1-1-2022

Ethics_ Security is Only as Good as the Weakest Link - Legal Tech Security Measures Every Lawyer Must Take

Indiana Continuing Legal Education Forum (ICLEF)

Ethics: Security is Only as Good as the Weakest Link - Legal Tech Security
August 2, 2022
Index

Index

Index

Ethics: Security is Only as Good as the Weakest Link - Legal Tech Security
August 2, 2022
Index

ICLEF Electronic Publications

Feature Release 4.1
August 2020

To get the most out of your *ICLEF Electronic Publication,* download this material to your PC and use Adobe Acrobat® to open the document. The most current version of the Adobe® software may be found and installed by clicking on one of the following links for either the free Adobe Acrobat Reader® or the full retail version of Adobe Acrobat®.

Feature list:

1. **Searchable** – All ICLEF Electronic Publications are word searchable. To begin your search, click on the "spyglass" icon at the top of the page while using the Adobe® software.
1. **Bookmarks** – Once the publication is opened using the Adobe Acrobat® software a list of bookmarks will be found in a column located on the left side of the page. Click on a bookmark to advance to that place in the document.
2. **Hypertext Links** – All of the hypertext links provided by our authors are active in the document. Simply click on them to navigate to the information.
3. **Book Index** – We are adding an INDEX at the beginning of each of our publications. The INDEX provides "jump links" to the portion of the publication you wish to review. Simply left click on a topic / listing within the INDEX page(s) to go to that topic within the materials. To return to the INDEX page either select the "INDEX" bookmark from the top left column or right-click with the mouse within the publication and select the words "*Previous View*" to return to the spot within the INDEX page where you began your search.

Please feel free to contact ICLEF with additional suggestions on ways we may further improve our electronic publications. Thank you.

Indiana Continuing Legal Education Forum (ICLEF)
230 East Ohio Street, Suite 300
Indianapolis, Indiana 46204
Ph: 317-637-9102 // Fax: 317-633-8780 // email: iclef@iclef.org
URL: https://iclef.org

ETHICS – SECURITY IS ONLY AS GOOD AS THE WEAKEST LINK – LEGAL TECH SECURITY MEASURES EVERY LAWYER MUST TAKE

August 2, 2022

WWW.ICLEF.ORG

DISCLAIMER

The information and procedures set forth in this practice manual are subject to constant change and therefore should serve only as a foundation for further investigation and study of the current law and procedures related to the subject matter covered herein. Further, the forms contained within this manual are samples only and were designed for use in a particular situation involving parties which had certain needs which these documents met. All information, procedures and forms contained herein should be very carefully reviewed and should serve only as a guide for use in specific situations.

The Indiana Continuing Legal Education Forum and contributing authors hereby disclaim any and all responsibility or liability, which may be asserted or claimed arising from or claimed to have arisen from reliance upon the procedures and information or utilization of the forms set forth in this manual, by the attorney or non-attorney.

Attendance of ICLEF presentations does not qualify a registrant as an expert or specialist in any discipline of the practice of law. The ICLEF logo is a registered trademark and use of the trademark without ICLEF's express written permission is prohibited. ICLEF does not certify its registrants as specialists or expert practitioners of law. ICLEF is an equal opportunity provider of continuing legal education that does not discriminate on the basis of gender, race, age, creed, handicap, color or national origin. ICLEF reserves the right to refuse to admit any person or to eject any person, whose conduct is perceived to be physically or emotionally threatening, disruptive or disrespectful of ICLEF registrants, faculty or staff.

INDIANA CONTINUING LEGAL EDUCATION FORUM

OFFICERS

LYNNETTE GRAY
President

HON. ANDREW R. BLOCH
Vice President

SARAH L. BLAKE
Secretary

HON. THOMAS A. MASSEY
Treasurer

ALAN M. HUX
Appointed Member

LINDA K. MEIER
Appointed Member

DIRECTORS

James H. Austen
Sarah L. Blake
Hon. Andrew R. Bloch
Melanie M. Dunajeski
Lynnette Gray
Alan M. Hux
Dr. Michael J. Jenuwine
Shaunda Lynch
Hon. Thomas A. Massey
Linda K. Meier
Richard S. Pitts
Teresa L. Todd

