Ethical and Budget Friendly Cybersecurity for Solo Lawyers

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

Current Climate

We are a very mobile society and our technology usage seems to increase with every passing day. Lawyers are no different. It is not uncommon to use the cloud for the practice of law using services such as practice management, document management, file storage, and multiple ways to communicate with clients. Solo attorneys in particular have embraced cloud services. The cloud has provided a secure, stable, cost-effective way to practice law.

While cloud vendors are better equipped to secure data than the typical lawyer, you still need to take reasonable steps to protect the technology you use to connect to the cloud provider. These days, it is particularly important to be very vigilant as the cybercriminals have increased attacks on home networks and those in the work-for-home environment. Even though home networks have been shown to be 3-1/2 times more vulnerable than law firm networks, there are very affordable actions the solo attorney can implement to improve their cybersecurity posture.

Ethics Considerations

One of the key requirements for all lawyers is to protect client confidential information. There is also an obligation to be competent with technology. We find that most lawyers don't know that there is also a requirement to monitor for data breaches. Not to worry. We're going to discuss some budget friendly solutions to help solo attorneys comply with their ethical duties, especially as it relates to cybersecurity.

Encryption

Encryption is your friend when it comes to protecting client confidential information. Whether the data is being sent in some communication stream or stored on devices, there are very affordable solutions to encrypt and protect the data. Microsoft and Apple provide encryption capability natively within the operating system for no additional charge. If you are a Windows user, make sure that BitLocker encryption is enabled. Apple users should enable FileVault 2 within the operating system.

To communicate securely with clients, consider using the client portal supplied with your cloud-based practice management solution. Client portals make it easier to communicate securely with clients and avoid the need for sending encrypted email. If encrypted email is needed, there are a couple of budget friendly solutions for solo attorneys.

Email encryption can be added to your Microsoft 365 subscription if you are not subscribing to the E3 or higher versions. There are third party solutions to provide email encryption as well. We recommend Proofpoint as an email encryption add-on service.

Multi-Factor Authentication (MFA)

You should enable MFA for every account and service that you use, whether for your law practice or personal use. Microsoft includes MFA with all of its Microsoft 365 subscriptions for no additional charge. However, it is not enabled by default.

You should also investigate MFA options for other services you use. Apple users should configure MFA for your Apple ID and iCloud access. Many of the practice management solutions support MFA too. As an example, Clio supports MFA using Google Authenticator. Install and use one of the free authentication apps such as Google Authenticator, Duo or Authy.

Many services support authentication apps, which are more secure than using SMS text messages for the second factor. Having said that, using SMS text messages for 2FA is FAR better than not having 2FA enabled at all. Bottom line…Microsoft's study of MFA has shown that it stops 99.9% of credential based account takeovers. In the words of Nike, "Just Do It!"

Next Gen Security Software

Every computer (and mobile device too) should have some form of security software installed. There are a lot highly rated anti-virus applications that do much more than just protect against virus infection. Without getting into specific recommendations for a vendor, any of the products from reputable manufacturers is fine. We would recommend against using any of the free security software and sticking with the paid versions.

The traditional anti-virus products are not very effective at combating ransomware attacks. That doesn't mean you don't need them. There is another product that should be used in conjunction with anti-virus products. As a general term, the next generation software is known as Endpoint Detection and Response (EDR). EDR solutions are particularly effective at dealing with modern day attacks.

EDR uses much more sophisticated technology such as artificial intelligence, machine learning, heuristics, etc. Essentially, the software constantly analyzes the device activity to create a "baseline" of what would be considered to be normal usage. If some abnormality is observed, EDR can take a variety of actions such as killing processes, quarantining files or even automatically disconnecting the device from the network.

Some EDR solutions work with a SOC (Security Operations Center) to add a human element to the analysis. Some also have the ability to roll back the computer to a known good state prior to the attack.

EDR is not just for large scale enterprises. While some do require minimum license counts (hundreds or thousands of devices), there are EDR products that are very affordable for the solo attorney. We recommend investigating the SentinelOne EDR product. You do have to acquire SentinelOne through a reseller, but you should be able to pay less than $15 per month per machine. Considering how effective EDR is with ransomware attacks, we feel EDR is now an ethical requirement to protect client confidential data.

Monitor for Data Breaches

Few lawyers seem to be aware of the need to monitor for data breaches as stated in ABA Formal Opinion 483. One way to provide monitoring is to implement an intrusion detection system (IDS) or intrusion prevention system (IPS). Fortunately, there is a solution to help solo attorneys meet the obligation to monitor. One option is to investigate the Meraki line of products from Cisco. The Meraki is an edge device firewall that can also have wireless access point capabilities and include an IDS/IPS.

A sufficiently sized Meraki device for a solo lawyer only costs $300-$400 as a one-time purchase. The software is licensed on an annual basis. A three-year license term will get the annual cost down to

around $350, making the Meraki a very affordable piece of invaluable technology. The Meraki can be configured to automatically alert you to any attacks and/or attempted data breaches.

Summary

We could go on and on with additional suggestions for budget friendly technology for the solo lawyer to improve their cybersecurity posture. As can be seen, the previous recommendations won't break the bank and are certainly reasonable steps to meet your ethical obligations.

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*.