The Future of Law Post-Pandemic: A Roller Coaster Evolution

Richmond Law School

February 19, 2021

Presenters: Sharon D. Nelson, Esq. and John W. Simek

President and Vice President, Sensei Enterprises, Inc.

jsimek@senseient.com; snelson@senseient.com

https://senseient.com; 703-359-0700

The Future of Law Post-Pandemic: A Roller Coaster Evolution

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

Introduction

The Future: By the Numbers

In October 2020, Clio's Legal Trends Report was officially released in conjunction with the Clio Cloud Conference 2020.

As Jack said in an interview with author Nelson, after the pandemic hit, we moved ten years into the future in 10 weeks.

What alternative did we have? None.

How are lawyers planning to change their ways? Take a look at these stats:

- 96% say they'll store firm data in the cloud.
- 95% say they'll support electronic documents and signatures.
- 96% say they'll accept electronic payments.
- 96% say they'll use practice management software.
- 83% say they'll meet clients through videoconferencing.

To show you how much change there has been, in planning and implementation, here's how lawyers are operating during the pandemic:

- 85% of law firms are using software to manage their practice.
- 79% of lawyers rely on cloud technology to store their firm's data.
- 62% of firms allow clients to securely share and sign documents electronically.
- 73% of firms allow clients to pay invoices electronically.
- 83% of firms are meeting with clients virtually.

As you can see, they are doing better with technology now and plan to do MUCH better in the future.

Clients and lawyers are also converging on a consensus – that brick and mortar offices are not very important. More than half of consumers believe that most legal matters can be handled remotely.

Before the pandemic, 21% of law firms were operating without commercial office space. Since the pandemic, another 7% of lawyers have given up their commercial offices and 12% are unsure they'll keep them in the future.

The larger firms will no doubt keep offices but may scale them back – and certainly reconfigure them.

You can read the full Clio report at https://www.clio.com/resources/legal-trends/

By the way, knocking off the commute to the office often gave lawyers, especially in large, urban-based firms, an extra two hours in their day.

Interview with Clio CEO Jack Newton

Few people have given as much thought to the future of law practice as Jack Newton. As noted above, he gave an interview to author Nelson at Clio Cloud Conference 2020, where he was happily surprised by having over 4500 attendees, more than double the 2000 attendees at last year's in-person conference.

Jack noted that there has been a "Teutonic shift" in the legal profession. Suddenly, lawyers who wanted to practice law the way they always had were embracing technology on all fronts. As Jack commented, there will be winners and losers in this process. There are lawyers who are still waiting for the pandemic to blow over, thinking they can return to the past. But this is not a blip on the radar. Perhaps not all changes are permanent, but many of them are. On that, the vast majority of lawyers are agreed.

Clio announced many integrations at the conference, including integrations with Google My Business, HelloSign, Zoom, Microsoft Teams and more.

Jack commented that no one "can do it alone" and that integrations are key to solving the problems that clients have. Why reinvent the wheel yourself when someone else already has? The answer is to integrate your work with theirs. We suspect the legal profession will see many more integrations.

Notable as well is the new Sign in with Clio feature, which will allow Clio users to log-in to integrated third-party applications using the same credentials used for Clio Manage and Clio Grow. This is launching initially for Clio's integration partners Fastcase, Legalboards, myFirmData, WiseTime and LawYaw, but Clio plans eventually to extend it to all of its more than 200 integrations.

No matter what software a lawyer uses, they are likely to see a lot more integrations in the coming years.

Jack stated that the unifying theme of the conference was that the future of law is client-centric and cloud based. Both have been themes that Jack has underscored for a long time. Lawyers may benefit from reading and then thinking about the concepts contained in Jack's recent book The Client-Centered Law Firm.

Two important points from that interview:

What clients want and what lawyers want is beginning to converge - both want to work remotely and collaborate digitally.

Law firms must now be cloud-based. Or, as Jack puts it, "The cloud has become table stakes." Minus the cloud, you're no longer in the game.

Cybersecurity Evolves Quickly After March 2020

Though the entire ABA 2020 Legal Technology Survey Report is out, first up online were the stats related to Technology Basics and Security. Respondents were asked a total of 262 questions, with 21 questions focused on security. The attorneys who responded were in private practice and here is the breakdown of participants: solos (26%); firms of 2-9 attorneys (30%); firms of 10-49 attorneys (17%); firms of 50-99 attorneys (5%); firms of 100-499 attorneys (10%), and firms of 500+ attorneys (12%).

The answers came in between March and May 2020 so they do reflect the initial impacts of COVID-19, particularly the work-from-home movement.

43% of respondents use file encryption, 39% use email encryption, 26% use whole/full disk encryption. Other security tools used by less than 50% of respondents are two-factor authentication (39%), intrusion prevention (29%), intrusion detection (29%), remote device management and wiping (28%), device recovery (27%), web filtering (26%), employee monitoring (23%), and biometric

login (12%). By in large, this indicates that lawyers are not taking cybersecurity as seriously as they should be, though the recent surge of ransomware will no doubt change those statistics next year.

How are firms doing with cyber insurance? Firms ranging in size from 10-49 attorneys are most likely to have cyber liability insurance (40%), followed by firms of 100+ attorneys (38%). One notable trend is the increase in the number of smaller firms with such coverage, with firms of 2-9 attorneys (36%) and solo attorneys (33%) up respectively from 27% and 19% since 2017. We are happy to see those numbers but they also reflect that we still have a long way to go.

As some firms have noted to their chagrin, insurance companies sometimes deny coverage. There are a lot of exclusions and there have been more than a few court battles. Cyber insurance is great and certainly helps fill the risk gap, but it won't protect you from having to deal with a data breach and you have to be darn sure to understand the coverage you have.

We were not surprised that the new survey shows that 29% of respondents have suffered a data breach (compared to 26% in 2019). We have always thought it likely that this stat is significantly low – in many firms, especially large firms, attorneys may never learn of a breach unless it becomes public.

This is borne out by 21% of respondents reporting that they do not know whether their firm has ever experienced a security breach, with big firms representing the highest percentage of that number at 62% for firms with more than 100 lawyers.

34% of respondents have an incident response plan (IRP), compared to 31% in 2019. Progress there seems very slow to us. Unsurprisingly, 77% of respondents from firms of 100+ attorneys said that their firms had an IRP.

Suggestion for the laggards: Read ABA Formal Opinion 483 – and then start drafting.

Zero Trust Architecture Will Become the Norm

Virtual private networks (VPN) are very standard these days. But they are riddled with vulnerabilities – and subject to a “man in the middle attack.” They have wreaked havoc in 2020 in a work-from-home environment.

Enter zero trust network access (ZTNA).

An October 2020 Forrester study (commissioned by Cloudflare) offered some key findings.

Working from home compelled firms to transform how they operated in the cloud. However, 80% of the IT decision-makers interviewed said their companies were unprepared to make the transformation. Existing IT practices made it difficult to support employee productivity without security compromises.

As a result, 76% of the decision-makers said their firms intend to accelerate their shift to the Zero Trust security framework. More than three-quarters (76%) of decision-makers polled said their companies' security practices were "antiquated" and needed to shift towards Zero Trust network access.

The report found that 82% of the firms said they were "committed" to migrating to a Zero Trust security architecture. To achieve this goal, close to half (49%) of the firms elevated the role of CISO to board visibility while 39% had a Zero Trust-oriented pilot for 2020.

The migration towards Zero Trust faces various challenges, with 76% of the firms identifying Identity and Access Management (IAM) as the major challenge.

For those who are unfamiliar with the Zero Trust security model, it allows remote workers to access applications through a secure web-based gateway. The solution implements least-privilege principles and supports multi-factor authentication (MFA) and device security checks. Unlike a VPN infrastructure, Zero Trust is highly scalable, more affordable, and easily integrates with various single sign-on (SSO) platforms already available in the marketplace. It also permits the configuration of access control policies to manage permissions based on users' privileges and devices.

More than half of all businesses have experienced data breaches (58%) or increased phishing attempts (55%) during COVID-19. Ransomware attacks affected 29% of the respondents.

Infrastructure outages and VPN connection latency issues disconnected 33% and 46% of workers, respectively.

Several vendors offered their services for free or on extended trial periods to allow customers to test their Zero Trust security solutions during COVID-19. The

free trial period allowed companies to migrate to a zero trust security model and test advanced security solutions from reputable vendors. They could then select the products that met their security needs and sign up on a permanent basis.

We always knew Zero Trust Network Access was coming, but COVID has accelerated its arrival.

Are Law Firms Downsizing or Rightsizing?

What the heck is rightsizing anyway? Basically, it seems to be a word meant to hide the downsizing. There is no question that law firms are downsizing – the trend has continued since the pandemic erupted.