ICLEF

SCOTT E. KING
Executive Director

James R. Whitesell
Senior Program Director

Jeffrey A. Lawson
Program Director

ETHICS – SECURITY IS ONLY AS GOOD AS THE WEAKEST LINK – LEGAL TECH SECURITY MEASURES EVERY LAWYER MUST TAKE

Description

Rule 1.6 stipulates that a lawyer must make reasonable efforts to prevent the disclosure of confidential client information. The comments to Rule 1.6 require lawyers to act competently to safeguard client information and use reasonable safety precautions when transmitting a client communication. The exact meanings of "reasonable efforts," "act competently" and "reasonable precautions" may be subject to debate. However, doing nothing certainly won't meet the standard. The good news is that 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 to make sure your confidential information remains confidential.

Faculty

Mr. Barron K. Henley, Esq.
Affinity Consulting Group, LLC
1550 Old Henderson Road, Suite S-150
Columbus, OH 43220
ph: (614) 602-5561
e-mail: bhenley@affinityconsulting.com

August 2, 2022

Barron K. Henley, Esq., Affinity Consulting Group, LLC, Columbus OH

Barron K. Henley, Esq. is one of the founding partners of *Affinity Consulting Group*, a legal technology consulting firm focused on automating and streamlining law firms and legal departments. He earned his B.S./B.A. (marketing and economics) and J.D. from The Ohio State University and is a member of the American, Ohio and Columbus Bar Associations, and the Worthington Estate Planning Council. He is a Fellow of the College of Law Practice Management, a Fellow of the American Bar Foundation, a member of Ohio Supreme Court Commission on Technology and the Courts, and a member of both the ABA Law Practice Management and the Real Property Trust and Estate Law ("RPTE") Sections. He's also a former member of RPTE Futures Task Force, a former Board Member for the ABA TECHSHOW, and the former Chair of the Ohio State Bar Association Law Office Automation & Technology Committee. Mr. Henley heads Affinity's document assembly/automation and software training departments. Barron is also an expert in launching new law firms, overhauling existing firms, and documenting and re-engineering law firm processes. Finally, Barron teaches continuing legal education (CLE) classes throughout the U.S. and Canada covering a wide variety of topics related to law practice management, technology, and ethics.

Cyber Security - 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, MN 43220
614.340.3444
www.affinityconsulting.com

Cyber Security - Digital Security Measures Every Lawyer Must Take
Table of Contents

Digital Security Measures Every Lawyer Must Take

I. **INTRODUCTION**: In 2012, the American Bar Association promulgated amendments to the Model Rules of Professional Conduct which dealt with technology and data security. 39 states have adopted those changes (for a full list, see http://bit.ly/2HJEoFH). 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]

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

Here's some frightening facts about business disasters which really underscore 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 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]
>
> "According to a report from the Federal Emergency Management Agency (FEMA), 40% of businesses do not reopen following a disaster. On top of that, another 25% fail within one year.[3]"

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**. The following quotes from experts underscore the accelerating threat these things pose, particularly in light of the fact that many are working from home where presumably, internet defenses are weaker than they would be at the office.

   > "Home networks are three to five times more likely than the law firm network to contract some form of malware. The cybercriminals know that, too, and are specifically targeting users in a work-from-home environment."[4]
   >
   > "[T]he total number of global ransomware reports increased by 715.08 percent YoY, potentially suggesting that threat actors

[2] Disaster Planning, by The U.S. Small Business Administration, see https://bit.ly/37QJcGh

[3] Study: 40% Of Businesses Fail To Reopen After A Disaster by Access Corp - see https://bit.ly/3oD3toH and https://bit.ly/3dNltqn

[4] Lawyer Tech Tips: Technology FAQs for the New Normal by Joan Feldman for AttorneyAtWork, August 7, 2020 - see https://bit.ly/2HJO31m

upped their ransomware campaigns to capitalize on both the pandemic and the work-from home context and the commoditization of ransomware-as-a-service."[5]

6. **Synchronization issues**. This relates to services like Dropbox, Box and others which synchronize files across multiple devices. If the sync fails, files can be lost.

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."[6]

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

> "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."[7]

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.

---

[5] Bitdefender Mid-Year Threat Landscape Report 2020 - https://bit.ly/3nBqCav

[6] 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.

