Baker's Dozen: Thirteen Cybersecurity Questions Lawyers Ask

by Sharon D. Nelson and John W. Simek

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 2019: https://www.pcmag.com/roundup/300318/the-best-password-managers. 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.

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 (phone)
www.senseient.com