Legal Ethics and Technology

By Jim Calloway
Director, Oklahoma Bar Association Management Assistance Program
Blogger, Jim Calloway's Law Practice Tips
http://www.lawpracticetipsblog.com
Digital Edge: Lawyers and Technology podcast
http://legaltalknetwork.com/podcasts/digital-edge/
Twitter @JimCalloway https://twitter.com/jimcalloway

Every Law Firm is a Technology Business

With all of the changes in business practices and society today no one can deny every law firm, and most every business today, is a technology business.

Your attention is directed to the September/October 2016 issue of Law Practice Magazine and my column "Every Law Firm Is a Technology Business."[1]. The concluding paragraph of this Practice Management Advice column states:

> A general counsel addressing a group of lawyers stated that she still saw a lot of Flintstones versus Jetsons when addressing technology in firms she has dealt with. Be a Jetson.

The "Duty" of Technology Competence

By order dated September 19, 2016 the Oklahoma Supreme Court amended the Oklahoma Rules of Professional Conduct to incorporate several changes, many relating to technology. These changes incorporated modifications made in 2012 to the ABA's Model Rules of Professional Conduct. In Re Oklahoma Rules of Professional Conduct, 2016 OK 91.[2]

One of those changes incorporated what some commentators have referred to as the ethical duty of technology competence. According to Robert Ambrogi, who tracks adoption of these rule change at his Lawsites blog, Oklahoma was the twenty-fourth of thirty six states to adopt this rule change.[3] This language adopting the duty of technology competence is contained in Comment 6 to ORPC 1.1. The language added by amendment is underlined. The comment now states:

> Maintaining Competence.
>
> [6] To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, engage in continuing study and education and comply with all continuing legal education requirements to which the lawyer is subject, including the benefits and risks associated with relevant technology.

This rule change would be considered a necessary and obvious to some, considering how critical technology is to the operation of all sorts of businesses today. But it also could be concerning for other members of the bar who are not confident with their understanding of technology advances.

Law practices have become, at least in significant part, technology businesses. This happened without lawyer's approval or consent. You may take some consolation from the fact that this is what has happened to most businesses. We all have to understand the risks and benefits of relevant technology and that was true even before it was officially enshrined into our Oklahoma Rules of Professional Conduct.

Another rule change to the Oklahoma Rules of Professional Conduct is found in Rule1.6 (c) which states:

> 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.

So what does this mean for you?

It means whether you are a lawyer in private practice or a lawyer working for a tribe or government agency you have to be a competent technology user.

You have to protect confidential information when you are entrusted with it.

If you work from home either occasionally or on a regular basis, to protect your clients, you also have to be a competent technology user at home. You should also consider the need to protect yourself and teach your family to protect their digital privacy and their personal technology tools.

Unencrypted email is not secure

We have just emerged from a Presidential election that led to more members of the general public becoming aware that email can be hacked and disclosures of stolen emails can be embarrassing and have profound consequences. Technology professionals and those who follow tech news have been aware of this fact for some time.

In November 2014 hackers announced their successful intrusion into Sony Pictures and released personal information about its employees and their families, e-mails between employees, information about executive salaries at the company and copies of then-unreleased Sony films. Since the hackers demanded Sony pull release of its film *The Interview*, which was about North Korean leader Kim Jong-un, North Korea was blamed. Some Sony employees sued because their social security numbers and medical information were released. The Sony co-chairwoman stepped down.[4]

In March 2016 it was revealed that nearly 50 large law firms, including some of the nation's most prestigious, were the targets of hackers[5], although there is some dispute about how successful the hackers were in obtaining client information.

No lawyer or law firm would want to be hacked, whether the target was confidential client information or the lawyer's credit card numbers and other financial information.

So, let's all resolve to take some affirmative action to improve our personal and professional digital security. Part of this action will be analyzing the appropriateness of using email for confidential client communications.

The ABA has released Ethics Opinion 477R (May 22, 2017) on encryption of attorney-client email. Ethics Opinion 477 (May 11, 2017) on encryption of attorney-client email.[6]

Those who do not want any rule requiring email encryption will rejoice if they skip down to the opinion's conclusion and read:

> Conclusion
>
> Rule 1.1 requires a lawyer to provide competent representation to a client. Comment[8] to Rule 1.1 advises lawyers that to maintain the requisite knowledge and skill for competent representation, a lawyer should keep

> abreast of the benefits and risks associated with relevant technology. Rule 1.6(c) requires a lawyer to make “reasonable efforts” to prevent the inadvertent or unauthorized disclosure of or access to information relating to the representation.
>
> 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. 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.