[7] 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.

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.

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.

A. **IN 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. **IN Rule 1.1 Comment 6**:

[6] 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 the technology relevant to the lawyer's practice***, engage in continuing study and education and comply with all continuing legal education requirements to which the lawyer is subject.

C. IN RULE 1.6 - Confidentiality of Information:

(a) A lawyer shall not reveal information relating to 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).

…

D. 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.

E. IN RULE 1.6 Comment 16 - Acting to Preserve Confidentiality:

[16] 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.

F. ABA Rule 1.6 Comment 18 - Acting Competently to Preserve Confidentiality:

[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.

G. IN Rule 1.6 Comment 17:

[17] When ***transmitting a communication*** that includes information relating to the representation 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*** or may give informed consent to the use of a means of communication that would otherwise be prohibited by this Rule.

H. IN RULE 5.1 - Responsibilities of a Partner or Supervisory Lawyer:

(a) A partner in a law firm, 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 all lawyers in the firm conform to the Rules of Professional Conduct.

(b) *A lawyer having direct supervisory authority over another lawyer 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 having direct supervisory authority over the other lawyer knows of the conduct at a time when its consequences can be avoided or mitigated but fails to take reasonable remedial action**.

I. IN 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 person's conduct is compatible with the professional obligations of the lawyer;**

(b) **a lawyer having direct supervisory authority over the nonlawyer 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.**

J. **ABA Formal Opinion 477[8] - Securing Communication of Protected Client Information**: This opinion is an update of Formal Opinion 99-413[9] (which addressed a lawyer's obligations for protecting confidentiality when using email) to address the technology and ethics rules changes which have occurred since that time. Key points from the opinion include:

1. **Observations About How The Practice Has Changed Since 1999**: The committee notes that unlike 1999, lawyers today primarily use electronic methods of communication. Each device and storage location for those communications represents the possibility of unauthorized disclosure or access. Further, the ABA adopted technology amendments to the Model Rules in 2012 which affected Rule 1.1 (Competence) and 1.6 (Confidentiality).

   "At the same time, the term 'cybersecurity' has come into existence to encompass the broad range of issues relating to preserving individual privacy from intrusion by nefarious actors throughout the Internet.

[8] See http://bit.ly/2HNSWEb, May 4, 2017.
[9] See http://bit.ly/2HRyB11, May 5, 1999.

Cybersecurity recognizes a post-Opinion 99-413 world where law enforcement discusses hacking and data loss in terms of 'when,' and not 'if.'"[10] The opinion goes on to describe why law firms are particular targets for hackers and other cyber criminals.

2. **Reasonable Efforts Standard**: The committee concluded that the reasonable efforts standard "rejects requirements for specific security measures (such as firewalls, passwords, and the like) and instead adopts a fact-specific approach to business security obligations that requires a "process" to assess risks, identify and implement appropriate security measures responsive to those risks, verify that they are effectively implemented, and ensure that they are continually updated in response to new developments."[11]

3. **Reasonable Efforts Factors**: When conducting a fact-based analysis as to what level of security should be employed, practitioners should consider the following (pulling directly from Rule 1.6 Comment 18):

    a. The sensitivity of the information,

    b. The likelihood of disclosure if additional safeguards are not employed,

    c. The cost of employing additional safeguards,

    d. The difficulty of implementing the safeguards, and

    e. 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)

4. **Other Findings**:

    a. "**A fact-based analysis means that particularly strong protective measures, like encryption, are warranted in some circumstances.** Model Rule 1.4 may require a lawyer to discuss security safeguards with clients. **Under certain circumstances, the lawyer may need to obtain informed consent from the client regarding whether to the use enhanced security measures**, the costs involved, and the impact of those costs on the expense of the representation where nonstandard and not easily available or affordable security methods may be required or requested by the client. **Reasonable efforts, as it pertains to certain highly sensitive information,**

[10] ABA Formal Opinion 477, lines 34 - 37.
[11] ABA Formal Opinion 477, lines 99 - 104.

might require avoiding the use of electronic methods or any technology to communicate with the client altogether, just as it warranted avoiding the use of the telephone, fax and mail in Formal Opinion 99-413."[12]

b. "[T]he use of unencrypted routine email generally remains an acceptable method of lawyer-client communication. However, cyber-threats and the proliferation of electronic communications devices have changed the landscape and it is not always reasonable to rely on the use of unencrypted email."[13]

5. **Guidance Regarding Reasonable Steps**: The committee recommends the following considerations:

   a. Understand the nature of the threat.

   b. Understand how client confidential information is transmitted and where it is stored.

   c. Understand and use reasonable electronic security measures.

   d. Determine how electronic communications about client matters should be protected.

   e. Label client confidential information.

   f. Train lawyers and non lawyer assistants in technology and information security.

   g. Conduct due diligence on vendors providing communication technology.