Many layoffs have been dubbed stealth layoffs – people are quietly furloughed and then laid off. Or the layoffs are immediate. We are seeing a lot of that in larger firms, primarily of supporting staff rather than lawyers.

How does the word get out? Often by employees talking to one another, sometimes forwarding the news to media outlets like Above the Law.

Sadly, with no end to the pandemic in sight, it may be some time before firms stabilize and revitalize. It is a bit tragic to see the latest title in the C-Suite, the Chief Sustainability Officer. As we were writing this article, Baker McKenzie announced the appointment of one its partners as its first Chief Sustainability Officer. Of course, clients also have Chief Sustainability Officers these days, so we suppose that having the same title makes some sense – and aligns the law firm's goals with those of their clients. Getting that alignment in place is major goal for many law firms now.

Going Cloud Crazy is All the Fashion

ILTA's 2020 Technology Survey was released in September 2020. When respondents were asked, "How would you describe the cloud philosophy at your firm?", over a third of responses were, "Cloud with every upgrade." (this trend was fairly even across firm size.) In other words, any upgrade would be done to the cloud. Once again, this determination echoes the thinking of Clio CEO Jack Newton noted above.

50% of firms reported their email was in the cloud or headed there soon – and 37% said the same of their document management software. Time and billing

software has been slower to move to the cloud, but it is definitely starting to go there.

Think Microsoft 365 had rapid adoption before the pandemic? Just look at the extraordinary charts below and see how quickly larger firms intend to adopt Microsoft 365.

WHICH PRIMARY EMAIL PLATFORM AND VERSION DOES YOUR FIRM USE?

	< 50 attys	50-149 attys	150-349 attys	350-699 attys	700+ attys
None/Not applicable	0%	0%	0%	0%	0%
Microsoft Exchange 2010	9%	10%	8%	7%	13%
Microsoft Exchange 2013	15%	14%	13%	9%	16%
Microsoft Exchange 2016	20%	32%	36%	55%	52%
Microsoft Exchange 2019	3%	3%	1%	11%	13%
Microsoft 365 or Exchange Online - subscription service	52%	41%	43%	18%	6%
Other	1%	0%	0%	0%	0%

WHICH EMAIL PLATFORM DO YOU EXPECT TO BE ON 12 MONTHS FROM NOW?

	< 50 attys	50-149 attys	150-349 attys	350-699 attys	700+ attys
Microsoft Exchange 2013	4%	1%	5%	0%	0%
Microsoft Exchange 2016	22%	27%	16%	36%	23%
Microsoft Exchange 2019	5%	14%	14%	14%	23%
Microsoft 365 or Exchange Online (subscription service)	68%	59%	66%	50%	55%
Other	1%	0%	0%	0%	0%

A lot of firms were not willing to invest in work-from-home technology at the beginning of the pandemic, shortsightedly trying to save money. As they realized how insecure home networks and personal devices were, they began to change their minds.

More and more, we are seeing firms buying more laptops for employees as firm assets, secured by the firm, and with the restriction that only the law firm employee may use the device.

As the survey noted, Zoom was the right technology at the right time, and Zoom's ability to respond to criticisms of security, usability and lack of features allowed it to make serious in-roads to our collective practices, including courtrooms, presentations, client meetings, and general collaboration. When asked, "Which videoconferencing software does your firm use?," Zoom usage has doubled (from 34% to 71%). And we would bet that the number would be even higher if the survey were done again today.

Microsoft Teams is being embraced as much for its collaboration features as for its eventual promise (as a multi-faceted tool that could prove to become a firm's Unified Communications solution.)

Thirty eight percent of firms used DocuSign, up 9 points from last year. Notarization moved to remote notarization processes, using applications like DocVerify. 21% of our firms responded they are using remote online notarization tools.

The Road Forward

As our friend at Microsoft, Ben Schorr, told us: "Hopefully this has given a positive, needed, shove to companies into digital transformation that will pay dividends for them down the road. It may have been unexpected/unplanned, and even uncomfortable right now, but hopefully 18 months from now they're saying 'I'm glad we did that, even if I wish it had been under better circumstances.' "

We are happy to see law firms discovering – even embracing – the notion that innovating how they practice law can propel them into a successful future. They are taking hard looks at new technology, upgrading their cybersecurity, changing their marketing efforts, planning to permit more remote working even after the pandemic and, most of all, making sure that their firms move toward operating in a client-centric mode.

Final Thoughts: The Times, They Are A-Changing

Our friend Judge Monty Ahalt used to say that we are the only profession that works by looking in the rear-view mirror. Well, that just won't serve well anymore. We expect some lawyers will conclude that and retire. Some will conclude that and change the way they practice.

And some will believe that this is all just a blip on the radar and stubbornly practice law as they always have.

That way lies extinction.

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.

Transcript from the 10/22/20 Legal Talk Network Digital Edge Podcast

Arizona First State to Approve Non-Lawyer Ownership of Law Firms

Intro: Welcome to The Digital Edge with Sharon Nelson and Jim Calloway, your hosts, both legal technologists, authors, and lecturers invite industry professionals to discuss a new topic related to Lawyers and Technology. You're listening to Legal Talk Network.

Sharon Nelson: Welcome to the 154th edition of The Digital Edge: Lawyers and Technology. We're glad to have you with us. I'm Sharon Nelson, president of Sensei Enterprises, an information technology, cybersecurity, and digital forensics firm in Fairfax, Virginia.

Jim Calloway: And I'm Jim Calloway, director of the Oklahoma Bar Association's Management Assistance Program. Today, our topic is Arizona is the first state to approve non-lawyer ownership of law firms.

Our guest today is Vice Chief Justice Ann A. Scott Timmer, who was appointed to the Arizona Supreme Court in 2012 by Governor Janice K. Brewer. Prior to her appointment to the Arizona Supreme Court, Justice Timmer was a judge on the Arizona Court of Appeals from 2000 to 2012, serving three years as chief judge. Notably she chaired the court's Legal Services Task Force, which recently recommended removing barriers for lawyers and non-lawyers to share fees.

She also chairs the court's Attorney Regulation Advisory Committee as a member of the National Conference of Bar Examiners Board of Trustees and has been elected as a member of the American Law Institute. Recently, she has been elected to serve on the Board of Trustees of the Appellate Judges Education Institute. Justice Timmer earned a bachelor's degree from the University of Arizona, a J.D. Magna Cum Laude from Arizona State University, and a master's in judicial studies from Duke University Law School. Thanks for joining us today, Justice Timmer.

Justice Ann A. Scott Timmer: Thank you very much, Jim. I'm delighted to be here.

Sharon Nelson: Justice Timmer, you chaired the Arizona Supreme Court's Legal Services Task Force, which recommended removing barriers for lawyers and non-

lawyers to share fees. How did this issue come before the Task Force and when did its deliberation start?

Justice Ann A. Scott Timmer: The issue came before the Task Force in January of 2019, which was the first month the Task Force, met and the purpose of the Task Force was to examine a number of issues as directed by our then Chief Justice Scott Bales, including whether we should allow lawyers and non-lawyers to share fees. So, right from the get-go, that was one of the tasks that the Task Force was to look at.

Jim Calloway: Ultimately, the Task Force recommended in favor for removing barriers for lawyers and non-lawyers to-share fees. How long did it take for the Task Force to make that recommendation, and were there any dissenting views?

Justice Ann A. Scott Timmer: Well, our Task Force moved very quickly. We met from January of 2019 through September that year and it culminated with a written report with ten recommendations to the Supreme Court which we sent to the court in October of that year. So, you can see it was a very fast-paced discussion that happened in the Task Force. So, it took about nine or ten months to digest it, have speakers, have work groups, have public input, and it moved very quickly. We did have — ended up having one dissenting view. Actually, all of us I think when we started out thought, "Well, this is just crazy. We can't we can't eliminate ER 5.4 and allow lawyers and non-lawyers to share fees. It's never been done that way." So, a number of us came from that place, myself included, but eventually in talking to people in different countries who have allowed this for years and having presentations and really discussing it and looking at the origins for the ER and its necessity in today's market, everyone on the commission save one person ultimately concluded that was the way to go. So, we did have one dissent, but the vast majority agreed with it.

Sharon Nelson: So, Justice Timmer, the recommended regulatory reforms were adopted unanimously by the court in late August and if I can read my notes here, they became effective, or they will become effective on January 1, 2021. Is that correct?

Justice Ann A. Scott Timmer: That's correct.

Sharon Nelson: And I understand there is now a framework to license these new businesses called alternative business structures, and also that the court instituted a new licensure process that will allow non-lawyers, called Legal Paraprofessionals, to begin providing limited legal services including being able to go into court with clients. How do you think these changes will positively impact the legal profession?