They would be rejoicing prematurely at the absence of the words "email encryption required." The opinion notes that a hard and fast rule cannot be crafted to apply to all situations, and therefore:

- "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 ..."
- "In contrast, for matters of normal or low sensitivity, standard security methods with low to reasonable costs to implement, may be sufficient to meet the reasonable-efforts standard to protect client information from inadvertent and unauthorized disclosure."

My first reading is that this is along the line of my suggestion that a text to a client asking "Court starts in 5 minutes. Where are you?" is not a problem even if you are using unencrypted SMS texting because of the low sensitivity of the information, the relative security of texting and urgency overrule the extremely slight risk. See Email Attachments vs. Client Portals.

Among the things that lawyers should understand is how confidential client information is transmitted and stored. The opinion also suggests that every device and access point "should be evaluated for security compliance." The law firm must have appropriate policies and procedures. They must train staff and supervise them on reasonably secure methods of communications. [Resources such as *Locked Down: Practical Information Security for Lawyers* (Second Ed., 2016) provide sample security policies that can provide a starting place for those preparing a security policy. This title is available from the OBA MAP Lending Library.]

Only then can the lawyer make the decision that a particular electronic client communication need not be encrypted.

There is a lot to unpack in this opinion, but there is some language to quibble with:

"In the technological landscape of Opinion 99-413, and due to the reasonable expectations of privacy available to email communications at the time, unencrypted email posed no greater risk of interception or disclosure than other non-electronic forms of communication. This basic premise remains true today for routine communication with clients, presuming the lawyer has implemented basic and reasonably available methods of common electronic security

measures.14 Thus, the use of unencrypted routine email generally remains an acceptable method of lawyer-client communication."

To say that there is no greater risk of email interception and/or disclosure today than there was in 1999 is simply nonfactual.

But overall, this opinion sends a clear signal that law firms have to pay attention to security of email and other client communication. Most law firms have already determined that is the correct policy. I still suggest lawyers also read Texas Legal Ethics Opinion 648[7] in addition to this opinion.

If you want to share the above post with anyone, here's the link:
http://www.lawpracticetipsblog.com/2017/05/2017-aba-ethics-opinion-email-encryption.html

On the other hand, properly-vetted cloud computing storage is generally quite secure.

When cloud computing first gained attention, lawyers were appropriately skeptical. After all, they kept their client files locked safely within their office and the idea of storing client information with a third-party company seemed risky. However, we now appreciate that the risks of disclosure for our client's confidential information relates much more to the information stored digitally on our computers then on paper in file cabinets.

Keeping information on computers is a necessary part of law office operations. But if these computers are connected to the Internet, a practical necessity, then that information is at risk. A properly-vetted cloud computing service, particularly those that were designed for lawyers like the practice management cloud-based solutions will provide better security than an individual lawyer or small law firm without dedicated IT support can accomplish.

Over the years this concept has been adopted by most everyone in the information technology industry. They have engineers, security experts and 24 hour monitoring. Plus a secure cloud storage vendor also has huge motivation to maintain their customer secrets because a single breach that was well-publicized and very damaging could bring down the entire company.

Small firm lawyers (and all lawyers) now have the ability to digitally share information with their clients in a secured manner by using client portals.

Client Portals

As the article title implies, the Oklahoma Bar Journal September 2016 Law Practice Tips column "Email Attachments vs. Client Portals" discusses the security of communications via email and client portals.

This article addresses a very important topic so if you missed it the first time, now is a good time to read it. Spoiler alert: Secure client portals are a much better way to share confidential information with your client than unsecured, unencrypted email attachments.

See an informative summary of an ABA seminar that OBA MAP Director Jim Calloway and OBA PMA Darla Jackson presented titled: *Why Attorneys Are Flocking to Client Portals,* YOUR ABA (June 2017), https://www.americanbar.org/publications/youraba/2017/june-2017/client-portals-provide-gateway-to-efficiency--privacy-.html

As you can note from the summary (*and this is an important link contained in this paper*), we believe that client portals are critical for sharing information with clients including all of the documents involved in the matter. Because many cloud-based practice management systems for lawyers now include a portal as a part of the basic package of services, providing a client portal is much simpler than it would've been in days past.

