Ready, Fire, Aim: The Wrong Way for Law Firms to Protect Their Data

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

The Way the Military Does It: Ready, Aim, Fire

So why are we hearing from so many proponents of the "Ready, Fire, Aim" contingent? As far as we can determine, the theory is that getting something done is better than taking time to think it through and devising a comprehensive plan.

As applied to cybersecurity, "Ready, fire, aim" makes very little sense – and it can actively be dangerous! Of all the many problems law firms must deal with, one of the most critical is protecting confidential data. That requires time, input from a number of people – and hopefully the outcome is a plan which encompasses all the current recommended actions for securing your data.

Not thinking things through makes no sense. And yet, there seems to be a proclivity to take action of some kind. We discourage this approach entirely. In an emergency, it is possible that you may need to take actions to protect data immediately. But in most cases, law firms have time enough to work through the complications of cybersecurity in an organized manner. Yet again, another reason to make sure you have an Incident Response Plan (IRP) to guide your actions.

There is No "Set It and Forget It" in Cybersecurity

We all wish we could "set it and forget it." Managing cybersecurity is a daunting task – and from year to year (sometimes month to month, and even week to week) cybersecurity threats evolve, as do defenses against those threats.

Commonly, law firms are resistant to reviewing, at least annually, the state of their cybersecurity and improvements that need to be made. The more it will cost them to upgrade their cybersecurity, the more resistant they are.

A normal reaction, but a poorly thought-out one.

We live in a world where law firm data breaches (in 2023) have proliferated in both large and small firms. Ransom demands are growing. All 50 states have laws requiring that data breach notifications be filed. Thus far, 13 states have passed privacy laws which have their own set of requirements in the event of a data beach. And, to the horror of many, it is not uncommon to see class action law firms filing class actions against law firms which have been breached.

That's quite the trifecta – to which we would add the severe reputational damage.

How Does Ready, Aim, Fire Apply to Law Firms?

Done right, aiming before firing can bring you a long way toward securing your data. Our greatest challenge these days is getting law firms to understand that the ways in which data was protected over the last several years is obsolete.

For those firms that have not yet accepted the absolute necessity of moving to Zero Trust Architecture (ZTA), now is the time. Ignore ZTA at your own peril. We say that constantly, but many clients seem to find it difficult to accept. So much to do – and a major investment of time and money.

Microsoft on Basic Cyber Hygiene

Microsoft, in August 2023, emphasized that basic cyber hygiene prevents 98% percent of cyberattacks – an impressive statistic. The #1 recommendation is that you require the use of multifactor authentication (MFA), which requires two or more factors for verification. Cybercriminals who know a password (or crack one) still can't access your network if you have MFA, which prevents 99.9% of attacks on your accounts.

There is no single step you can take to protect your data more than that one. Is it regarded as inconvenient? Absolutely. Users hate it and term it inconvenient. It sure as heck is a lot less inconvenient than a data breach.

Take the time to make it easier on your employees by using biometrics or security keys such as YubiKey. There are other measures you can take without diluting the effectiveness of MFA – talk to your cybersecurity expert to get the details.

Also, keep training your employees on cybersecurity awareness to prevent successful phishing attacks, still very much a peril. Running periodic phishing simulations is a great supplement to yearly training.

Microsoft Also Advocates for Zero Trust Architecture

ZTA is now the norm and reportedly will be used across the board by the federal government by the end of fiscal 2024. This is going to be part of establishing a "standard of care."

ZTA will verify every authentication, allow least-privileged access, utilize AI and high end detection defenses as well as provide automated responses to threats.

Is it a little complicated to understand? Yes. We work hard to make the sometimes obtuse language of ZTA simpler to understand. Lawyers do seem to comprehend that ZTA helps to make remote working safer – and reduces the risk of a successful attack by constantly monitoring and taking immediate steps to counter an attack.

If it sounds a little like magic, it is. The best part is that embracing it now substantially reduces your risk of having a data breach. Your clients love ZTA and so do cyberinsurance companies – some clients and cyberinsurers are now demanding that you adopt ZTA.

Final Words

While all the sound advice above should be followed, we often bemoan the truth of the following words: "Never underestimate the power of lawyers to resist change." And please aim before you fire!

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*