Justice Ann A. Scott Timmer: Well, we're hopeful that it will positively impact the legal profession in a number of ways. First, with what I think most lawyers are very interested in and this is this alternative business structure, what we hope it will do is it provide additional capital to be infused in legal firms, which in turn will allow for greater technological innovations in the delivery of legal services to the public. So, right now, you might put money into your law firm to, "Let's have the latest technology," that kind of thing, but at this point if you're in private law firms, at least the feedback we got most often, people aren't looking down the line 10, 20 years. They think they want to have a lot of their profits taken out now and aren't really looking that far into the future. So, with an infusion though of capital from someone who's able to invest, maybe in the long-term you can have more technology and partnering with technologists with a stake is anticipated to result in more innovation than just hiring someone to put technology into an existing practice. So, that's one thing. Also, we're hoping that it would allow firms to attract the best and the brightest non-lawyer partners, as they also desire equity in a firm that they're putting their time, sweat, and tears into.

So, this happens in the Washington D.C. market now to a limited degree. So, they might allow for example PR people or lobbyists to have equity interest in the firms, and that attracts the best and the brightest because if they know they can have a stake in the firm, that's something that that they would like to invest in as well. Also, it'll allows smaller-scaled, maybe one-stop shopping to provide legal and non-legal services to a client, and it will also help hopefully people who right now primarily use do-it-yourself platforms to be able to get greater services as well. So, for example, if you might have a LegalZoom or one of those who sell forms and such, they have the ability then — they have a lawyer there to say, "Well, you direct people in using the correct form." For example, you don't need a guardianship form. You maybe need a conservatorship form, that kind of thing. With the legal paraprofessionals, this was simply intended to provide more

avenues for legal assistance in areas where we're just not seeing lawyers currently. So, for example in the administrative hearings, criminal proceedings, and limited jurisdiction courts that don't involve incarceration and very small dollar cases and family court matters, with the exception of family court matters, you really don't see lawyers in the other areas and in family court, you don't see lawyers in the vast majority of cases. So, it will help with certainly the clientele. The people in the community who need legal services can get them from legal paraprofessionals, but as far as lawyers go, lawyers can also hire legal paraprofessionals and expand their practices. Lawyers in the family law practice for example can lower their costs by deploying these people and having a greater quantity in their practice, and also for — just it's always worth throwing out that it will reduce the number of pro per litigants, especially in the family law area, which is a huge benefit to the court system.

Sharon Nelson: Well, I asked you an awful lot of questions in one question, so thank you for that that extensive answer. You know, the funniest part to me was you reference lawyers not necessarily looking 10 to 20 years down the road and wanting to take money out but one of the very strange benefits of the pandemic has been that they've been investing in technology like never before, and they have moved themselves 10 years or more down the road because of that investment, but they were forced into it by the pandemic so that was kind of a curious benefit, don't you think?

Justice Ann A. Scott Timmer: It has been, and you could see it during the pandemic that at least in Arizona and— I'm sure elsewhere where you saw great use of like telemedicine for example, even in the legal industry of Rule 11 hearings and such done with that kind of technology in place, because of course the medical profession has gone down this road 50 or 60 years ago, allowing for these kinds of things. We saw it more in the pandemic and I think people saw the value of being able to use technology to enhance their practices.

Jim Calloway: Well, I know in other states, and notably Utah and California, have considered similar regulatory reforms and instead decided on a sandbox approach, a trial approach. Can you tell us about their progression down the same path and why you believe they weren't willing to flatly adopt these regulatory reforms in the way that Arizona did?

Justice Ann A. Scott Timmer: Well, of course I can't speak definitively for them but I can speculate a bit and I have had discussions with the Utah folks in particular and somewhat with the California people as well. We too considered the sandbox approach originally. So, after you got us all off the diamond thinking, "Well, we can't possibly do this," into the realm of, "Well, this is possible. Maybe we should do it as a sandbox approach," it does have the benefit of dipping your toes so to speak in a new regulatory regime, and then withdrawing quickly if that regime is not desirable, if the water is too cold or too hot. It also has the advantage of building the regime after determining how the test cases have fared. So, I'm assuming that that, it's a more measured approach and I'm assuming that's why Utah and California probably went that way, and it's a reasonable way to go. We ended up rejecting the approach, mostly because we feared that people, entities, firms wouldn't want to invest a lot of time and capital into constructing something when there was a chance that we might pull the plug in a couple of years. Instead, we drew on the experiences that the U.K. has had in regulating entities and in our own experience, frankly in regulation the court regulates, we already regulate entry entities, fiduciary entities. For whatever reason in Arizona, we regulate defensive driving schools and the like. And so, we have some of those experiences so instead, we just went ahead and drafted the rules that entities would have to follow, and then we'll know to apply for licensure.

Oddly enough, I've looked at Utah, at least in some depth, their sandbox approach and in effect, our systems really are not all that different from each other, in both a committee stillness that the application — the application still has in both systems regulations behind them and rules and things that must be provided, and a recommendation must be made to the Supreme Court in both states who ultimately have the final say, and then in Utah if you're in, you're in. You're grandfathered in even if they decide the program should be sunsetted, so it's not that different in the end, but there are two different approaches to get to the same place.

Sharon Nelson: Justice Timmer, what do you see as the strongest driver for these regulatory reforms?

Justice Ann A. Scott Timmer: The strongest one has to be the widening civil justice gap. According to the World Justice Project, the U.S. is presently tied for 99th out

of 126 countries in terms of access to and affordability of civil justice, and if I'm writing, throw out a couple other statistics that 86 percent of civil legal matters reported by Americans with low incomes received no or inadequate legal help, and 76 percent of cases involve at least one self-represented party. In those cases as well, if they're money cases, the medium judgment is only 2,441 dollars, and the average is just a bit over 5,000. So, these are not cases that most lawyers would consider worth their time, but they're still important to the litigants. So, I think that everyone knows it anecdotally, that people for the most part aren't able to get their legal needs met in the civil arena, and that's why they're going outside of our regulatory framework of the legal profession. They're simply going around us through looking for legal help in different arenas, so I think that was the biggest driver of the reforms.

Jim Calloway: As you know, there's been considerable opposition to the elimination of Ethics Rule 5.4. In fact, the ABA House of Delegates has had some very vigorous debates on the topic. Could you outline for our listeners what the opponents of such reforms typically argue?

Justice Ann A. Scott Timmer: Well, I've heard of course of many, many arguments and I think they all go into three categories, at least as I've seen them. Most of the arguments center around concerns that elimination of ER 5.4 will adversely affect lawyer independence. In other words, non-lawyers will be pressuring the lawyers into violating the rules of ethics, client confidentiality, and conflicts of interest. Those are the three big arenas that our people are most concerned with, having non-lawyers moving into partnership with lawyers.

Sharon Nelson: So, how would you answer those arguments of the opponents? Because I know one of the things we hear all the time is that what Arizona did is a great boon to the big four accounting firms, and obviously for you this really is an access to justice issue, but I would love to hear your answer to their arguments.

Justice Ann A. Scott Timmer: Oddly enough, we didn't hear one thing from the big four accounting firms or about the big four accounting firms, in all of the Task Force work and all of the rules — rule agenda forums that the Supreme Court conducted in deciding this. The only time we ever even heard about the big four was from the media, the national media law media that would call up saying, "What about the big four accounting firms? Aren't you doing just as you said,

giving them a great boon?" One of our Task Force members who's in a large firm and has contacts with the big four contacted a friend there who said, "We have no interest in Arizona. We're just two small potatoes." So, that could be why. We just we just didn't hear anything. Nobody cares about us. So, it was very interesting, however.

So, how do I answer the arguments of the opponents? Well, first of all, to answer how non-lawyer investors are going to pressure lawyers to violate their rules, those pressures exist now. Firms exist to profit. They have — a lot of the big ones have CFOs that will put pressure, partners that will put pressure for others to be profitable, so maybe take shortcuts in some of your discovery that you don't need to or try to get rid of this case. You have lenders, you have clients. Now, all of those put pressure on lawyers yet somehow, we manage to follow our ethical responsibilities. We have captured law firms from insurance companies but somehow, again, they're able to competently and ethically represent their clients regardless. Risk will always exist that that pressure can cause lawyers to violate their ethical rules. However, what we did as well is we took our other ethical rules and tightened up in the areas that I just mentioned, of independence, client confidentiality, and conflicts of interest. So, those rules will be toughened up.