6. **Conclusion**: "A lawyer generally may transmit information relating to the representation of a client over the Internet without violating the Model Rules of Professional Conduct where the lawyer has undertaken reasonable efforts to prevent inadvertent or unauthorized access to information relating to the representation. However, a lawyer may be required to take special security precautions to protect against the inadvertent or unauthorized disclosure of client information when required by an agreement with the client or by law, or when the nature of the information requires a higher degree of security."[14]

[12] ABA Formal Opinion 477, lines 116 - 124.
[13] ABA Formal Opinion 477, lines 135 - 139.
[14] ABA Formal Opinion 477, lines 333 - 339.

V. **INDIANA BREACH DISCLOSURE LAW**: Ind. Code § 4-1-11 et seq.; § 24-4.9-1 et seq.

IC 24-4.9-2-2 "Breach of the security of data"

Sec. 2. (a) "Breach of the security of data" means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by a person. The term includes the unauthorized acquisition of computerized data that have been transferred to another medium, including paper, microfilm, or a similar medium, even if the transferred data are no longer in a computerized format.

(b) **The term does not include the following:**

(1) Good faith acquisition of personal information by an employee or agent of the person for lawful purposes of the person, if the personal information is not used or subject to further unauthorized disclosure.

(2) **Unauthorized acquisition of a portable electronic device on which personal information is stored, if all personal information on the device is protected by encryption and the encryption key:**

(A) **has not been compromised or disclosed; and**

(B) **is not in the possession of or known to the person who, without authorization, acquired or has access to the portable electronic device**.

VI. **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."[15]

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 now a standard security measure for protecting laptops and portable devices—and attorneys should be using it."[16]

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. **AlertBoot** - http://www.alertboot.com/

   b. **BitLocker** - included for free with Windows 8, 8.1, 10 & 11 Professional.

   c. **Broadcom Full Disk Encryption** - https://bit.ly/3IpGfmd

   d. **ESET Protect** - https://bit.ly/3IcsGAg

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

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

   g. **Micro Focus Full Disk Encryption** - https://bit.ly/3pjfLE0

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

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

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

i. **Trend Micro Endpoint Encryption** - https://bit.ly/3lpJ9qQ

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 Rule 1.6, Comment 19**: Let's look at that again.

> "When transmitting a communication that includes information relating to the representation of a client, the lawyer must take 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."[17]

> "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

[17] 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.

should be encrypted or sent through collaboration tools that send encrypted links rather than plain text data."[18]

"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."[19]

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.

   a. **Office 365 Message Encryption**: http://bit.ly/2L8zW2I

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

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

   d. **Trustifi**: https://trustifi.com/

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

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

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

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

   i. **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

[18] ibid., quoting Marco Maggio.
[19] ibid., quoting Steve Santorelli.

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."[20]

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

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 protection to the public."[21] Here are some options for this. Private Internet Access is the one I use personally.

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

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

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

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

v. **ExpressVPN**: https://www.expressvpn.com

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

vii. **StrongVPN**: https://strongvpn.com

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

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

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

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

[21] The Best VPN Services for 2016, by Max Eddy, Fahmida Rashid, 3/9/2016, PCMag - see http://tinyurl.com/njuv7br.

xii. **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.[22]

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![23] or HackerWatch[24]. 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.[25]

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

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):

[22] See http://www.webopedia.com/TERM/F/firewall.html
[23] See https://www.grc.com/x/ne.dll?bh0bkyd2
[24] See http://www.hackerwatch.org/probe/
[25] See http://searchsoftwarequality.techtarget.com/definition/penetration-testing

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

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

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

d. **1Password** - https://1password.com/

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

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

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

h. **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.