Encryption is Your Friend

Just because people don't want to deal with email encryption doesn't mean the security benefits of encryption can be ignored.

Encryption is not a four-letter word and anyone concerned about confidentiality and privacy should understand how it works. Lawyers should know how to encrypt data on an "as needed" basis. I have previously noted the OBA member benefit Citrix ShareFile for email encryption and online file storage in the Oklahoma Bar Journal September 2016 Law Practice Tips column "Email Attachments vs. Client Portals."[8]

If you have a laptop computer, you should seriously consider encrypting the hard drive.

For reference I suggest reading "Encryption Made Easier: The Basics of Keeping Your Data Secure"[9] by Sharon D. Nelson, Esq. and John W. Simek; and another post that has been circulating online "How to encrypt your entire life in less than an hour"[10] by Quincy Larson of FreeCodeCamp. One note about some content in the Larson article is that the Tor browser is really for expert users. It can be also used as a gateway to those parts of the Internet you may have heard of but don't want to visit. I discourage lawyers without significant expertise to avoid experimentation with the Tor browser.

The Basics: A Password Manager and Two-factor Authentication

Almost all lawyers are aware that they need to use these tools, but many still resist due to the time it takes to set up these tools and the perceived inconvenience of using them.

Using the same password for all password-protected services you use means that when someone obtains your password to one of those sites, they will have access to all of them. Using words from the dictionary for a password means a brute force dictionary attack by hackers will crack your password.

Using long strings of letters and symbols and numbers means that passwords will be difficult to remember. Many sites now require the use of numbers and characters in a password. The current guidance is to keep passwords "simple, long and memorable. Phrases, lowercase letters

and typical English words work well . . . Experts no longer suggest special characters and a mix of lower and uppercase letters."[11]

But if you want to generate and securely store a longer password, it is time to start using a password manager. Password managers are extremely affordable and allow you to generate long passwords of 20 to 30 characters without resorting to words found in the dictionary. It is not an oxymoron to say that a password that is short and simple enough for you to remember is too short and simple to be secure. In the endnotes you will find links to reviews of some of the popular password managers. The basic version of LastPass[12] is now free; however, I suggest you pay the twenty-four dollars per year for the premium edition. Other popular password managers include 1Password[13], KeePass[14] and Dashlane[15]. Large firms may want enterprise solutions.

Using two-factor authentication for accounts that you consider important is a great way to protect against hackers. There is no doubt the two-factor authentication is a bit of an inconvenience. But you should always use it with your financial accounts and any services where you have a credit card number on file. And if it would be devastating to lose all of those photos that you have stored online, you might consider using it for that photo storage account as well.

At the simplest level using two-factor authentication means that when you log into a website a code number will be sent via text to your mobile device. You must enter that code to continue. So if some hacker manages to steal your password by whatever method, they can still not log in to access your information without also having access to your mobile phone. Note that when you set up this process individually at each website, it is very important to understand and preserve information about what to do if you lose your mobile phone.

Be Smart with your Use of Social Media

By now the horror stories of the trouble that people have gotten themselves into by indiscriminate posts on Facebook or other social media. But it still seems surprising to many of us how many lawyers find themselves in hot water over their use of social media.

In December 2018, the Louisiana Supreme Court has disbarred Sal Perricone, a former Assistant United States Attorney for the Eastern District of Louisiana for posting anonymous, online comments about cases being handled by his office from November 2007 through March 2012. http://www.legalethicsinmotion.com/2019/02/louisiana-supreme-court-disbars-attorney-for-anonymous-online-posts/.

In one case that involved the prosecution of police officers over the shooting of unarmed civilians in the aftermath of Hurricane Katrina, Perricone wrote: "NONE of these guys should have ever been given a badge." The officers were convicted but, the district court judge reversed the police convictions, in a 129 page opinion that cited "grotesque prosecutorial misconduct," referring in part to Perricone's comments.