Another thing is that in order to allow this, we decided that ABSs will have to be regulated as an entity. Currently, the court only regulates lawyers, not entities, not law firms but if you're going to partner with a non-lawyer, then you will be an ABS and you will have to submit yourself to regulation by the Arizona Supreme Court. I always wonder if the big four people are worried about maybe that'll be an impediment. Maybe they simply wouldn't want to submit themselves to yet another set of regulators, which they would have to. That regulation will follow more of the traditional route that we do with lawyers, so there's an ethical code, there's consequences for a violation including, not only sanctioning the lawyers, but also pulling the plug on licensing of the entity and imposing a monetary fine so there are certainly disincentives for violating any of the ethical rules or causing the lawyers to do that. I think we also shouldn't assume that non-lawyers are motivated to cause lawyers to violate their ethical rules. I mean, they they're there to be successful and to make a buck and because there would be a consequence to violations including pulling their license, it wouldn't be good for business to have that go on. And finally, we've seen that the information coming

from the U.K. and Australia showed us that complaints against lawyers did not increase when lawyers started partnering with the non-lawyers. In other words, the non-lawyers simply did not make the lawyers more unethical. As far as the client information, will that be safeguarded? Well, that goes on now, because certainly law firms don't employ just lawyers. You employ people in the mailroom, you employ people to be secretaries, paralegals, all kinds of things, and yet there's obligations that the lawyers have to ensure that the client information will be kept confidential. That shouldn't change with allowing non-lawyer partnership in the law firm.

Sharon Nelson: You know, all of your answers, it was fascinating there but the most interesting part to me was that I took this question about the big four accounting firms directly out of the media reports I had read.

Justice Ann A. Scott Timmer: Yeah. It's the media that's focused on this, and as I said, I haven't heard it from — we didn't hear it, and you would think that you would have at least the big firms in Arizona would be distressed and would have come forward, and we had big firm representation on our Task Force, and they like didn't bring it up. It wasn't an issue.

Jim Calloway: Well, I think a lot of the solo and small firm lawyers are concerned because for some of them, they do a lot of the same things that the paraprofessionals are going to get to do but I think they're already competing with lawyers, and they're going to have to adjust. We're hoping to improve the system, so how do you think the practice of law will evolve in Arizona in light of these reforms, Justice Timmer? And how fast do you expect progress to be?

Justice Ann A. Scott Timmer: Well, if I had a crystal ball, I would think that the practice is really going to see very little change at first, and that's mostly because one, information doesn't get out quickly about these types of things, and two lawyers are slow to change anything. We had an experience a few years ago. We changed our ethical rules to allow for unbundling of services, and you would think that people would, especially the small firms and solo practitioners, would take advantage of that but we found that they didn't. It took probably four or five years for people to start even realizing the rules had changed and what that means, and people are just slow to do that. I think what will happen is the first people to take advantage of the new ABS rules will be law firms. I've heard

already, mid-sized law firms are already starting to explore that. They've hired lawyers who typically advise law firms in their ethics and their practices to start asking questions about this and what does it mean, and what could we do. And so, they're starting to — some firms at least are starting to try to be more innovative, how can we take advantage of this to increase our practice, and I think what will happen is you'll have some of the first brave people that will try it in the first year or so, and then word will filter out if it's successful. Other firms will start thinking about joining in. If it's not successful, of course they won't. I don't know if any of the national firms like the LegalZooms and such will come into Arizona. I think that's certainly distinctly possible. I know that one of those platforms is going into Utah, so perhaps people will be watching that to see if it works. If it works, people will follow. That's just how it is.

I do know that one thing that I hadn't mentioned that was also a somewhat, I don't want to say a driver but a secondary factor that we're very well aware of, and that is that lawyers aren't all thriving in the legal profession. And I saw that one of your sponsors is Clio and I recall reading a survey that Clio did have about 60,000 of its clients, lawyer clients, who are small and solo firms using their software asking a number of questions about how much time they're spending, billing time, and how much they're collecting and charging, et cetera, and it's very surprising to see the results of that, that if I recall the average that people are making is a little — about 105,000 a year assuming a two-week vacation, and that's before paying overhead, so lawyers aren't thriving. A lot of lawyers aren't, and they've been — the solos and the smalls in particular have been squeezed over the years with the proliferation of online forms and do-it-yourself, and that kind of thing. So, they've had — it has become a more competitive business and somewhat, we thought what defines the legal market has been the ethical rules.

And ER 5.4 is one that has really restrained lawyers from competing in a number of areas that, as I say, has simply gone around our regulatory framework. So, I would think and what I would hope is that eventually, hopefully within the next 10 years, people will innovate more, it will give opportunities for small and solos to have more thriving practices and eventually, we could have something like the multi-tier system that the medical profession has with the different types of practitioners at different levels, and have more tech and such like the

telemedicine with Tele Law, that will not only serve the public better but also serve the needs of lawyers as well.

Sharon Nelson: Justice Timmer, after you had adopted these reforms, what kind of feedback did you get?

Justice Ann A. Scott Timmer: Well, most of our feedback was really before we adopted it, and that's simply because the way Arizona does it is that we have a very active public comment period in the nine months or so before we vote on whether to adopt a rule, so most of it came beforehand, and we also — because this is such an important reform, we also affirmatively reached out to public town halls, public opinion polls, and lawyers as well to try to get a full picture of what's needed. After we adopted it, that was just this past August, we didn't think of it much. I don't know if people are scared of us or what, but I've heard from other lawyers that represent lawyers that do it, the ethics lawyers, that they got a lot of feedback. Some people were very distressed we're changing everything, you know cats and dogs will live together, all that kind of thing. And so, some people are very distressed. Other people said it's about time things have to change and this is the way to move forward in a measured, contemplative way. I think most people that I've heard are simply watchful, want to see how this happens and how things will unfold, and they're well aware of course that we can always make changes here and there. That's the great thing about being on the court.

Jim Calloway: Well, you commented about the District of Columbia having a set of rules, but Arizona is the first state to have these kinds of rules. So, what's your prediction about what the rest of the states will do about non-lawyer ownership of law firms over time?

Justice Ann A. Scott Timmer: Well, I think that you're going to see more and more people looking at it. I know that a number of states are looking at it because they've invited me to talk to their Task Force that they've had, so I think there're about 10 states that are actively looking at the issue. I believe that what they'll probably do is, "Let's wait. While we're talking about it, let's wait and see how Utah and Arizona do and California if they adopt it because that will give us a better idea if this is a good idea or a bad idea, and we can learn from their mistakes and we can take the best of what they've done and move forward if it's

something that we would want to do." So, I think things will change in the country, particularly if we're successful in these two states.

Sharon Nelson: Well, we certainly do thank you for joining us today, Justice Timmer, and I suspect you will be successful. You certainly have studied all the various positions on this, and I must say as a former president of the Virginia State Bar and having been through this issue ad infinitum with lawyers, I hope that a lot of them will listen to this podcast because you do a really good job of explaining all the positions and why certain things maybe don't matter as much as we thought they did, but we know your time is valuable and we're so grateful that you were with us today.

Justice Ann A. Scott Timmer: Well, thank you so much for asking me as they're important issues and I'm happy to get the word out about it, and I will say that we even — I think I was very proud that we did get our Bar Board of Governors ultimately to vote in favor of this. So, I thought, "Wow, people were good at keeping an open mind."

What Kind of Fool Am I (That Doesn't Use MFA)?

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

Those of you of a certain age will remember the song "What Kind of Fool Am I?" That song was about love, but for Pete's sake, why is it that some lawyers keep insisting that they won't use MFA (multi-factor authentication)?

Thanks to our good friend Ben Schorr (who works at Microsoft) for sending us an August 7 Microsoft update on why multi-factor authentication is so critical. It is short, sweet and should be read by anyone who has resisted multi-factor authentication (and there's a lot of you!).

From the post:

"*When you sign into your online accounts - a process we call "authentication" - you're proving to the service that you are who you say you are. Traditionally that's been done with a username and a password. Unfortunately that's not a very good way to do it. Usernames are often easy to discover; sometimes they're just your email address. Since passwords can be hard to remember, people tend to pick simple ones, or use the same password at many different sites.*

That's why almost all online services - banks, social media, shopping and yes, Microsoft 365 too - have added a way for your accounts to be more secure. You may hear it called "Two-Step Verification" or "Multifactor Authentication" but the good ones all operate off the same principle. When you sign into the account for the first time on a new device or application (like a web browser) you need more than just the username and password. You need a second thing - what we call a second "factor" - to prove who you are."

Probably the most important point is that you do not need to use the second factor every time. You can make your phone and laptop "trusted devices." If the bad guys know your ID and password, but try to access your account from another device, they will need that second factor. Statistics show that using MFA stops over 99.9% of all account takeover attacks. It doesn't get much more persuasive than that.

