

How Lawyers Can Manage Their Technology Well

by Sharon D. Nelson and John W. Simek

© 2015 Sensei Enterprises, Inc.

Can lawyers actually manage their technology (instead of it managing them)? Buying, implementing, replacing and securing technology are huge challenges – especially when you have billable work to do. And yet, technology is the most important part of a law firm today – at least after the carbon-based units!

What are lawyers doing wrong?

Rare is the solo/small firm which does an annual review of its technology. Firms tend not to plan, but rather to buy technology when a new need arises, when a partner demands the latest cool tech toy, or when something breaks. In our world, we call that the “Break/Fix” method of (not) managing technology.

For the most part, lawyers don’t even have a list of all the equipment they own. They don’t know when it was placed in service - they may think about this briefly in terms of depreciating capital expenses at tax time, but not in terms of planning to replace technology.

And, God help them, they often listen to a vendor they just happen to run into at a conference or someone who persistently stalks them with a deal that sounds too good to be true (hint: it is). A lot of decisions are made quickly because lawyers are in such a hurry to get back to practicing law. Understandable, but it often results in poor decisions being made.

Getting yourself organized

First, let’s stress an important point: Technology has a life span. For most computers, laptops, tablets, smartphones, etc., that tends to be about three years. That does NOT mean that the devices will cease to work. It just means that we tend to replace them that often because performance will deteriorate as we ask more of our devices (specifically when software asks more) and because we tend to want/need new features in our technology. You may be able to stretch the lifespan of some equipment – servers, printers, multi-function machines, etc. -to five years.

Second, let’s acknowledge that lawyers are terrible about budgeting. Make yourself a list of all the equipment you own, when it was placed in service and who has the devices (this will need updating each year). For the most part, experts recommend that you plan on refreshing your technology, with the exceptions mentioned above, every three years. That means you need to budget for replacing 1/3 of your technology each year. At the outside, budget for replacing ¼ of your technology each year.

The ultimate and often seen nightmare is a “big bang” purchase of almost all the technology because everything is so out-of-date. This is a major hit to the law firm wallet. It is far less painful to do this over time.

And don't be cheap in your buying decision because you'll regret it – lawyers need “business class” machines which can handle a lot of software being used at once. As we have wryly observed, lawyers have zero patience with slow computing.

Hopefully, you have a relationship with a trusted IT consultant. Listen to the consultant when it's time to purchase. Don't just willy nilly buy things because you think you've found a great deal or because a vendor promises you the moon for a song. Your colleagues can be a good source of validation as well. But know what you don't know and find someone who can lend a hand. Remember that Model Rule of Professional Conduct 1.1 now includes being competent with technology. If you are not, find someone who is (and if you find competence – hold it close, because it is darn rare).

Kick the Tires!

It is rare to find software that doesn't come with a 30-day free trial, so for heaven's sake kick the tires first and see if the software will work for you. Just as you might explore a lot of houses before you find the one you want to call home, you need to be comfortable (especially with an expensive or significant-to-your-practice purchase) that the product is a good fit for you.

If there's not a 30-day free trial, the odds are good that you can get an online demo – those are also very instructive – and you can ask tons of questions or ask to have particular features demonstrated.

Try before you buy – and *caveat emptor* because the legal tech world is full of snake oil.

Security and Ethics – It's a New World

If you haven't read the changes to Model Rule of Professional Conduct 1.6, including the comments, now is a good moment to make a strong cup of coffee and do so. With the tsunami of data breaches that we've seen in the past couple of years, even staid and traditionalist law firms have awakened with a start and are scrambling to shore up their data security.

The #1 answer to most basic security questions is “encryption is your friend.” Strong encryption has not been broken, even by the NSA. 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 a product like Zixcorp (which we are seeing more and more in law firms) and encryption is as simple as clicking on an “Encrypt and Send” 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.

In all aspects of your tech planning and review, consider security. Want to allow employees to bring their own devices and connect to your network? Bad idea. They may be carrying malware and infect your network. Is BYOD (Bring Your Own Device) cheaper? NEVER if you have a data breach. We've heard folks argue that mobile device management solves the problem. Maybe, but the price of that

management has soared in the past several years – far beyond the reach of small law firms. Buying and issuing work devices makes the management of their security far easier – and employees have nothing to say about how you choose to manage them.

If your firm has a wireless network, it should also have a guest network that keeps folks away from your business network. Easy peasy for your IT consultant to set one up.

To Cloud or Not to Cloud?

Every state that has weighed in on lawyers using the cloud to store data has fundamentally said it is fine, so long as the lawyer is reasonably careful to ensure the security of the data. We still have a lot of hold-outs who are not comfortable with the cloud. We were long called (with good reason) “cloud curmudgeons” – but we finally came around to the stark realization (hat tip to Jim Calloway here) that most clouds protected data better than most lawyers.

Still, to return to our “encryption” theme, it is important that you make sure that your confidential data is protected. That means that the data has to be encrypted in transit and at rest. MOST IMPORTANTLY, you have to be the one who holds the decryption key. In the case of the iCloud, Dropbox, OneDrive, Box, Google Drive, the terms of service make clear that these providers have master decryption keys. This is one reason we like SpiderOak, which is designed so that it has “zero knowledge” – you have the only knowledge of the decryption key. Sure, if someone shows up with legal paperwork, they can give them data, but it’s fundamentally garbage because it’s encrypted with the user’s encryption key.

Final Thoughts

Clearly, we could go on and on about managing technology. The real point here is that technology should indeed be managed – and this is not an ad hoc process. If you haven’t gotten your arms around a process for managing your technology, it’s time to roll up your sleeves and get to work!

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