In 2009 Illinois public defender Kristine Ann Peshek was fired for revealing client confidences by blogging about her cases and describing her clients in a way that made it possible to identify them. She referred to them by either their first names, some form of their first names, or by their jail identification numbers.

In other posts Peshek called one judge was clueless another an ---hole. She blogged that one client was "taking the rap for his drug-dealing dirtbag of an older brother" and said another was "stoned" for a court appearance. She was suspended as a lawyer for that and another ethics violation.[16]

A mistrial was granted in a murder trial after a Florida public defender posted a photo of leopard-print underwear that clients family had given him for trial to her Facebook page with mocking comments that the defendant's family believed the underwear was "proper attire for a trial." She was fired from her job as public defender.[17]

There are simply no legitimate reasons for blogging about an on-going matter. Even after a case is concluded the wisest course is to get signed permission from the client before posting or writing about the matter.

It should go without saying at this point that one cannot rely on privacy settings with social media sites - particularly with Facebook.

Practice safe computing when out of the office

Unprotected public Wi-Fi hotspots are by definition not secure. You should only use Wi-Fi services that require a password or other authentication. If you plan on logging in to your office from a remote location, it is best to set up a virtual private network (VPN) for you to login securely. Invest in a sufficient data plan for your phone or other mobile device through your carrier so that you are not tempted to login in to Wi-Fi hotspots.

Lawyers should be aware that many of the free VPNs do not deliver the privacy and security that they promise.[18]

Search for VPN reviews to make sure you are investing in a legitimate VPN. A google search like "best VPNs 2019" will yield sites like this one: https://www.pcmag.com/roundup/296955/the-best-vpn-services Just be sure to scroll past the sponsored links at the top of search results to a publisher you recognize.

Appropriate Backups of Critical Client Data is Likely an Ethical Responsibility

Backup any data that you are not willing to lose. Have a disaster response plan printed out on paper so if your network or computer has a major problem or an intrusion, you know who to call for help and what steps to take. If you are in possession of client data that is valuable and could adversely impact your representation of their matter if it is lost or destroyed, then you have an

ethical duty to back up that data in the same way you have an obligation to store a client's jewelry you are entrusted with a secure location rather than just tossing it in a desk drawer.

Training and Technology "Smarts"

It is important to understand that most digital intrusions occur via email. Constant training and communication of emerging threats is now important for any office that must have use of its computer systems.

Just prior to the 2016 Thanksgiving holiday, many Oklahoma Bar members received an email with a subject line of "Oklahoma Bar Association Complaint." Of course the email was a fake. Our General Counsel's office does not send out these types of official notices by email. But cyber criminals hope that the surprise and horror at reading a complaint has been filed will override judgment and generate a quick click on a link or attachment. If you receive an unexpected email that makes you want to instantly click on something, ALWAYS pause and think.

Every year our department places several phone calls or send emails (not replies) to lawyers asking "Did you just send an email?" Although our department is known as having technology skills, we are not embarrassed to make outreaches, so you shouldn't be either. We have received a number of emails with Zip file attachments relating to online shopping orders that we have not placed. The Zip file attachment is a warning all by itself and if you hover over a suspicious link in an email you will often be able to see a preview that the link is actually to a suspicious location.

For more information see the blog post "The Holidays Bring More Email Threats."[19]

Here's a hypothetical for you. You have been out of the office doing a series of depositions and had informed everyone in advance that interruptions could not happen during those two days. When you return, your assistant rushes up to you with a big smile and says "Don't worry. I got those funds wired out for that settlement before the deadline." You are puzzled and ask "what funds?" and your day rapidly goes downhill from there.

The short version of how this works is that criminals reserve a domain name that looks very similar to the victim's domain name. So, if their target used Smith law.com they might reserve Smiith law.com and few would notice the extra "i" in the emails they receive. It works even better if they have previously convinced the target to respond to an email so they can include the victim's actual signature block in their scam email.

The bottom line is wiring out money is often an irreversible action and you should have very clear procedures with checks and balances before a wire transfer is made. Your staff should be specifically instructed that if they receive an email from you directing them to wire out funds when you are temporarily unavailable, this should only be done after they are able to contact you by phone and hear your voice confirming the instructions.

Be cautious carrying your personal information or client information on USB flash drives

Flash drives are ubiquitous. Most people who work with computers use them. But they are also easy to lose. Carrying confidential client information on them raises issues.

