# The NEW Best Cybersecurity Bang for Your Buck: A Guide for Solo/Small Firms

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


Has your New Year's resolution to up your cybersecurity game turned to dust? Don't let that happen – there's still time in 2024 to address your cybersecurity posture. As readers know, lawyers have an ethical duty to protect the confidentiality of client data. That means preventing unauthorized access. It is a well-known fact that cyber-attacks rose significantly in 2023, therefore requiring particular vigilance when addressing cybersecurity. It didn't help that the class action law firms began going after breached law firms last year. That has intensified the resolve of law firms to up their cybersecurity game.

However, upping your cybersecurity game is particularly challenging for solo and small firm lawyers because funds available for cybersecurity are often limited. So where should you invest your hard-earned dollars? The authors do cybersecurity for a living and are devoted to providing budget friendly solutions for the solo and small firm attorney. We'll give you a few suggestions for the best cybersecurity bang for your buck and a suggestion to help you prepare for the future of constantly evolving cyber threats.

## MFA Everywhere!

Going once. Going twice. Going three times. The winner is MFA. Multi-factor authentication (MFA) is by far the top choice among all of our recommendations. According to Microsoft's data analysis, implementing MFA will stop 99.9% of credential-based account takeovers. Considering that MFA is generally a no cost solution, you can't get much more bang for your buck.

Put simply, MFA is another factor used to log on to an account or access a service. The default MFA for most systems is delivery of a code via SMS text message. In other words, you log on (step one) and a code is sent via text to your phone. You then enter the code to the system (step two) in order to complete the logon process.

Of all the MFA delivery mechanisms, SMS text is the least secure. Even though it is not as secure as other delivery methods, it is FAR better than not having any MFA at all. So if text is your only choice, by all means use it. A more secure method is to use an authentication app (e.g. Google Authenticator, Microsoft Authenticator, Authy, Duo, etc.) that generates a code every 30 seconds. Instead of entering the code received in a text message, you enter the code that displays in the authentication app. If you have a choice between text messages and authentication app, choose the app. An even more secure method is to use push notifications to the authentication app. Finally, the most secure MFA method is to use a physical token such as a YubiKey.

We know some of the language about MFA is foreign, especially to solo/small firm attorneys, but a little extra research online will quickly help you understand MFA and how to implement it. Guidance from whomever provides your cybersecurity support is recommended.

## Recover from Ransomware

In addition to death and taxes, one more thing you can count on is the continuation and escalation of ransomware attacks. According to the Verizon 2023 Data Breach Investigations Report, ransomware was involved in 24% of data breaches. The attacks may not specifically target your law firm but may be introduced via a supply chain attack. In other words, you may be compromised because of some product or service you use in your practice. Bottom line…maximizing your ability to recover from a ransomware attack should be at the very top of your cybersecurity budget.

Making sure you can restore your data following an attack is key. The whole point of ransomware is to encrypt your data so that you pay a ransom to get the decryption key in order to make your data accessible again. If you have a good backup to restore from, then you won't have to pay a ransom for a decryption key. Just restore the data and you're back in business. Today's problem is that current ransomware attacks look to destroy your backups so you can't restore the data. This means you need to engineer your backups to be resistant to ransomware. There are many ways to accomplish this, but we'll concentrate on lower cost alternatives for the solo and small firm lawyers.

A lot of solo/small firm lawyers use external USB drives to backup data. External USB drives are a cost-effective way to have good backups. However, you should have at least two drives and make sure you disconnect them from your computer once the backup is completed. If the drive is connected, it may get encrypted as a result of ransomware. In addition, sending backup data to the cloud (e.g. Carbonite, Mozy, Backblaze, etc.) should also be considered. Even in the cloud, you need two backups, one of which is not connected to your network – it's a piece of cake for the attackers to destroy backups that are connected to your network.

One last item to consider when designing backups to be ransomware resistant is immutable storage. Basically, immutable data can't be changed or deleted for any reason for some period of time. The ability to have immutable data is most commonly found in cloud backups. You can set an expiration date after which the immutability is removed. Think of it as a litigation hold where data can't be deleted or changed until after the matter is completed.

## EDR, XDR and MDR – Oh, my!

We fully understand that the header above is headache-inducing. Read this portion of our article slowly because it is invaluable in protecting your data. One best bang for the buck is the new breed of security software known as Endpoint Detection and Response (EDR). You may also see the software marketed as Extended Detection and Response (XDR) or Managed Detection and Response (MDR). EDR is the next generation or endpoint protection and uses advanced technology such as artificial intelligence, machine learning, heuristics, etc. to analyze activity and take the appropriate action when suspicious activity is discovered. For example, transferring a file from the internet without any human interaction might be suspicious causing the EDR software to stop the transfer and/or quarantine the downloaded data.

EDR software is particularly effective in combating ransomware. When files begin to be encrypted in a systematic way, the process can be terminated, and the offending programs quarantined to prevent further activity. EDR can go even further and automatically disconnect the computer from

the network to prevent spreading malware to other systems. Some EDR software can also roll back the computer to a known good state (e.g. 10 minutes before the ransomware attack).

There are many affordable EDR solutions that fit the budgets of solo and small firm lawyers. You should be able to implement quality EDR software for around $10-$15 per endpoint per month. We highly recommend implementing some sort of EDR software for all your endpoints. Cyber insurance companies are increasingly asking about EDR in your environment. EDR may even be considered an ethical requirement, especially since it is so affordable and a very reasonable solution to protect your data from ransomware attacks.

## The Future is Here

Finally, what other cybersecurity measures should you be taking for the future? The short answer is *Zero Trust*. Firms should be budgeting for and implementing a Zero Trust Architecture (ZTA). Zero Trust means just that. Trust nothing and verify everything. ZTA is an architecture and not a "thing" you purchase off the shelf. The focus of ZTA is to verify the identity and access of every device and every person.

Perimeter security no longer works. We can't put a "wall" around all of our devices and data anymore. We are much more mobile (e.g. a hybrid workforce) and increasingly use more cloud services. This means we have to authenticate every access whether it is internal or external. In addition, we need to periodically re-authenticate access since there may be a compromise after initial access. In other words, assume the network or endpoint is compromised.

Implementing ZTA will take some time and it needs to be planned. The best approach will be to implement portions of ZTA over time. MFA is a good starting point to begin your ZTA journey. The key is to implement changes that enable your workforce to be secure without a lot of pain.

## Final Thought

If you can't afford to take reasonable steps to secure your data, you sure as heck can't afford to be the victim of a data breach!

***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 (CISSP), Certified Ethical Hacker (CEH) 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/Director of Cybersecurity and Digital Forensics 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