When will you HAVE to use the second factor? When you get a new device or change the password for your account. But that's not very often. Sometimes, you

may be required to enter the second factor when you are accessing particularly sensitive data – medical sites and financial institutions often require two-factor authentication at every logon for your own protection. But for the most part, it won't be nearly the inconvenience that most people think it will be.

If you are really interested in security, consider the different kinds of two-factor authentication. SMS texts are infinitely better than not using 2FA, but there are more secure methods that you might consider.

SMS text messages are the least secure of the MFA implementations, primarily because it is vulnerable to SIM-jacking. That's where someone obtains a SIM card with your phone number and hijacks your phone number to another phone. Those SMS text messages then get sent to the hijacked phone.

A more secure MFA method is to use an authentication app such as Authy, Duo, Google Authenticator, Microsoft Authenticator, etc. The app generates a unique six-digit code every 30 seconds. When prompted for the MFA code, you type in the code that is displayed in the authenticator app. This type of MFA is susceptible to man-in-the-middle (MITM) attacks where the code can be intercepted as you type it in.

An even more secure MFA method is to receive a push notification to your authentication app. When you logon, the system sends a push notification to your registered phone. All you do is tap the notification to allow access. This means there is no code to enter or intercept.

Finally, the most secure of the MFA methods is a physical security key. YubiKey is a very popular security key as is the Titan Security Key from Google.

Recently, we have seen more account takeovers than ever. Read the Microsoft post carefully – it will answer most common MFA questions. And then begin to use MFA for all your online accounts. It's almost always FREE (your favorite price, right?). Very effective too. Just do it.

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 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 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.

The Practice of Law: Catapulted into the Future by the Pandemic

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

When lawyers turned the calendar page to January 2020, they could not have dreamt of the two-fold nightmare that would descend upon the profession so quickly. A global pandemic and a troubled economy at the same time? We thought we had seen the end of hard times when we finally emerged from The Great Recession in 2009. Some of our lawyer friends still have lines of credit to pay down from that recession.

The New Normal

In the "new normal," we learned that lawyers could work effectively from home. In the beginning, it was a bit of a mess getting everyone working remotely and safely but it was accomplished with amazing speed.

As we write this in May, new legal matters are down more than 30% according to a survey by Clio. 56% percent of legal professionals say they have seen a serious reduction in the number of people asking for legal help, and 53% say they are significantly less busy.

Sixty-seven percent of lawyers are worried about the success (and even the survival) of their practice and 57% are worried about making a living over the next few months.

We have also seen in a May LAW.COM report on actions taken by major law firms in response to the economic downturn. Firm after firm reported some mixture of layoffs, furloughs, hiring freezes, pay cuts, reductions in party distributions, freezes on discretionary expenses and suspension of summer associate programs.

Young lawyers are looking at a grim future. Those who graduated this year and passed the bar will not likely find jobs and those who have been with firms for just a year or two are the most likely to be laid off or furloughed. Add to that the burden of their student loans and it is no wonder that they are so anxious.

Where Are We With Technology?

The Clio report says 69% of lawyers view technology as more important to their firm than before COVID-19. Cloud computing is now seen as a necessity for survival by 83%. The fear of the cloud, once commonplace among law firms, has all but evaporated.

Will the way we practice law change? Two-thirds of lawyers believe it will. And we think they are right.

For years, lawyers have deferred (mostly because of cost considerations and inertia) upgrading their technology and cybersecurity enhancements. We have explained the importance of endpoint protection endlessly, but not until everyone was working remotely did that message hit home.

Cybercriminals, always sniffing the air for new opportunities, quickly realized that lawyers working at home were vulnerable, both because they were often using home machines (unprotected by their firm's security) and using home networks, many of which were not secure. Everyone had to scramble to up their security game under this new working environment. Now everyone wanted endpoint protection – immediately.

Webinars we taught on "Working Remotely – and Securely" attracted hundreds of attendees, suddenly interested in recommended VPNs, ways to speed up home networks, video conferencing tools and their safe usage . . . the list of live questions was so long that we had to extend the webinars past their scheduled end times.

Crystal Balls, Goat Entrails and Tea Leaves

Predicting the future of law practice is a dicey business. In two months, we changed how we practice law more than we did in the last two decades. Virtually everyone now knows about e-notaries, how to prepare documents for electronic signature, how to videoconference with colleagues, clients and courts, how to deposit checks via a phone app – and the list just keeps growing . . .

Though lawyers have traditionally grafted technology onto the way they always practiced law, they are now fundamentally changing the way they practice law. We are not likely to go back to the way law was practiced before this pandemic.

More than we ever thought possible, lawyers are evolving in how they practice law. Online court proceedings are still new, but rapidly becoming normal. Why do we need to congregate in person to do justice? There has been lots of lawyer resistance to online courts in the past – but it appears that more and more lawyers and judges are rethinking how we solve our disputes. Mediators have quickly glommed onto Zoom and other software tools for conducting mediations.

All those law firm meetings in conference rooms (which won't seem safe for a very long time) are now being conducted via video conferencing. While we started a bit awkwardly (inadvertently muting ourselves, talking over one another, etc.), we seem to have developed video conferencing etiquette rapidly. Lawyers are getting better at hosting meetings, muting everyone but the host(s) at the beginning and then unmuting folks after they electronically raise their hand. And we are learning how to secure our video conferences.

Which video conferencing service should you be using? It depends on your needs and desired features. The three big players are Zoom, Webex and Microsoft Teams. Many lawyers have turned to Zoom, which is feature rich, intuitive, well known to clients and other lawyers – and likely will be end to end encrypted by the time this article is published. A remarkable number of lawyers now own green screens so that they look more professional in their video conferences when using virtual backgrounds.

Getting payments electronically has become critical for most law firms – sending an office manager to deal with the checks in the mail has been the band-aid for many law firms, but for those solo/small firms who were not accepting electronic payments, they are now seeing the need to do so.

Will we ever go back fulltime to brick and mortar offices? It seems unlikely. There is a big push for "more work time, less commute time." And no one wants to go to work via carpools, subways, trains or buses. Since there is no expectation that we will have a COVID-19 vaccine until sometime in 2021, it unlikely that we will simply return to how we practiced law in the past. Amazingly, in May, the research firm Valoir conducted a broad survey of people working from home and only found a 1% average loss in productivity. Though work-at-home distractions (social media being the biggest distraction) occupy a little more than two hours a

day, workers are extending their workday to an average of 9.75 hours. That is driven, no doubt, by everyone's need for job security.

Anecdotally, law firms tell us they are regretting the amount of physical space that they have contracted for with their landlords. Many are thinking of downsizing during their next lease renegotiation. Rent abatements and renegotiation are taking place on a regular basis.

Facebook, Google and Zillow have announced that their employees will work from home for the remainder of 2020. Twitter has said that its employees may work from home indefinitely. As of May, most law firms tell us that they are not comfortable reopening yet – and they will listen to medical experts, not politicians, about when it is safe to reopen. Moreover, they are considering partial reopening, with some people working in the office and some from home, to make social distancing at work easier to achieve.

Global Workplace Analytics (GWA) thinks that, even after we triumph over COVID-19, 25%-30% of the workplace will still be working from home – because 80% want to work from home, at least some of the time. Rather to the surprise of many supervisors, who didn't trust people to work untethered from the office, they are learning that people do work when not in the office.

We are learning how to adapt. As we write, law firms are still ensuring law firm stability and business continuity while they institutionalize new ways of working. Ultimately, they will have to survey their progress. It isn't possible to think of everything in a crisis and no plan survives first contact with the enemy. Lawyers will have to review all they have done in the midst of the crisis and find the best practices they have developed and modify or abandon those which have not worked well.

In the end, lawyers have learned that clients want to contain costs and receive exceptional service. Using new ways to practice law can give them both – if we are willing (and we are) to embrace innovation in our thinking. Phone calls are less personal than video conferencing – and personal relationships are what we need to nurture. The best thing lawyers can do today in marketing is call their clients and simply ask "how are you doing?" And then listen, carefully and thoughtfully. It is important that the interests of clients and their lawyers be aligned. We are learning that technology can help do exactly that.

When we look back from a future that it is hard to fully see at this moment, we may be astonished at how this topsy-turvy time catapulted the practice of law forward more in two months than the previous two decades.

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 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.

Ten Cybersecurity Lessons Learned About Working From Home

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

The year 2020 will be remembered as the year that lawyers were catapulted into the future. As a result of COVID-19, the majority of law firms suddenly found themselves thrust into a work-from-home (WFH) environment. Some were prepared for working remotely, but many were not. We've helped a lot of lawyers transition to a different working environment by providing training and implementing new technologies in their practice. Along the way, we've learned some things about how lawyers have responded to the pandemic. Here are ten cybersecurity lessons we've learned about WFH.