If you lose a flash drive, there is a strong likelihood someone who finds it will insert it into a computer to see if it works. They then would have access to all of the files on it. Generally speaking you want to either encrypt the confidential files or the entire flash drive, which leads to a discussion on encryption. One easy method that is a bit more expensive but still affordable is to purchase an IronKey flash drive.[20]

Border Crossings

Crossing a border with confidential information on your electronic devices is an ethical challenge today. Please read Digital Privacy at the U.S. Border: Protecting the Data On Your Devices from the Electronic Frontier Foundation at http://bit.ly/2Ij2Iyz

Conclusion

Many lawyers resist learning about new technology. But today none of us can avoid learning basic technology competence and basic digital security practices. By taking some of the steps above you can provide safeguards so that you and those around you can be safer with your law firm and client digital information.

If you feel like you are behind in this area, don't be deterred from starting your study on technology competence. This paper should provide you many starting points. As the old saying goes: How do you eat an elephant? One bite at the time.

IMPORTANT NOTE: An additional paper "A Baker's Dozen: Thirteen Cybersecurity Questions Lawyers Ask" by some of my colleagues has been appended to this paper after the ENDNOTES.

ENDNOTES

---

[1] Jim Calloway, *Every Law Firm Is a Technology Business*, 42 LAW PRACTICE MAGAZINE 72 (Sept/Oct. 2016), http://www.mazdigital.com/webreader/43138?page=74 [https://perma.cc/KYY5-X5RJ].

[2] In Re Oklahoma Rules of Professional Conduct, 2016 OK 91, http://www.oscn.net/applications/oscn/DeliverDocument.asp?CiteID=479331.

[3] https://www.lawsitesblog.com/tech-competence

[4] *Sony's Amy Pascal Steps Down In Aftermath Of Cyber Attack,* NPR.ORG (February 5, 2015 5:36 PM ET), http://www.npr.org/2015/02/05/384119642/sonys-amy-pascal-steps-down-in-aftermath-of-cyber-attack [https://web.archive.org/web/20150428092546/http://www.npr.org/2015/02/05/384119642/sonys-amy-pascal-steps-down-in-aftermath-of-cyber-attack].

[5] David Lat. *Beware of Big Hacking in Biglaw*, ABOVE THE LAW (Mar. 30, 2016, 5:34 PM), http://abovethelaw.com/2016/03/beware-of-big-hacking-in-biglaw/ [https://web.archive.org/web/20161027133359/http://abovethelaw.com/2016/03/beware-of-big-hacking-in-biglaw/].

