What's On the Horizon for Law Firms in 2021?

by Sharon D. Nelson, Esq. and John W. Simek

Jim Calloway, Director of the Oklahoma Bar Association's Management Program, frequent speaks with us about the future of law. Recently, Jim recorded a Legal Talk Network podcast with Sharon which bears the same name as this article. You can find the podcast at https://legaltalknetwork.com/podcasts/digital-edge/2020/12/whats-on-the-horizon-for-law-firms-in-2021/.

The authors continue the discussion below.

We were glad to see the backside of 2020. But 2021 carries many uncertainties with it and that makes predictions risky. Fortunately, we are not averse to risk-taking and it is a worthwhile effort to make predictions, especially about things we're fairly certain will come to pass.

One thing that both lawyers and clients seem to have changed their minds about is the importance of physical office space. Until we read the Clio 2020 Legal Trends Report which surveyed a combination of Clio users and non-Clio users, we had no idea that 21% of law firms were already operating without commercial office space and since the pandemic, another 7% of lawyers have given up their commercial offices and 12% are unsure they'll keep them going forward.

It's a pretty good bet that those numbers are higher today. We have heard from some of our big law friends that they are actively looking to sublet some of their space. Those that were near the end of their leases were the lucky ones because they can negotiate for downsized space. We, on the other hand, signed a five-year lease in February 2020. Great timing, huh?

We may also see rotating offices (yes, there will be institutional resistance), where lawyers showing up to work get assigned to an office with the office space rotating among the firm's lawyers. Large, luxurious partner offices may also become a thing of the past. The physical footprint of the office may be reduced but virtually everyone seems to agree that firms of a certain size need some kind of office in which to conduct meetings, have a receptionist to deal with mail, packages, etc.

Another topic that comes up frequently is the cloud. We've been saying for a very long time that the cloud protects the security of law firm data better than the lawyers would and that is so true. We regularly hear stories of cloud breaches but lawyers often misunderstand their cause. The majority of those breaches are caused by users who misconfigured the security of the cloud and their presence in the cloud.

Recently, we've begun to say that the best time to move to the cloud was five years ago and the second-best time is today. Clio CEO Jack Newton has said that if you're not in the cloud, you're not in the game. He calls the cloud table stakes, which we thought was a very interesting term. Also of note is the ILTA 2020 survey where the majority of respondents said, with every upgrade, they were going to the cloud. So, it's a staged process but it's in place for every upgrade.

In the beginning of the pandemic, those lawyers that had all their data in the cloud were way ahead of those who still had all their data locked in physical files. If your files were in the cloud, you could work. You weren't stuck with lugging files back and forth from the office.

We worry sometimes that lawyers are rearranging the deck chairs on the Titanic because they've been holding on to the past so much, not adapting to the future. We did see a lot change caused by the pandemic and we're hopeful that we will continue to innovate. Lawyers need to take a look at what they've always done and say, "Is this what we always should do? Is there a better way?" The seven most dangerous words might be "But we've always done it that way."

Cybersecurity has been a huge issue and will continue to be. The pandemic has been a nightmare of people calling and saying, "We're down, we're down, we're down. We've got a ransom that we're supposed to pay. What is all this about? What do we do?"

It was clear that there is not a lot of incident response planning going on because any incident response plans they had (if any) were just frozen in time, never updated. Cyber criminals of course are always sniffing for new opportunities and we certainly gave it to them with our new work from home environment. We saw more than a 750% rise in ransomware in the first six months of 2020 and home networks are about three and a half times more vulnerable than law firm networks. Using home machines rather than work-issued laptops that we bring

home that are secured by the law firms – well, those home machines just complicate the problems.

As a result, one change we are seeing is that law firms are warming to the idea of making sure that all devices connected to the law firm network must be owned and secured by the law firm. That's one trend we are sure will continue.

We have fond memories of the days when a thousand dollars was a big ransom. Seems like a long time ago. In the third quarter of 2020, the average cost of ransomware was approximately $233,000 according to the cybersecurity and ransomware specialist firm Coveware.

Law firms are getting hit left and right among many other entities and, of course, recently, we've had government agencies and others hit in the SolarWinds attack which seems to be more about espionage than it does about ransomware.

With law firms, we now have the double ransom where the bad guys steal your data before they encrypt it. If you're able to recover from backups without paying the first ransom demand, you will then get a second ransom demand for supposedly destroying your data and, of course, since we always trust cybercriminals, paying the ransom is often what we do. We pay them and trust them that our data has been deleted. When they make the demand, they will send you samples to show you that they have the data or they'll post them on the dark web to scare you into paying. If you chose to pay for the decryption key in the beginning, you may still get that second ransom demand.

Insurance companies are often choosing to pay the ransom rather than pay for an extended business interruption and possibly the costs associated with the theft of the data. So, as of the end of 2020, fully 25% of victims today were paying ransoms.

We saw a 75% increase in business email compromise in the first three months of 2020, but the whopping great statistic was that we then saw a 200% increase each week from April to May. We have to assume that this means that cyber criminals are having a great degree of success using these compromised accounts.