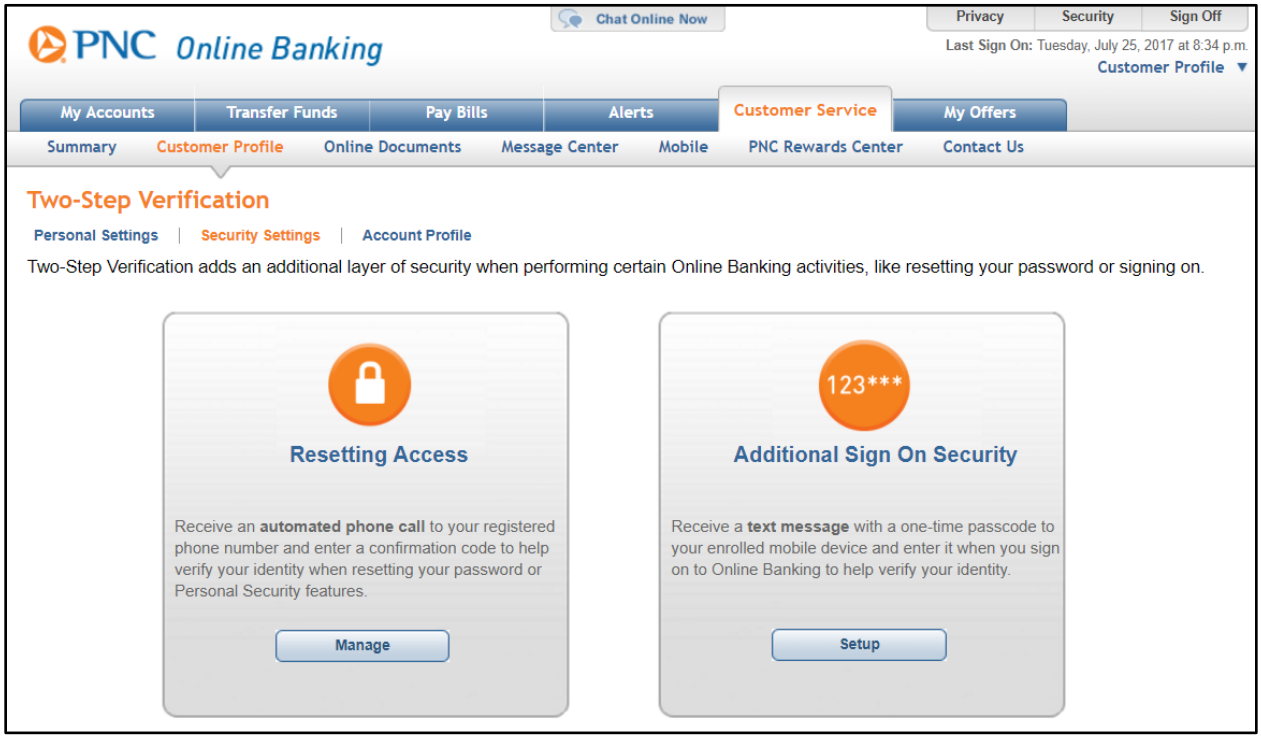
The ways in which someone can be authenticated usually fall into three categories known as the factors of authentication, which include:

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.