[6] ABA Standing Comm. on Ethics & Prof'l Responsibility, Formal Op. 477 (2017), https://www.americanbar.org/content/dam/aba/administrative/professional_responsibility/aba_formal_opinion_477.pdf
[7] Texas Prof'l Ethics Comm., Formal Op.648 (2015), https://www.legalethicstexas.com/Ethics-Resources/Opinions/Opinion-648.aspx.
[8] *Email Attachments vs. Client Portals*, *supra* note 8.
[9] Sharon D. Nelson, Esq. and John W. Simek, *Encryption Made Easier: The Basics of Keeping Your Data Secure*, https://perma.cc/VNU9-V4M2 .
[10] Quincy Larson, *How to Encrypt Your Entire Life in Less Than an Hour*, FREECODECAMP, (Nov 9, 2016), https://medium.freecodecamp.com/tor-signal-and-beyond-a-law-abiding-citizens-guide-to-privacy-1a593f2104c3#.3p7wdrn63 [https://perma.cc/KM7W-BGBC].
[11] *Forget Tough Passwords: New Guidelines Make It Simple,* NPR.ORG (AUGUST 14, 2017 4:51 PM ET), http://www.npr.org/sections/alltechconsidered/2017/08/14/543434808/forget-tough-passwords-new-guidelines-make-it-simple [https://web.archive.org/web/20170920212733/http://www.npr.org/sections/alltechconsidered/2017/08/14/543434808/forget-tough-passwords-new-guidelines-make-it-simple].
[12] Neil J. Rubenking*, LastPass 4.0 Premium*, PC MAG, (Nov. 2, 2016), http://www.pcmag.com/review/317692/lastpass-4-0-premium [https://web.archive.org/web/20170910020526/http://www.pcmag.com/review/317692/lastpass-4-0-premium]
[13] Lee Munson, *1Password Review*, COMPARITECH BLOG (May 18, 2016), https://www.comparitech.com/password-managers/reviews/1password-review/.
[14] Jason Carpenter, *KeePass Password Manager Review*, TOM'S GUIDE (Jul 20, 2016, 11:56 AM), http://www.tomsguide.com/us/keepass,review-3768.html.
[15] Neil J. Rubenking, *Dashlane 4*, PC MAG, (Mar. 9, 2016), http://www.pcmag.com/article2/0,2817,2461280,00.asp.
[16] n the Matter of DISCIPLINARY PROCEEDINGS AGAINST Kristine A. PESHEK, 798 N.W.2d 879, (Wisc. 2011) https://apps.fastcase.com/Research/Public/ExViewer.aspx?LTID=Q3QXLB6HtoP9yTlBKxBh9Zy%2bRTYc5serEL9QmGCz36Yn17Gs8ZlaXg0sC1jHO%2bpp.
[17] Florida Lawyer Fired for Posting Client's Leopard-Print Underwear, https://www.yahoo.com/news/florida-lawyer-fired-posting-clients-leopard-print-underwear-205820383--abc-news-topstories.html
[18] Lauren Silverman, Turning To VPNs For Online Privacy? You Might Be Putting Your Data At Risk, NPR.ORG (August 17, 2017 3:00 PM ET), http://www.npr.org/sections/alltechconsidered/2017/08/17/543716811/turning-to-vpns-for-online-privacy-you-might-be-putting-your-data-at-risk [https://web.archive.org/web/20170920212723/http://www.npr.org/sections/alltechconsidered/2017/08/17/543716811/turning-to-vpns-for-online-privacy-you-might-be-putting-your-data-at-risk].
[19] Jim Calloway, *The Holidays Bring More Email Threats,* JIM CALLOWAY'S LAW PRACTICE TIPS BLOG (Nov. 21, 2016), http://www.lawpracticetipsblog.com/2016/11/holidays-bring-email-threats.html.
[20] Kingston Technology, *Ironkey*, http://www.ironkey.com/en-US/ (last visited Sept. 21, 2017).

A Baker's Dozen: Thirteen Cybersecurity Questions Lawyers Ask

By Sharon Nelson and John Simek

The authors are the President and Vice President of Sensei Enterprises, Inc., a legal technology, information security and digital forensics firm based in Fairfax, VA. 703-359-0700 www.senseient.com

As many readers know, we lecture a lot. A whole lot. So we thought it might be interesting to relate the questions we have been asked most often in the past several months. Always fascinating to see what is "top of mind" at conferences and CLEs.

"I've been thinking about cybersecurity - what's most important? A security assessment, penetration testing or employee training?"

Well . . . let's start with penetration testing. For most solo/small law firms, this is probably overkill unless you have major league clients or extremely high value data. In pen testing, you are asking a company to pretend they are the "bad guys" and attack you – it is scary stuff, and tends to be expensive. The company will generally require a "get out of jail" free agreement, saying that they are not liable for any damages resulting from a successful compromises of your network.

A security assessment (sometimes also called an audit) is far less expensive. The assessment is usually done using software tools and involves a thorough review of your network. The result is generally a report identifying your critical vulnerabilities, medium-level vulnerabilities and low-level vulnerabilities. As a rule, it tends to come with a proposal for (at least) remediating the critical vulnerabilities along with the estimated cost. We believe it is wise to do these assessments, using a certified third party cybersecurity company, annually. Many clients and cyberinsurance companies are beginning to require these assessments as well.

There is no getting around the absolute need for annual employee cybersecurity training. It is generally fairly inexpensive and covers the basics of current threats and how to avoid such things as clicking on suspicious links/attachments, going to sketchy websites, giving information over the phone (duped by social engineering), and many other easy-to-make mistakes. A solid hour of good training each year is a small price to pay for educating your employees and creating a culture of cybersecurity.

"What is the best password manager?"