Worse yet, once the criminals have all of your email, your contacts, your calendar, et cetera, you can't do anything about that. That horse has left the barn. What

everyone should do is have multi-factor authentication which prevents 99.9% of business email compromise attacks. Wherever you can, you should enable MFA. It's almost everywhere these days. But it's a matter of security versus convenience because lawyers don't want to have to enter a text code from their phone. If you can block 99.9% of these attacks, focus on security instead of convenience. Microsoft itself thought it was so important that they made MFA free.

Yes, most lawyers are afraid they'll have to enter a code from their smartphone, on their laptop or other device, but in most cases, that's not true. It might be true of your doctor's office. It might be true of your bank or your stockbroker but most of the time, you can make your devices "trusted devices" so that no code is needed unless you buy a new device, you change your password or perhaps you're visiting someone and using their device for some reason.

Recently, we're trying to move people away from text messages because SMS text messages can be so easily compromised. But if that's all you have, it's infinitely better than nothing. Authenticator apps and authenticator tools are what's going to replace both two-factor authentication and multi-factor authentication. There are actually hardware tokens like Yubico's YubiKey line or CryptoTrust OnlyKey where you have a physical thing you carry on your key ring or in your purse and it plugs into either your USBA slot or USBC slot or Lightning for iPhone users.

Most people are going to prefer the software tokens - Microsoft authenticator, Google authenticator, etc. These apps constantly generate new codes that are only valid for about 30 seconds, so when you log into an account and you're prompted for a code, you just open your app and enter that most recent code and you're good to go.

Obviously, there's a lot of change in cybersecurity.

But let's go back to the daily business of law.

Some things are going to stick post-pandemic. Virtually all law firms now do electronic contracting, most using DocuSign (our preference) or AdobeSign.

Every lawyer now knows about e-notarization, which they didn't before. People who didn't have case management software are getting it and recognizing the value of secure client portals. Clients love the security of client portals where they

can go in anytime and see their documents, review/pay their bills, etc. This has become part of being a client-centric law firm.

There are still an amazing number of lawyers who refuse to accept credit card payments. We've never understood that because 40% of consumers, according to one of the Clio surveys, would never hire a lawyer who didn't take debit or credit cards. We've accepted credit cards for a very long time, but the pandemic caused cash flow to slow (slow mail delivery may have been a part of that). We began emailing our clients asking those who were writing checks to shift over to credit card payment. We immediately saw a marked increase in people paying promptly and the cash flow is much more dependable. It is critical these days to send out bills electronically with a payment link.

The thing that we are most certain will stick is the dependence on video conferencing. Yes, we'll go back to in-person meetings and courtrooms again, but now that the legal world and even the judicial world has learned to use virtual conferencing software, we doubt that we'll ever totally go back to our old ways. Too much money and time is saved by meeting clients via Zoom (the clear winner of the video conferencing software wars) – the same is true of court proceedings.

There are drawbacks of course. Some things are just better in person – when you can look a client or opposing counsel in the eye, you may "read" them better – and you may be more persuasive in-person. There are trade-offs and we're still figuring out what works when.

Clients are totally sold on video conferencing – they don't want to be waiting in your well-appointed reception area, which they are now keenly aware that they are paying for. They don't want to travel to your office. They don't want to take time off from work. Clients and prospective clients all seem to have mastered Zoom – at least its fundamentals – so we doubt it will lose its dominance no matter how many of its features are imitated by its competitors.

Finally, we are seeing artificial intelligence being adopted more rapidly by firms of all sizes and that's likely to be a continuing trend in 2021. Could it be unethical NOT to use AI? We just read an article with that title. The answer is yes!

Though there are several ethical rules which may be implicated, notably a lawyer's failure to use AI could implicate ABA Model Rule 1.5, which requires

lawyer's fees to be reasonable. If AI reduces costs, limits risks and is much faster, not using AI may result in a lawyer charging an unreasonable fee to a client." We are seeing more and more lawyers, even in small firms, beginning to use AI in e-discovery, legal research, contract analytics, predictive analytics, document management and expertise automation, among many other arenas.

These are just some of the changes that law firms will see in the future. Nothing is more worthwhile to the thoughtful lawyer than to constantly scan the horizon for changes that can enhance the successful practice of law. If there's any silver lining to the pandemic, it is that it has shaken the legal world up and brought it years into the future.

Sharon D. Nelson, Esq. is a practicing attorney and the president of Sensei Enterprises, Inc. She is a past president of the Virginia State Bar, the Fairfax Bar Association and the Fairfax Law Foundation. She is a co-author of 18 books published by the ABA. snelson@senseient.com.

John W. Simek is vice president of Sensei Enterprises, Inc. He is a Certified Information Systems Security Professional, Certified Ethical Hacker and a nationally known expert in the area of digital forensics. He and Sharon provide legal technology, cybersecurity and digital forensics services from their Fairfax, Virginia firm. jsimek@senseient.com