1. **Home networks are 3.5 times more likely to have at least one family of malware than corporate networks.** A study by BitSight analyzed data from 41,000 U.S. companies. The study found that 25% of devices (e.g. printers, computers, IoT devices, etc.) on a home network had services exposed to the internet. Another scary statistic is that "Nearly one in two organizations (45%) had one or more devices accessing its corporate network from a home network with at least one malware infection." Ouch.
2. **Sharing the device you use for law firm work with family members is a bad idea.** Devices used to access the law firm network and work on confidential client data should only be used for that purpose. Family members should not be using the same device even if there is a separate login ID and password for the device. If a family member inadvertently performs an action that allows the installation of malware, client data and law firm access could be compromised.
3. **Zoom is currently the choice of clients/potential clients.** Teams, Webex, Zoom, and GoToMeeting are all good video conferencing platforms. The reality is that Zoom is the technology of choice for your current and potential clients. All the other platforms are playing catch-up to Zoom. Despite some early histrionic media reports, you can use Zoom securely for client communications.
4. **Make sure your confidential client conversations are kept private.** Many of us are sharing working space in our homes. As a lawyer, you have an obligation to ensure that client conversations are private. That means

having a separate room to conduct client conversations and consider using a headset too. You wouldn't loudly discuss a client matter while commuting on the train so why would you allow family members to eavesdrop?

5. **Employee security awareness training is more important than ever.** The WFH environment has put law firm employees into situations that carry different risks than when they were in the firm's office. As item #1 in our list identifies, we need to be even more diligent with practicing safe computing. The cyber criminals know there are a lot of targets working from home using insecure home networks, Training employees to recognize the current cyber threats is an absolute must at this time.
6. **Have a Work-From-Home policy.** If you don't already have one, now would be a good time to develop a WFH policy. The policy serves to set employee expectations and what they should and shouldn't do. Specific technology requirements may be part of the policy too. The policy can also have a statement about family use of devices to further support item #2 in our list.
7. **Consider issuing firm-owned laptops so that you control the security of devices used at home.** More and more of our clients are not purchasing desktop computers, opting for laptops (or tablets) with docking stations as the primary computing device. Taking that approach makes it much easier to quickly migrate to a WFH scenario. A firm-owned laptop is configured with the security software and applications the user needs to perform their job. Relocating the laptop to the home network preserves the security of the computer, making it safer to use than the typical home machine.
8. **There are options for home users "competing for bandwidth."** Your spouse is probably working from home and your children may be attending school remotely as well. This means that you are probably sharing the same Wi-Fi network as everyone else and experiencing a slowdown. You may want to try the hotspot on your phone to see if the speed would be better than your home network. Directly connecting your computer via Ethernet to the router will help maximize speed. If you don't have Ethernet cabling in your walls, try using an Ethernet powerline adapter. The TP-Link AV1000 is a good choice and should be around $50 at Amazon, although pricing and availability are all over the place.
9. **Utilize a Virtual Private Network (VPN) for remotely connecting to the firm network.** Using a VPN is better than not using one. A VPN creates an

encrypted communication channel from your computer to the firm network. Many users will be tempted to use Remote Desktop Protocol (RDP), especially since it is included free with Windows. There are many known vulnerabilities with various versions of RDP. If you must use RDP, consider running RDP through a VPN tunnel instead of exposing RDP directly to the internet and by all means, utilize multi-factor authentication (MFA) for any connection.

10. **Prioritize lawyer wellness.** Lawyers in wellness trouble are a security risk. Lack of concentration, mental health problems or substance abuse can cause serious lapses in making smart decisions concerning the use of technology.

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 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 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.*

Working From Home Efficiently, Ethically and Securely

by Sharon D. Nelson, Esq., John W. Simek and Michael C. Maschke

The world is trying to deal with the COVID-19 in a variety of ways. Controlling the spread of the deadly virus is at the top of the list. Travel is being restricted, and some countries have even closed their borders. The United States was slow to react, but eventually states imposed restrictions for business operations to reduce the coronavirus spread and then began re-opening in phases. Social distancing and maintaining clean hygiene practices are the normal mode of operation now. More and more businesses are allowing their employees to stay at home where possible.

What does that mean for the practice of law? How will you meet with clients? Most firms have adopted a telework environment and allow their employees to work from home, even while some firms have begun re-opening. Working from home has different consequences depending on your current capabilities and whether a plan is already in place. While we can't cover all the possibilities and capabilities of every law firm, we'll attempt to attack some of the common considerations.

Equipment

Let's start with a very basic item…the computer. Hopefully, everyone is already using a laptop as their main office machine. As expected, some popular models of laptops are still in short supply. Worst case, you may have to find a Best Buy, Target, Walmart, etc. and see if you can purchase a consumer-grade machine. If you planned properly, laptop users are already configured for remote access. Perhaps now would be a good time to modify your infrastructure plans and budget for laptops and docking stations for those folks that need a mobility option. You may even consider docking stations for home use in addition to one at the office.

Many firms have already adapted and have their employees working from home. Believe it or not, in the early days of responding to the pandemic, some people picked up their work computers, monitors, keyboards and all other peripherals on their desk and took them home. We can't imagine the headaches the IT support people had instructing a user to connect all the cords and devices up properly, not

to mention configuring the desktop to connect to the home network. Our suggestion is to avoid taking desktops home and just deal with laptops and home machines. It will save a lot of headaches, wasted time and support costs. Speaking of home machines…they bring a whole new set of problems and liability which we'll address later.

Many firms are trying to determine when they will resume full or partial operation and have employees return to the office. Some employees are now back at the office but the majority seem to be home (and they have been home for months!) If they haven't upgraded their home work environment, we recommend having an external monitor, full-size keyboard (wireless preferred) and mouse available. You will be much more productive with a full-sized keyboard and a larger screen. Another consideration is printing. Understand that you may need to help your employees configure their home printer (if they have one) to work with the firm's computer. If they don't need to print, so much the better. That should pretty much do it for the hardware requirements.

Workspace

If possible, designate a separate area as your work environment. The space should be away from the kitchen, living room, family room, or other active family areas. If you don't have a desk available, you can always use a table for your work surface. Remember the old days when you fabricated a table using cinder blocks and a board? As mentioned earlier, use an external monitor and full-sized keyboard to create a more comfortable, productive work environment. Consider positioning your work area, so you have a view out of a window if possible. The view will help when you have those periods of mental blocks. Working in a windowless area will make you feel like you're in prison, which isn't a good thing. Of course, maybe it was like that in the office!

Network Connectivity

Many of us have a home wireless network that can be used for our work-from-home (WFH) environment. We recommend avoiding using your home wireless, especially if other family members are also working from home. Besides the security issues, connecting to the home wireless means you are competing for bandwidth with all the other connected devices. Now would be a good time to make sure your home wireless is protected with WPA2 encryption.

We suggest that you connect your computer directly to an Ethernet connection. You can purchase a long Ethernet patch cord if you are not too far away from your internet router. Ideally, you would have a hard-wired Ethernet connection in your house (we do) for your home office. As an alternative, purchase a powerline Ethernet adapter. The adapter provides Ethernet connectivity utilizing the electrical wiring in your house. You plug one adapter in an electrical outlet near your router and a second adapter where you set up your computer. The TP-Link AV1000 Powerline Ethernet Adapter is an excellent choice and is around $55 on Amazon. If you purchase a different model Powerline Ethernet Adapter, make sure the speed is 1000/100/10 and not just 100/10, which may be slower than your Wi-Fi connection. Also, the Powerline Ethernet Adapter isn't always faster than Wi-Fi and is dependent on the electrical wiring in your residence. Having said that, our experience is that the adapters are faster than Wi-Fi in the majority of installations.

If you still want to connection using Wi-Fi, you may consider upgrading to a mesh network. A mesh wireless network has multiple devices to extend the range and speed of the Wi-Fi network without having multiple network names. Amazon eero, TP-Link Deco and Google WiFi are all good mesh network systems.

Depending on your situation, you may need to get re-educated in how to use the hot spot capability of your smartphone. While the connection speed may be a little slower, it's a more secure network than connecting to free Wi-Fi at a Starbucks, McDonald's, etc. Our long-standing recommendation has been to avoid any free Wi-Fi and use your hot spot, even if using a VPN.

Remote Access Software

There are a lot of choices for provisioning remote access. Many firms will already have a VPN (Virtual Private Network) available. Make sure you check the licensing and capacity for your VPN implementation. If your entire firm is working remotely using a VPN, there may not be enough capacity at your office to handle the load. Check with your IT personnel to see if there are any limitations with using a VPN. It's probably a good idea to refresh the procedure for using the VPN with those that will be connecting remotely, especially if they don't regularly access the firm's network with the VPN.