In our opinion, the best password manager is **one you actually use** – because most of you don't use one. Seriously, any good password manager is fine and the selection is largely a personal one. What features do you need? Does the password manager have to automatically fill in website forms for login? Can the password manager store all the various types of data (e.g. Passport, credit cards, prescriptions, etc.) you need? Is the password database stored in the cloud or locally on your own device? Can the password database be replicated and synchronized across multiple devices, including your smartphone?

If you want a little neutral help, check out PC Magazine's review of the best password managers of 2018: https://www.pcmag.com/article2/0,2817,2407168,00.asp. The two highest rated are Dashlane and Keeper, but you should review the feature sets and pricing to see what works best for you.

"Is it really safe to move my law firm data to the cloud – and is it ethical?"

Virtually all cybersecurity experts now agree that the cloud will protect your data better than you will. Is the cloud absolutely secure? Of course not. But do law firms, especially solo/small firms tend to be woefully insecure? Yes, they do.

Most lawyers are using the cloud these days – perhaps for email, perhaps to share files, perhaps because they have Office 365. There isn't a single state bar that has a problem with cloud computing – provided that you take reasonable precautions to comply with your ethical duties. This means asking questions such as:

- Where will my data be stored?
- Is it encrypted at rest and in transit?
- Who holds the master decryption key? (preferable if you do)
- How long has the provider been in business?
- Is the provider accustomed to working with law firms and familiar with legal ethics?
- What happens to your data if the provider declares bankruptcy?
- What happens to your data if you change providers? What format is your data provided in? Is there a charge?
- If law enforcement appears with a search warrant for your data, will your provider notify you right away so you have the chance to file a Motion to Quash?
- Who has responsibility for reporting a data breach should information be compromised?

As you might imagine, there are a lot of questions that you might ask. You can find many useful expert tips for moving your firm to the cloud at https://www.attorneyatwork.com/tech-tips-making-move-cloud/.

"How can I keep up with legal technology? It moves so fast!"

Trust us – we have the same problem. We each read about two hours a day – and we still can't keep up. We have a couple of resources to recommend. We didn't want to recommend a long list, but here's our favorite two resources:

Bob Ambrogi's LawSites blog at https://www.lawsitesblog.com/ Bob keeps up at the forefront of legal technology.

Attorney at Work blog, which offers a good tip each day which may be found at https://www.attorneyatwork.com/. Not all of the tips are legal tech, but all the tips are interesting and many involve technology.

If you sign up for these free resources, you will receive an email each day. The vetting process is very simple – just look at the subject line – you'll know right way if this is a topic you're interested in. If not, hitting the "delete" button is simple.

Beyond these two resources, there are plenty of legal tech podcasts at Legal Talk Network. https://legaltalknetwork.com/ If you are driving to work every day or taking a train/plane/bus, listening to a podcast is a perfect way to learn – and it makes travel time pass faster!

Don't forget CLEs – and ask your colleagues for recommendations regarding speakers who both inform and entertain. Legal tech is hard enough for most lawyers – a few entertaining stories along with the legal tech education is always a good mix.

"Is it safe to open emails as long as I don't click on a link or attachment?"

Generally speaking, yes. You are unlikely to have any malware installation if you use a browser to access your email. The majority of lawyers use Outlook as their email client, which also has safeguards against automatically running scripts. As with all technology, things can change so be sure you are especially careful when opening a suspicious email.

"What is the security software you recommend for smartphones?"

ALL smartphones should have some security software, even iPhones. Many of the major desktop security suites (e.g. Symantec, Trend Micro, Kaspersky, etc.) also have agents for mobile devices. The advantage is that the same centrally managed administration console can monitor desktops, servers and mobile devices. We would suggest investigating Lookout or Sophos for stand-alone installation of security software for mobile devices.

"How do I recognize a phishing email and what should I do with a suspicious email?"

There are obvious red flags to pass on to employees:

- You don't know the sender
- You do know the sender but if you look closely, the address is one letter off (this one happens a lot)
- Nothing in the note seems personal to you
- You weren't expecting the email
- Reference is made to a bank/product/service you don't use
- Words are misspelled
- The grammar is poor
- The email doesn't address you by name
- The message asks for personal information
- There is an attachment which seems suspicious in conjunction with other factors or a link to a website (and no, hovering over the link doesn't necessarily ensure that you will go to the address shown – drive-by malware infections from visiting malicious sites are quite common)

The list goes on and on – you need to advise your employees to be on the lookout for anything suspicious and not to be click-happy! If something about the email doesn't feel "right", you should have them forward the email to your IT or cybersecurity folks.

