Three Compelling Reasons for Solo and Small Firm Lawyers to Understand Their Technology

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

Let's dive right in. If lawyers understand their technology . . .

Lawyers can save money

Serious money can be saved if you don't listen to a vendor peddling snake oil at a conference or an IT consultant whose prime concern may not be your wallet/purse. When you learn about technology, you at least know the right questions to ask. You may not know enough to make the decisions and you may still need guidance, but you may know enough to be a "BS filter." And once you smell that bull, you'll know you're talking to the wrong person. That is very useful in and of itself.

An example: If you hear someone telling you that Apple devices are inherently secure and that you don't need security software installed on them, do not listen to anything else that person has to say. You have just established that they are not credible. And we mean no offense to Apple, which has upped its security game in recent years and now itself advises users to install security software. But old legends die hard.

Another example: A vendor tells you that a piece of software will make your device 100% secure. That software doesn't exist, so leave that huckster to fleece someone else.

Once you know about technology, you will understand that you need a business class device but you also understand that you don't need a whiz-bang gaming computer or the Cadillac of computers. There is always a "sweet spot" in legal tech, balancing all the stuff you really need with cost. Understanding more about that technology can help you identify that sweet spot – or recognize that the consultant you are talking to is try to guide you to that sweet spot. That's the kind of help you need!

When you understand something about your technology, you can also budget for tech upgrades, knowing (as you do from reading this article) that a four year cycle of refreshing technology is about the average. You certainly don't want to find yourself at a point where a "big bang" replacement is required. Spread the pain over time. Not only does this allow you to budget better, you are less likely to have a catastrophic failure from using old, unsupported equipment or software.

Lawyers can make their practices more efficient

As our friend Jim Calloway likes to say, every law firm is a technology business. It is true that we are all dependent on our technology. But in a world where competition for legal work has gotten . . . shall we say **intense . . .** the smart lawyer is eyeballing technology all the time to see how to make the practice of law faster and more efficient – which appeals to clients because the work is done more quickly – and (ok, a bit painful, this part) more cheaply.

The truth is that keeping clients and attracting new clients requires more efficiencies and lower prices. That is what budget-conscious people and companies are searching for. And that is precisely what alternative legal providers are offering. We have pretty much given up the battle of fighting alternative legal providers, so now we are in the position of competing with them. Of course, you can leverage their technology and work for them, but your effective income (and independence) will wane. Perhaps ok if you are trying to gain experience, but not what most lawyers want.

If you invest some time in understanding technology, you can find ways to keep yourself not only in the game but competitive. Your technology becomes a selling point. As an example, law firms are flocking to client portals, which clients adore – they can securely and in real time see the status of their cases, correspondence, bills, etc.

We know many lawyers who wistfully say they want a client portal but don't understand them, how they work, how to select one, etc. That knowledge can be gleaned from spending a little time with several client portal vendors on test drives.

Lawyers can make their data more secure

Without question, 2016 was the year of the law firm data breach. Lawyers pretty much quit arguing with us about the increasing need to pay attention to security during that year. They began doing security assessments, often at the insistence of clients or insurance companies and they were appalled to find, when they sat down with us to answer assessment questions, that they not only didn't have the right answers but they didn't even understand many of the questions.

With 27 states having adopted some variant of the ABA Model Rules of Professional Conduct changes to Rules 1.1 (Competence) and 1.6 (Confidentiality), lawyers began to fret, and rightfully so, that not paying attention to cybersecurity might be an ethical violation.

We began to see audiences growing in cybersecurity CLEs – and lots of questions asked. That's a good thing. Going to CLEs presented by law firm cybersecurity experts is an excellent way to learn – and there are plenty of webinars available as well. There are books as well, several of them published by the Law Practice Division!

The #1 answer to most basic security questions is "encryption is your friend." Strong encryption has not been broken, even by the NSA or CIA. Your laptops, computers, tablets, smartphones and backups should all be encrypted.

Lawyers believe encryption is hard. It used to be, but no longer. You don't need to understand the mathematics behind encryption, you just need to have an IT pro get encryption set up. For example, if you need to encrypt e-mail, you can install and use a product like Mimecast Secure Messaging (which we are seeing more and more in law firms) and encryption is as simple as clicking on an "Send Securely" button – from within Outlook. If you want to encrypt an attachment (Word or PDF) just put a strong "open" password on it (simple instructions can be found in "Help") – just don't put the password in the accompanying e-mail. Yes, we've seen that. Good grief. And it's not unaffordable. Promise.

When you understand security, you know how to plan security policies. Do you really want employees' personal devices connecting to your network? You need to understand the potential dangers and possible solutions to answer the question.

When you understand your technology, you can see what you can control via technology and help to fill the holes by sensible law firm policies and employee training. Nothing's foolproof but the magic in cybersecurity comes from technology, policies and training – and the remaining risk is passed off (hopefully) to your insurance company. Make darn sure you know what it covered if you have a data breach!

Conclusion

What we see, all too often, is lawyers confused and bedeviled by their technology. We hear you when you scream “I just want it to work!” But if you expend some serious effort in learning about your technology, there is a process of demystification that takes place over time – you’d be amazed at how much you can accomplish by yourself. And never be afraid to Google a question or search YouTube – you’d be astonished how many questions can be asked and answered by reputable sources!

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