While we're talking about VPNs, not all VPNs are created equal. As organizations increase the use of VPNs for working at home, more vulnerabilities are being discovered. The bad guys are shifting focus to target VPNs since they know so many more users will be remote during the pandemic. In addition, make sure the latest Windows security updates and patches are installed. It goes without saying that you should be using MFA (multi-factor authentication) for your VPN and any other remote access solutions. Have your IT support personnel review AA20-073A: Enterprise VPN Security (https://www.us-cert.gov/ncas/alerts/aa20-073a) from CISA for technical details about using and securing VPNs as a result of the COVID-19 pandemic.

Without getting too much in the weeds, there is a concept with VPNs called split tunneling. Basically, you configure the VPN to route desired traffic through a specific encrypted tunnel. As an example, one tunnel would be configured to send work traffic to your office, and a second tunnel would be for all other internet traffic. This helps reduce the bandwidth requirements at your office as only traffic destined for the firm's network would be coming in. Normally, you would not be implementing split tunneling for a variety of reasons, but now may be the time to change the configuration to allow more capacity since there will be a lot more work-at-home employees.

Some firms will want to enable the Remote Desktop Protocol to connect to their office computers. Words of caution – there is a reason the Remote Desktop Protocol is disabled by default on Windows computers. Generally, it's not recommended to expose your firm's computer(s) to the internet using Remote Desktop Protocol. Larger firms with Terminal Services have controls in place to safely use the Remote Desktop Protocol.

Another alternative is to use a remote-control solution such as LogMeIn. Many of our clients already have LogMeIn licenses available as part of the desktop monitoring solution that we deploy. If you use a remote-control solution, you will have to leave your office computer turned on at all times. We would recommend investigating Control by ConnectWise as a remote-control alternative. You can get the software on a monthly basis and it's a lot cheaper than LogMeIn Pro, which is $350/year.

Larger firms may already have a remote access solution such as Citrix or Microsoft Terminal Services. As previously stated, make sure you have sufficient licenses and bandwidth for all the intended connections, and you have configured MFA for both Citrix and Microsoft terminal server.

Using Home Computers

We understand that not everyone is using laptops as their primary work computer and law firms don't want to spend the money to purchase laptops for remote employees. Many firms want their employees to use their home computers to work remotely. Understand that there are a LOT of issues and concerns when you decide to allow a home computer to connect to the firm network even if you are using a VPN.

The obvious concern is security. The firm doesn't own or control the home machine. You really don't know what security software may be installed or if the computer is fully patched with the latest updates. The reality is that many solo and small firm lawyers will be using home computers to connect to the office.

One of the first considerations is to determine what you will do about the security software on the home machines. Will you allow employees to use their personal security software and enforce it through policy? We would suggest a better approach is to extend your law firm's licensing to the home machines. In other words, make the home machines part of the centrally managed endpoint security system that already exists for the office. Such an approach may not be economically feasible, depending on your size and licensing terms. If you are using an MSP (managed service provider) for your IT needs, you should be able to add licenses on a monthly basis instead of paying an annual fee for each seat, which could get pretty expensive.

Do the employees have the necessary software on their home computers? At this point, you are probably rethinking the options for using cloud services. If you subscribe to Microsoft 365, users could use Office in the cloud or possibly install Office on their home computer. If you use a VPN to connect, does the employee already have the appropriate software installed and configured? Bottom line…you will need to assess what capabilities will be required for your work-from-home employees and address any gaps that may exist.

Another challenge with home machines is the mixing of business and pleasure. Make sure you understand any applicable data protection laws (e.g. GDPR). Using a home computer puts you at risk for exposing client confidential data. It would be a nightmare if you inadvertently shared confidential data using your personal social media account. If you do use your home computer for work, try to limit (or ban) family members, especially children, from using the machine. Family members may be duped into downloading malware that compromises your computer and may transfer to your firm's network.

Telephone and Mail

Don't forget to address how you will handle telephone calls, especially those inbound from current or potential clients. If you have traditional phone lines, don't forget to forward the firm's number(s) to a number that you will be using to answer calls prior to closing the office. If you are not going to forward the number, have a message for callers to advise what number to call and how best to reach you.

The situation is so much better if you have VoIP phones. You should be able to just take your VoIP phone home, connect it to your home network, and it will ring just like it was sitting on your desk. As an alternative, you may have a soft phone available, where you install software on your computer to emulate your desk phone. You would then use your computer sound and microphone (or headset) to answer and make calls.

Don't forget about mail deliveries. Many firms have at least one person at the office to deal with mail and deliveries. The mail may need to be scanned (converted to electronic form) and sent to the appropriate person. Obviously, you'll need a scanner. You may be able to use your copier as a scanner if you don't have a separate scanner. An alternative is to use a scanning app for your smartphone.

Video Conferencing

Instead of face-to-face meetings, many law firms are currently utilizing some sort of video conferencing capability. There are a lot of choices out there to connect with people visually. As a result of the pandemic, many companies are allowing temporary free usage. As an example, Microsoft is offering free usage of Teams

for up to six months. Microsoft 365 subscribers already have Teams included, but we're sure not all your clients are using Microsoft 365.

Zoom is a very popular video conferencing solution. There is a free version that can host up to 100 participants. The Pro version is an affordable $15/month. Of course, many larger firms already have enterprise accounts for services such as GoToMeeting or Webex, to name a couple. Zoom has improved its encryption scheme and now utilizes AES 256-bit GCM encryption just like its competitors. End-to-end encryption will be available for all users (including free users) after the initial beta period, which starts in July of 2020.

To state the obvious, you will need some sort of camera to participate in a video conference call. Most modern-day laptops are equipped with a webcam for video calls. You could even use your iPad or smartphone with some of the video conferencing apps. If your computer is not equipped with a webcam, consider investigating the various models from Logitech. The biggest challenge will be finding someone with webcams in stock since they are in extremely short supply because of COVID-19.

Another consideration is sound. The built-in microphones for laptops or phones may not sound particularly good if you are on the receiving end. Consider using a headset (with microphone) or earbuds. You'll be able to hear better, and so will all the other participants.

Don't forget where you physically sit during the video conference. If your back is to an open window, the brightness may make you difficult to see. Objects behind you may be distracting too. Think about what the person on the other end is seeing. Be cognizant of those around you too. Family members may be able to hear you discussing confidential information even if you are wearing a headset.

Finally, remember the recommendation to connect your computer to a wired Ethernet port? Utilizing Ethernet will significantly improve the stability of your connection during your video conferencing call. The last thing you want is choppy video or garbled audio when you are working with a client or other counsel.

Cloud to the Rescue

Is it too late to move to the cloud? Not in our opinion. Putting your client's confidential information in the cloud brings different considerations for security.

How does the cloud provider protect your data from unauthorized access? Will you need to encrypt the data before you use the cloud service? There are so many great tools available to enhance your law practice.

Cloud-based practice management is a good place to start. We've already mentioned Microsoft 365 for your productivity software. There are options for document management and document assembly in the cloud too. Backups are critical for surviving a ransomware attack. We've always recommended having a local backup and additional encrypted versions stored in the cloud too.

If you are not currently in the cloud; it's probably not a good time to take your critical business functions and move them to the cloud during the current pandemic. However, if you don't intend to return to the office for several months or the balance of the year (or until there is a vaccine), conversion to some cloud services may make sense at this time. Like us, we're sure you can see the value of using cloud services for any future disaster that may come along.

Opportunity Knocks

The cybercriminals never miss an opportunity to profit from a disaster. The coronavirus pandemic is no different. The goal is to target people searching for information about the virus and infect them with malware. Thousands of domain names have already been registered to host malicious websites. The bad guys know that a lot of people are now working from home and have initiated campaigns targeting those remote users. Be particularly vigilant concerning requests to reset your password even if the email looks like it is valid.

Final Tip

If you are not currently participating in a work-from-home environment, you should be planning for it in the future. If you have a laptop as your primary work machine, bring it home every day if you are still going to the office. That way, you'll be ready to respond quickly should the situation change overnight. It would also be prudent to have any needed data readily accessible. Perhaps now would be a good time to have secure cloud storage so you could access the data from anywhere.

Hopefully, your firm has some sort of policy for the changing of passwords. It is no longer necessary to change passwords as frequently as we have done in the past, but they should be changed periodically for the time being. There is no reason

these days to change your password at intervals of less than 90 days. No matter what your password expiration policy is, if you have closed your firm, you should have changed your password prior to leaving the office and starting your work-from-home experience. Changing the password will reset the timer so that it hopefully won't expire while you are not physically connected to the firm's network. Contact your IT provider for instructions on how to change your law firm's network password while working remotely.