"What's the most important security tip for 2019?"

Beyond a doubt…DO NOT reuse passwords! The bad guys are now using computer bots to brute force attacks using passwords revealed from past data breaches. If you continue to reuse passwords, there is a high probability that the password will be used against other systems. This is another great reason to use password managers so that you can have unique passwords for every system.

One password you should NEVER reuse is the password you use to log into your law firm network.

"I've heard that Office 365 and Windows 10 are not inherently secure – what can I do to make them secure?"

Default configurations are never good – and Microsoft acknowledges that, though users seem blissfully unaware of it. Microsoft has developed a program called Secure Score. Microsoft first introduced Office 365 Secure Score to help to understand your security position by giving you advice on what controls you should consider enabling, and helping you understand how your score compares to other organizations. As an example, enabling MFA (multi-factor authentication) is worth 50 points. The higher the score the better the security posture. The program was so successful that it has been expanded to include Windows Secure Score since there are also options and features you can enable in a Windows environment. As a result, the program is now called Microsoft Secure Score and includes Office 365 and Windows. Just do a search for 'Microsoft Secure Score' and you'll see information on how to grade and improve your Secure Score.

"What is the most common cause of data breaches and who is behind them?"

Every year, the Verizon Data Breach Investigations Report gives us the most current answer to that question. You can download the report at https://enterprise.verizon.com/resources/reports/dbir/. Hacking is the most common threat, with 81% of the hackers using stolen credentials (ID/password).

More stats that are useful:

- 73% of the breaches were perpetrated by outsiders while 28% involved internal actors (this could mean simple error as well as malicious actions).
- 50% of breaches were carried out by organized criminal groups.
- 12% of breaches involved actors identified as nation-state or state-affiliated.

"What should I do when I get an email with wiring instructions from a client or one of the law firm partners?"

There should always be a verification process – a written policy is a very good idea. If you can walk down the hall to see the person in your office who actually sent the instructions, that's a good way to get verification – and a little exercise. You can also pick up the phone and call the partner or client – but never use a phone number contained in the email about the wiring instructions. Use a number you know to be that of the partner or client.

The same advice applies to requests for W-2 information – this scam tends to peak every year around tax time.

"What are new rules for making passwords?"

New Digital Identity Guidelines were published by the National Institute of Standards and Technology in June of 2017 and may be found at https://pages.nist.gov/800-63-3/sp800-63b.html. First, passphrases

are recommended – they are much easier to remember. “Breaker19,you’vegotabearintheair” is a perfectly good choice (for fans of *Smokey and the Bandit*).

While the guidelines call for a minimum of eight characters, most experts are recommending fourteen. NIST says passwords should be allowed to be as long as 64 characters, which we know isn’t something lawyers are going to do. Passwords should allow all printable ASCII characters, including spaces, and should accept UNICODE characters too, including emojis. We note with a chuckle that we saw emoji passwords demonstrated on *The Today Show* and no one could remember them just a couple of minutes after making them.

Every time you make a new password, it should be checked against a database of known compromised passwords, so you can’t choose one of those. This is slowly being automated as we write. Very soon, this will be standard.

Also, for those of you with security fatigue (and isn’t that all of us?), you don’t need to have passwords expire without reason. Passwords should only be reset when they are forgotten, if they have been phished or if there is reason to believe that they may have been compromised.

“I do work from home – how do I secure my wireless network at home?”

First, change the default settings of the wireless router. You should change the settings for the network name (SSID), IP address range, administrator ID, password, etc. Next, configure the Wi-Fi to be encrypted. Currently, there are three types of Wi-Fi encryption - WEP, WPA, and WPA2. WEP and WPA have been cracked and there are free tools available to break the rather weak encryption. WPA2 has also been cracked, but vendors have developed patches to improve the security. That means that you should be configuring your wireless router to use WPA2 encryption at this time. The good news is that the WPA3 standard has been approved. We should start seeing products supporting the new standard in 2019, perhaps even by the time this column is published. Keep an eye out and upgrade/replace your wireless router to one that supports WPA3.