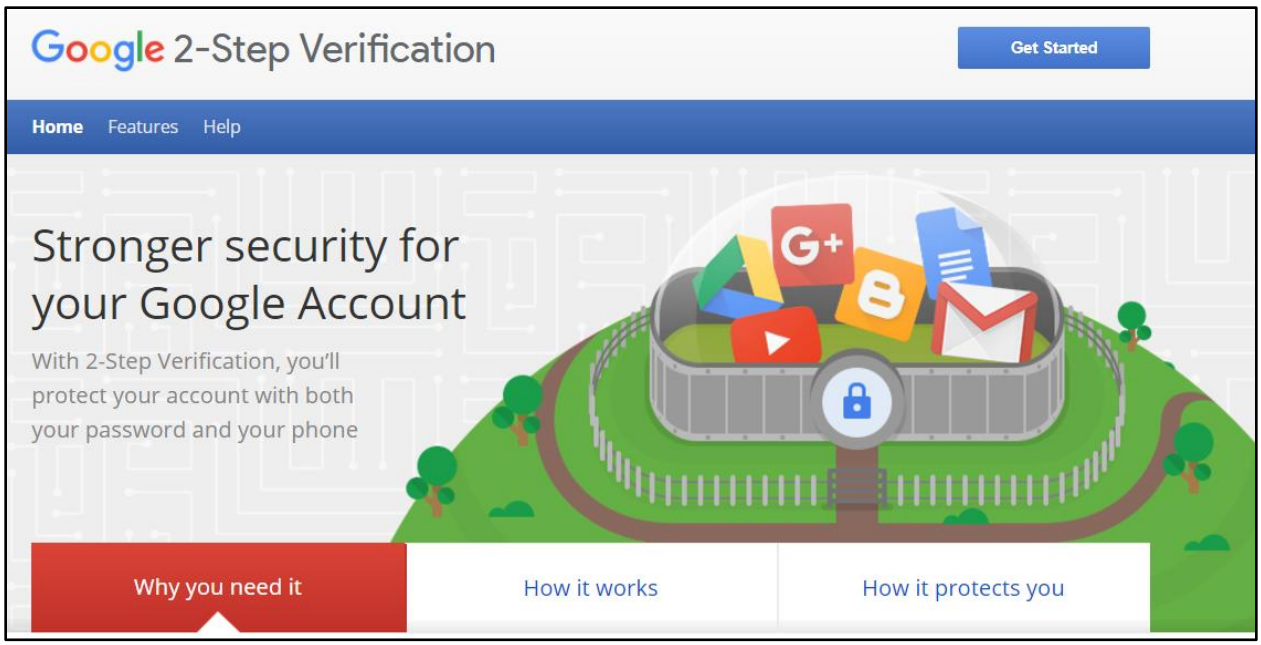
3. **Inherence factors, more commonly called biometrics** -- something the user is. These may be personal attributes mapped from physical characteristics, such as fingerprints, face and voice. It also includes behavioral biometrics, such as keystroke dynamics, gait or speech patterns."[26]

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:

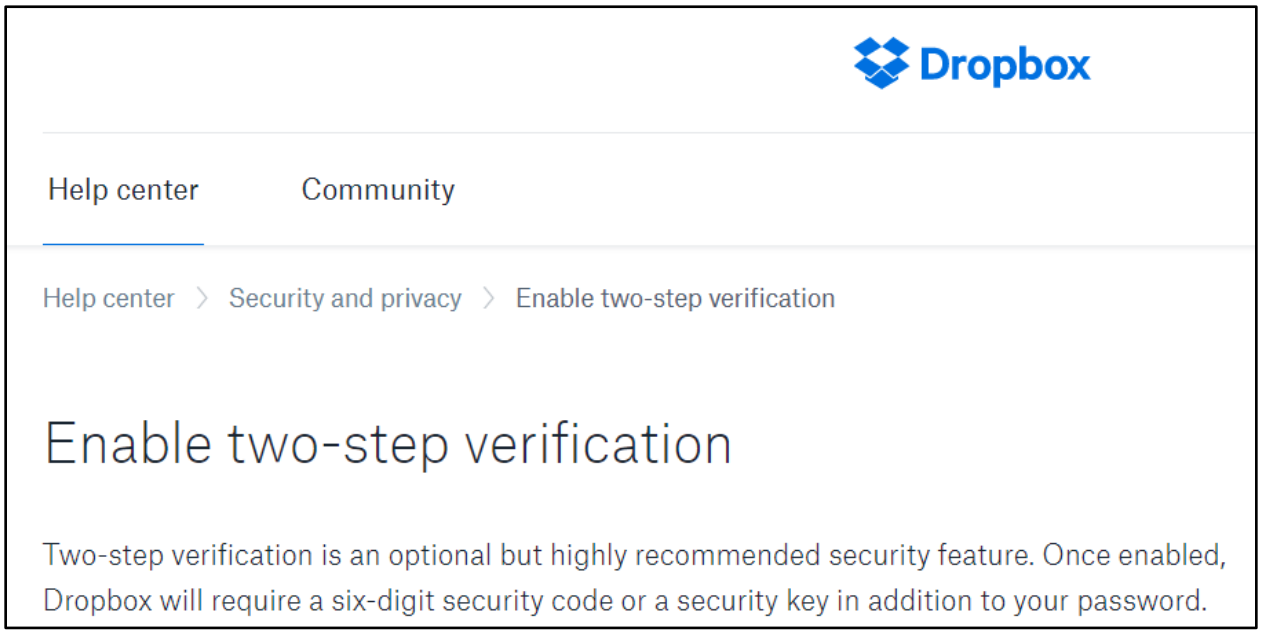


Your email account probably offers it:

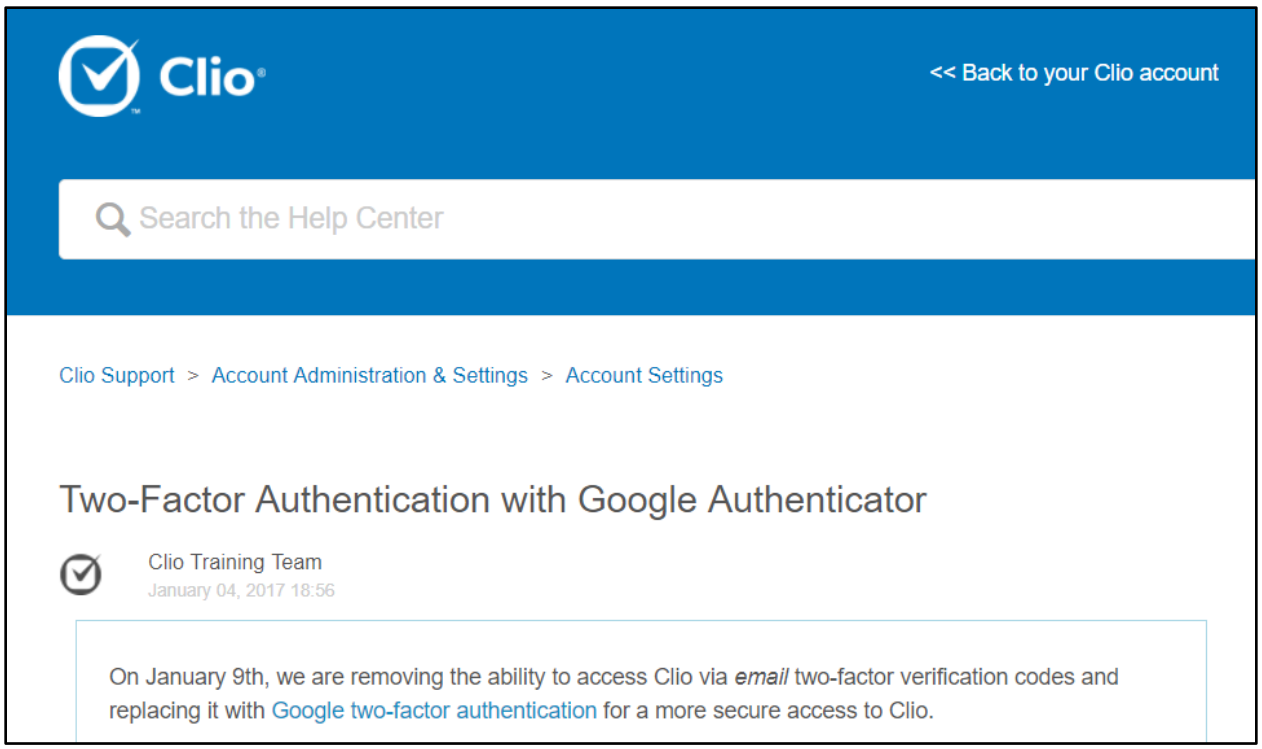
[26] See http://searchsecurity.techtarget.com/definition/two-factor-authentication



Your file sharing service probably offers it:

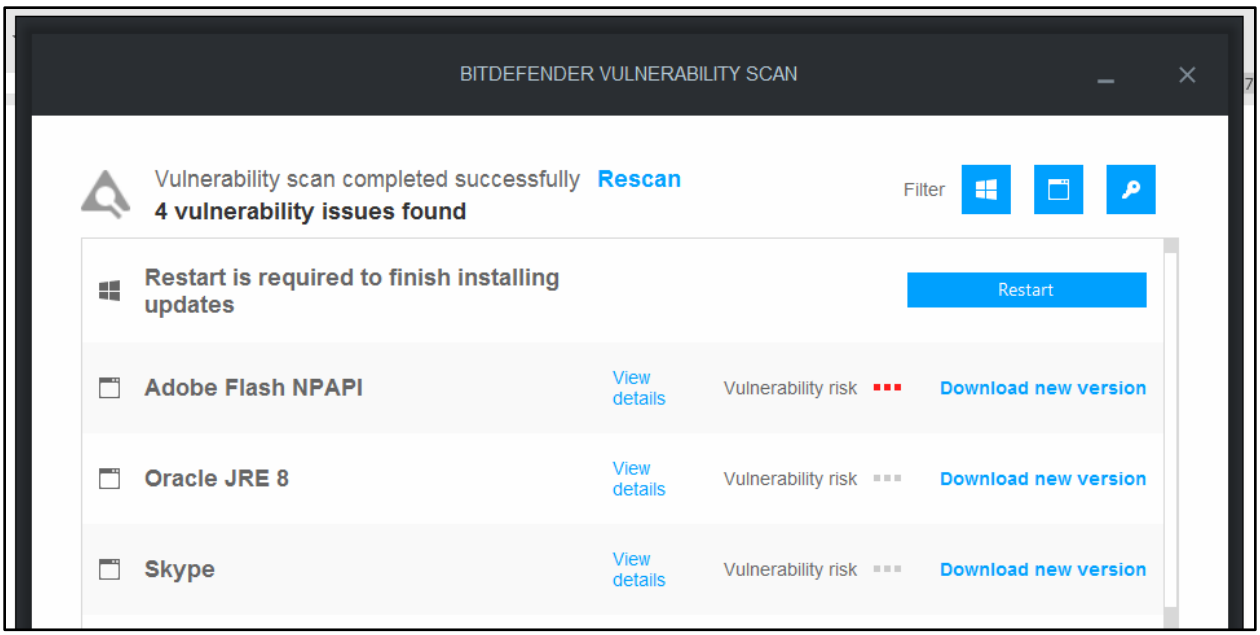


Your case management system probably offers it:



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 Norton[27] which I *really* like. Of course, there are many good options available from McAfee, Webroot, Bitdefender, 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:

[27] See https://us.norton.com/antivirus



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/

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

2. **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[28].

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

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.

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

- 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.[29]

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 must proceed expeditiously to preserve the relevant electronically stored information."[30] 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.

VII. OTHER COMPONENTS OF A DISASTER AVOIDANCE STRATEGY:

A. **Paper Reduction**: Electronic files can easily be backed up, copied, duplicated, and held in many locations for safety. The less paper your office has to manage, the better. If you need advice on how to reduce paper without causing paper-dependent people to become uncomfortable (or angry), we can help.

---

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

[30] 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.

B. **Go Cloud**: If you choose a secure vendor who understands and is willing to abide by the Rules of Professional Conduct (as arguably required by Rule 5.3), then having your critical information accessible from any device with internet access (plus your logon and password, of course) should provide quite a measure of comfort. If a law office stores all electronic data is on a server in the office, it's not uncommon for crashes to occur. Even if you have a good backup system, it may take multiple days and a lot of money to get everything back online. In our experience, law offices that rely on reputable cloud vendors simply don't experience that kind of thing.

C. **Mobile Communications**: Hosted VoIP[31] phone systems mean that the only thing you need in order to use your phone system is a desk phone or wireless headset connected to your computer. In our office, almost everyone has a wireless headset and a laptop. As such, my office phone works anywhere my laptop has an Internet connection. If my office burned to the ground, my phone system would be unaffected because it's not on-site.

D. **Mobile Hardware**: If you rely on (encrypted) laptops for all employees, then your office can be where ever you are. Not only do I have the convenience of working from where ever I want, if a disaster befell my physical office, it wouldn't shut us down. Of course, you can also buy portable printers/multifunction machines, scanners, and backup devices.

E. **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

[31] VoIP stands for Voice Over Internet Protocol.

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

F. 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.

G. **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.

H. **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.

I. **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.

J. **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.

K. **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.

L. **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.

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

N. **Consider Cyber Insurance**: Some experts argue that for today's law office, this is essential insurance.

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
Web: www.affinityconsulting.com