Final Thoughts

As we mentioned at the beginning, it would be impossible to address every situation a law firm may encounter during the pandemic. Hopefully, some of our suggestions and recommendations will assist in your practice and allow you to serve your clients well and securely in these difficult times. Be safe out there.

Sharon D. Nelson *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*.

Michael C. Maschke *is the CEO of Sensei Enterprises, Inc. He is an EnCase Certified Examiner, a Certified Computer Examiner (CCE #744) a Certified Ethical Hacker and an AccessData Certified Examiner. He is also a Certified Information Systems Security Professional.* *mmaschke@senseient.com*.

Ransomware as a Data Breach: An Evolving Threat

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

It is hard to believe there was such a thing as "the good old days of ransomware," but we might be forgiven for looking back nostalgically. While ransomware was a bloody nuisance, law firms generally felt protected if they had a well-engineered backup system to facilitate recovery.

With multiple backups, usually in the cloud, or (with small firms) on two or more external USB drives, you could ignore the badgering requests to pay the ransom, the clocks counting down to when your data would be totally inaccessible, etc.

The trick was always to have multiple backups so that a single backup solution didn't leave you vulnerable to having all your data encrypted if you were struck by ransomware while backing up. Having that "virgin" backup meant you could restore the data. This of course assumes that you regularly performed test restores on your backups to make sure you could indeed restore data from them.

Good guys, 1 — bad guys, 0.

The exception was often in the health-care industry, where lives were at stake and taking the time required to restore data might cost lives. Often, those entities paid up—and once the cybercriminal discovered that, health-care entities were targeted.

If you are scratching your head about all the state and city governments that were brought to their knees by ransomware in the last two years, you should know that their backups were not properly engineered. In fact, they were a mess. The cleanup took forever and cost millions of dollars. Many local and state government agencies never understood what constituted properly engineered backups—nor did they budget for it. Even now, they are more likely to get cyber insurance to cover the risk than to adequately address the baseline problems.

Cyber Incidents vs. Data Breaches

Fast-forward to December 2019 when ransomware gangs upped their game and began to threaten that they would "out" the data of those hit by ransomware if they didn't pay the ransom.

That altered the previous rules of engagement—and it meant that they had exfiltrated (taken) the data before encrypting it.

Previously, it was generally safe to say that ransomware attacks were only rarely data breaches—mostly they were cyber incidents. Your data was encrypted but not exfiltrated. What did that mean? You didn't need to report those incidents under state data breach laws or under many other laws/regulations.

Innocent days indeed. Ransomware cybercriminals are upping their game—some say they will begin publishing data taken from entities that don't pay the ransom. To the horror of victims, one ransomware gang now has a public website naming entities that have restored their data and reconstructed their systems instead of paying the ransom. For the moment, information given for each Maze victim comprises the date of infection, the size of files supposedly taken from victims (in gigabytes) and a handful of stolen Microsoft Office, text and PDF files. Also identified are the IP addresses and machine names of the Maze-infected servers.

In fractured English, the site says, "Represented here companies don't wish to cooperate with us, and trying to hide our successful attack on their resources. Wait for their databases and private papers here. Follow the news!"

Yes, indeed, we will be continuing to follow the news. If the Maze tactic is successful, this is very bad news for law firms, which have almost invariably regarded ransomware infections as a security incident and not a breach.

Did We Have Warning of this New Ransomware Tactic?

From our foxhole, the strictly correct answer is no. Until the recent news broke, we had not heard a specific case of data being exfiltrated. But we had thought about it. It seemed logical to us that bad guys who would demand ransomware to get your encrypted data back would be very likely to take your data before encrypting it.

There is, after all, no great honor among thieves. We ultimately concluded that the only thing stopping them from taking data (as an insurance policy for getting

payment, if nothing else) was if the exfiltration could be traced. And there's the rub—maybe it could be traced, maybe not. But we fretted over it—and thought that the smarter cybercriminals might indeed be able to erase their tracks.

Law firms were happy to hang their hat on the most convenient nail—and that meant that there was no evidence of data compromise (but did they look for evidence?) and they didn't need to report data breaches. Convenient thinking, but in light of the new threats, we believe law firms need to take ransomware much more seriously than they have in the past. Frankly, many law firms do have well-engineered backups and could return to full functionality fairly quickly after a ransomware infection. And that's where they wanted the story to end.

It appears we should have worried more. Lawrence Abrams, founder of the computer security blog and victim assistance site BleepingComputer.com, recently said in his blog that the bad guys have warned us about this problem: "For years, ransomware developers and affiliates have been telling victims that they must pay the ransom or stolen data would be publicly released. While it has been a well-known secret that ransomware actors snoop through victims' data, and in many cases steal it before the data is encrypted, they never actually carried out their threats of releasing it."

Well, it wasn't a well-known secret to us or to many of our colleagues. But OK, let's start from where we are today.

Does Your Law Firm Have a Managed IT Services Provider?

It gives us no pleasure, as a managed IT services provider (MSP) ourselves, to report that MSPs are being targeted by ransomware groups. MSP Synoptek was hit in late December 2019, with many of its more than 1,000 customers having their services disrupted. The company has reportedly paid a ransom in an attempt to restore services as quickly as possible.

In October 2019, law firms using cloud-based TrialWorks case management software lost access to their legal documents for four days after TrialWorks was hit with a ransomware attack. Several of our friends were near hysteria, severely crippled by the inability to do their jobs.

TrialWorks serves roughly 2,500 clients. It did not own up to the attack publicly but did email customers assuring them it was "actively decrypting and restoring data," which implies to us that the ransom was paid.

As of October 2019, 13 managed services providers or cloud-based providers (including TrialWorks) were victims of ransomware attacks causing serious outages to their customers.

There is certainly a lesson here: "This uptick in successful ransomware attacks against MSPs and/or cloud-based service providers is a harsh reminder that organizations have to ensure that the third-party vendors they do business with are as equally protected against the current and emerging cyber threats as they are," said Chris Hinkley, head of Armor's Threat Resistance Unit research team, when he spoke to SC Magazine. "This is especially true because, as we have seen, a successful ransomware attack against an MSP/cloud-based service provider can be debilitating to their customers, as well as to their own company, as the attack can quickly shut down key systems which the customers depend on to run their organization." Yet another reason to check your cyber insurance for coverage of third-party providers.

"And of course, a ransomware attack against an MSP can be fatal, putting an MSP out of business," Hinkley added. He was referencing PM Consultants, an IT consulting firm and support provider for dental practices. The firm shut down in July 2018 after being devastated by ransomware.

So Where Are We Now with Ransomware?

"Ransomware attacks are now data breaches," Abrams said. "During ransomware attacks, some threat actors have told companies that they are familiar with internal company secrets after reading the company's files. Even though this should be considered a data breach, many ransomware victims simply swept it under the rug in the hopes that nobody would ever find out. Now that ransomware operators are releasing victims' data, this will need to change and companies will have to treat these attacks like data breaches."

In case law firms need more bad news, cybercriminals responsible for managing the "Sodinokibi/rEvil" ransomware have indicated that they will follow Maze's course of actions.

This is dreadful news for entities that are very likely facing major fines and other penalties both because they didn't report data breaches and didn't appropriately safeguard customer data. Though most lawyers don't know it, health-care providers must report successful ransomware attacks to the U.S. Department of Health and Human Services.

Final Thoughts

To be frank, the ransomware incidents we've seen previously gave no clue that data had been taken before being encrypted. It is impossible to know how often this was done in the past. Some folks have said publicly that it was an open secret (but we never heard it!). If this tactic becomes the norm, then Abrams is right—ransomware attacks may need to be treated as data breaches and reported. Digital forensics teams may need to be deployed to determine if data was exfiltrated before it was encrypted.

This is a serious game-changer. We have already revised/updated almost all of our cybersecurity PowerPoints!

As we were about to finish editing this column, Reuters reported that cyber insurance companies are increasing their cyber insurance rates by as much as 25 percent—a very large hike! It also reported that the average ransom requested to decrypt files tripled from the first quarter of 2019 to the third quarter. The average ransom was a hefty $41,198 and it doubled again in the fourth quarter to $84,116, a sticker price far beyond the reach of solo and small law firms!

If your law firm hasn't given serious thought to how it will handle a ransomware infection in the future or how it should adjust its incident response plan and its BYOD (bring your own device) policy (we told you in previously columns that acronym really meant "bring your own disaster"), time to roll up your sleeves and get to work.

Sharon D. Nelson *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.*