercial products that are fully integrated, in addition to the offerings of Untangle and pfSense above, other popular and respected commercial hardware firewalls but also have UTM capabilities include, but are not limited to:

SonicWALL: http://www.sonicwall.com/us/en/
Fortinet: http://www.fortinet.com/
Calyptix: http://www.calyptix.com/
Barracuda: https://www.barracuda.com/
Zyxel: http://bit.ly/1KtuwWL

6 ANTI-VIRUS AND ANTI-MALWARE

You need to be running into virus software and all your devices (yes, this even includes Mac's) as well as anti-malware software. You also need to keep the definitions up-to-date which the software should do automatically and you need to run the latest version. Depending on your Internet service provider, you may arty have several licenses available to you of various comprehensive security suites such as Norton Security Suite or another. Otherwise consider using products from companies such as BitDefender, Avira, WebRoot and others. Check out PC mag.com The Best Security Suites for 2015 at http://bit.ly/1KtuK05 and Tom's Guide Best Antivirus Software and Apps 2015 at http://bit.ly/1KtuMF6 for trusted reviews of these Internet security suites.

7 CLOSING

Data and Cloud security need to become second nature to you at all times. You need to put this first and foremost in your mind as you use the cloud and digital devices in both your personal and business daily life. For a good overview of the steps you can take to protect your digital assets, Read lifehacker's "The Start-to-Finish Guide to Securing Your Cloud Storage" at http://bit.ly/1uGouNj

Security in your Practice: Mobile Devices, Firewalls, Using the Cloud

Profile: Nerino J. Petro, Jr.

Attorney Nerino Petro is the Chief Information Officer for Holmstrom KennedyPC, in Rockford, Illinois where he is responsible for all in-house technology and training as well as new technologies and providing direct support to the firm's team members and attorneys in the office and at trial. HolmstromKennedy is a century-old, 18-lawyer firm providing innovative solutions to complex issues throughout Northern Illinois, with offices in Rockford and Byron.

Nerino served as the first Practice Management Advisor for the State Bar of Wisconsin's Practice411™ Law Office Management Assistance Program from 2006-2014. Nerino assisted the more than 24,000 Wisconsin Bar members operate their offices more effectively and efficiently. Licensed in Illinois and Wisconsin, Nerino uses his 20+ years of legal practice experience and experience being CEO/Senior Legal Technologist for CenCom Legal Technologies (which he founded in 1994), to help lawyers and their staff deal with the technology and practice management issues confronting them.

He is a Certified Independent Consultant for TimeMatters® practice management software, Billing Matters® time and billing software, as well as Clio cloud based practice management and has provided consulting, installation, customization and training for clients throughout the country. He is a NetDocuments Certified Partner and has worked with other leading products including TABS® time, billing and accounting software, Practice Master® practice management software, Lucion FileCenter, Quikscribe Digital Dictation, Dragon NaturallySpeaking and TValue financial software as well as Fujitsu and Canon Scanners.

Nerino was the ABA LPM Magazine Product Watch columnist (2006 -2012) and is a regular contributor to other local, state and national publications including the Illinois Bar Journal, Wisconsin Lawyer, Wisconsin InsideTrack and ABA GP|Solo Magazine. Nerino serves on the ABA GP, Solo and Small Firm Division GP|Solo Magazine Board as its Technology Editor. He has presented throughout the US and abroad including the ABA TECHSHOW, Pacific Legal Technology Conference, Missouri, Illinois, Oklahoma, Indiana, South Carolina and Wisconsin Solo and Small Firm Conferences, ABA GP|Solo National Solo & Small Firm Conference, US Virgin Islands Bar Association, National Association of Bar Executives meetings as well as other ABA, State and local conferences and events in the US and Canada. He served on the ABA TECHSHOW Planning Board from 2012-2014 and is a member of the State Bar of Wisconsin and ISBA Solo & Small Firm Conference Planning Committees. Nerino was named to the inaugural Fastcase 50 list of the top legal techies in 2011. He provides information on legal technology, practice management and items of interest to lawyers on his blog at www.compujurist.com .Nerino continues to provide technology consulting, training and practice management services to lawyers and firms throughout the United States through CenCom Technologies.

Nerino J. Petro, Jr.
CIO/Attorney
Holmstrom & Kennedy, P.C.
800 N. Church Street
PO Box 589
Rockford, IL 61105
TEL: 815.962.7071 C: 815.669.0075
FAX: 815.962.7181
EMAIL: npetro@holmstromlaw.com nerinopetro@cencomtech.com
WEB: www.holmstromlaw.com
LinkedIn: **http://tinyurl.com/linkedin-npetro**
Twitter: @nerinopetro

HolmstromKennedyPC attorneys at law

complex issues. innovative solutions

fastcase 50 Award Winner 2011