

IT Managed Service Providers – Nearly an Imperative

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

© 2017 Sensei Enterprises, Inc.

Legal IT – A brief history

For more than 20 years, the authors have been providing IT services to law firms. Ah the good old days, when life was simpler. Here's how IT once worked. We would get hired, generally to install and configure computers, servers, etc. Once our initial work was done, do you know what we would do? We would wait for the phone to ring. Perhaps something wasn't working or perhaps the client needed training. Now and again, they would get upgraded hardware or software. Most clients would have us do updates on a regular basis – in those more primitive times, perhaps monthly. Most IT work was called “break/fix” – if something didn't work, we fixed it. And there were of course occasional projects . . .

Fast forward to today, when almost all businesses, including law firms and other legal entities, are turning to managed service providers.

Managed Service Providers (MSPs)

Today, only the smallest of firms tend to operate without a managed service provider. The reason is simple. The world has gone and gotten itself a whole lot more complex. It's not enough to fix things that are broken. We need to prevent problems proactively. We need to monitor our networks constantly. Clients are demanding that law firms do a reasonable amount to secure their confidential data – and the ethical rules demand that they do that – so MSPs have become a large part of the answer to safeguarding client information.

There are threats to law firm data everywhere – disgruntled employees, hackers, nation-states, etc. – and their tools are more advanced. Ransomware has fueled the need for carefully engineered backups which are impervious to ransomware. Vulnerabilities in software and hardware abound. The failure to patch software and hardware promptly is rampant. People lose their devices (or have them stolen) at alarming rates.

Data leaks used to be a relative trickle – and now they are a raging river. In response, managed service providers emerged on the IT landscape and began to monitor everything on a 24/7 basis. They automated patching, instituted backups that “report back” any issues, automated malware detection, installed intrusion detection systems and began receiving system-generated alert of possible intrusions or “anomalies” in behavior. When malicious files were detected, smart systems refused to allow you to open them.

As we have learned to our chagrin, our greatest asset (our employees) are also our greatest danger. Software now helps to protect people from themselves.

The Benefits of Managed Service Providers

Guess what? Most lawyers hate technology. All they want is for it to work. Period. They have hated managing technology. Provided that you have a competent MSP, you can pretty much divorce yourself from day-to-day technology management. This is a good thing on many levels, but it is certainly true that most lawyers who try to be the firm's IT director are absolutely terrible at that job. And no wonder – this is not their core competency. That's why they went to law school!

Yes, you will probably pay a little more to get an MSP. But you know what you'll get back? Time, lots and lots of billable time. Depending on how negligent you were in a previous technology life, you may even pay less since problems will be detected before everything melts down.

Unlike the old days, you won't take your server and stick it in a room, hoping it will continue to function. Your MSP will load a variety of agents on your server which will fundamentally monitor its health, right down to how much free disk space you have remaining. Your MSP will be able to give you reports on software resource hogs and warnings when you may need to replace the server or expand its capacity. These early warnings will allow you to budget for the money to do whatever needs doing and to set aside the time for it to be done – often during off-hours so productivity is not impacted.

Your systems, automatically patched and updated, will now run optimally. What do lawyers hate? Downtime. What do they love? Uptime. The greater the uptime your systems have, the more profitable you are.

Cybersecurity

We alluded briefly to cybersecurity above. So now that you've reasonably fulfilled your ethical duties (and client demands for cybersecurity), you know what you now have? One of the world's best marketing tools. Law firms regularly trumpet their cybersecurity measures today, eager to provide reassurance to anxious client or potential clients.

Don't hesitate to make use of all the advantages an MSP provides. Go ahead and have a cyber-audit done, preferably by a third party. Not only will clients and potential clients be impressed with a good report, you may well get a discount on your cybersecurity insurance. And doggone, that insurance is not cheap.

As we often say, law firms have data on many individuals and businesses; hence, they are especially valued targets, frequently the "soft underbellies" of their clients who may have far more extensive cybersecurity in place. And law firms hold a lot of PII (personally identifiable information) as well as a lot of regulated data (SOX, HIPAA, Gramm-Leach-Bliley, etc.) Fines and penalties for not adequately securing data can be stiff.

Recognizing that an advanced hacker with sufficient skill and funding WILL get into your network, you need to have systems in place to detect and immediately report a breach. MSPs can provide you with proactive security monitoring which will detect all kinds of potential

trouble, including firewall services, anti-malware software and software which operates utilizing heuristics, watching how something behaves to determine whether it is a potential danger. In other words, if it quacks like a duck and walks like a duck, it must be a duck.

There is no silver bullet to ensure cybersecurity, but practicing lawyers are not in a good position to protect the firm's data. A qualified MSP – and make sure it has cybersecurity certifications since most don't – is a far better alternative.

No MSP worth its salt is going to agree to manage an antiquated system. So if you've been ignoring upgrades for a while, do not be surprised if a qualified MSP requires you to upgrade your systems before taking you on as a client. If you're behind, you'll need to spend money to catch up – and that's a good thing!

What does an MSP Cost?

The very unsatisfying answer is that costs can be hard to determine. Usually there are monthly charges – and you may have to agree to be locked in for a year because the MSP may be locked in for the same time period with some of its service providers. We would resist being locked in for more than a year, having seen unhappy “marriages” drag on miserably for as much as three years. On top of that there are charges for project work – when systems are upgraded either at the outset or as time goes on. And though you have paid for the 24/7 monitoring, if alerts require work to be done, that work is billable.

Is there an alternative? Of course. You can pay for both monitoring and support. Most often, this will entitle you to monitoring and remote support, but those pesky onsite visits will still be billable. Clearly, this option costs more.

Probably the most common pricing structures involves charging for monitoring and full support by device. Obviously, servers cost more than desktop computers to support. Some people swear by this model, but we often find that they are paying for support they aren't using. From the vendor's point of view, that makes good financial sense. From the law firm's point of view, not so much.

There is also a per-user model. Since most users have three or more devices, the per-device pricing model can get, well, pricey. This is theoretically taken into account by charging per user. Again, we have some skepticism about this.

There is also a model which includes all monitoring and support for a flat fee. Once again, we think you are often paying for support you don't receive. We prefer the monitoring only (cheapest, often even with support added on top). Pay for what you need in terms of support. You may be pleasantly surprised to find that you are paying less than some of the other plans you are offered. Obviously, there is an element of uncertainty here – and that's why some law firms prefer to budget with certainty – we just think they are often overcharged.

Remember that buying new equipment is not within the definition of “support”. That you will be charged for, just as you would be charged for equipment relocation or upgrading (not patching) software.

Law Firm Specific MSPs

The best of all worlds may be an MSP which specializes in law firms, but one that has considerable experience with law firms may be good enough. Make sure you verify that the MSP does have sufficient law firm experience and do check out the law firm references asking hard questions! You want an MSP that is familiar with legal ethics and commonly used legal software.

Parting Words

Automating processes as described above is good business sense. It is more efficient – and in the case of cybersecurity, safer. But bear in mind the words of our good friend Barron Henley (who phrased it more strongly than what is printable), “Decrapify processes before you automate them.” Make sure the MSP you hire understands how to do that!

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