25% of Law Firms Have Been Breached

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

What We Learned in 2021

In December 2021, Dave Ries, a frequent co-presenter with the authors, wrote an excellent summary of the cybersecurity portion of the *ABA's 2021 Legal Technology Survey Report*. You can find his summary at https://www.americanbar.org/groups/law_practice/publications/techreport/2021/cybersecurity/. Perhaps the most striking statistic is that 25% of the survey's respondents reported that their law firm had been breached **at some time**. Clearly, law firms are an attractive target for cybercriminals – with a plethora of data about so many people and businesses, law firms are a one-stop shop for harvesting a wealth of information.

Quick Refresher on the Ethics Rules

Several of the ABA Model Rules are particularly related to safeguarding client data, including competence (Model Rule 1.1), communication (Model Rule 1.4), confidentiality of information (Model Rule 1.6) and supervision (Model Rules 5.1, 5.2 and 5.3).

What do these duties require? When using technology, they require that we employ competent and reasonable measures to safeguard the confidentiality of client information, that we communicate with clients about our use of technology and get informed consent from clients where appropriate and that we supervise subordinate attorneys, law firm personnel and service providers to ensure compliance with these duties.

There are currently three opinions from the ABA (and others from state bars) that you should be familiar with, including ABA Formal Opinion 477R, "Securing Communication of Protected Client Information" (May 2017), ABA Formal Opinion 483, "Lawyers' Obligations After an Electronic Data Breach or Cyberattack" (October 2018), and ABA Formal Opinion 498, "Virtual Practice" (February 2021).

Don't forget common law duties or contractual and regulatory obligations involving protecting client data and personally identifiable information (PII).

Who's In Charge of Cybersecurity?

It won't surprise anyone that 80% of solo practitioners have primary responsibility for the security of their firms. The larger the firm, the more likely it is to have expert consultants, IT staff or a chief information officer.

A chief security officer has primary responsibility in some large firms, 13% of firms with 100-499 attorneys and 16% with 500+ attorneys. That number surprised us a little – we would have expected the percentages to be higher given what's at risk and the available resources of larger firms.

Law Firm Policies are Still Missing in Too Many Firms

53% of respondents say their firms have a policy to manage the retention of data held by the firm, 60% have a policy on email use, 56% for internet use, 57% for computer acceptable use, 56% for remote access, 48% for social media, 32% for personal technology use/BYOD (Bring Your Own Device), and 44%

for employee privacy. As you might expect, the numbers have increased over the years, and they are particularly higher in larger firms. The smaller firms tend to lag behind.

We are concerned that 17% of respondents report that they have no policies and 8% don't know about security policies. Clearly, many firms need to up their game.

Incident Response Plans (IRPs) Are Critical, Yet Many Law Firms Don't Have Them

Just 36% of respondents say their firm has an incident response plan. Firm size makes a big difference here, with 12% of solo firms having them and 21% of firms with 2-9 attorneys. The number jumps to 80% at firms with 100+ attorneys.

As the authors regularly give CLEs on cybersecurity, these numbers are consistent with what we've seen, and they are deplorable. We have borne witness to the chaos and panic that ensues after a cyber incident or a full-blown data breach – it isn't pretty. We hear many lawyers says that developing an IRP is expensive and time-consuming. If you believe that, you may well discover just how expensive and time-consuming a data breach can be!

Cybersecurity Awareness Training: Another Essential

Though this statistic is not from the ABA Report, it is generally agreed that there is a human element involved in 82% of data breaches. It is relatively inexpensive to provide law firm employees with security awareness training. They need to know what a phishing email is, how social engineering is used to extract information from law firm employees, the dangers of re-using or sharing passwords – and the list goes on and on.

Is it expensive? If you go to the big cybersecurity firms, yes. If you have your training done by the smaller firms, you'll find the costs modest.

How often should you train? People just plain forget some of what they learned. Also, both threats and defenses in cybersecurity change regularly. Train at least annually. Twice a year is better.

Clients Driving Cybersecurity Requirements

Some clients are requiring third-party security assessments, though there is resistance from law firms. Only 27% of law firms reported that they had a full security assessment, and they were mostly large firms.

30% of respondents reported that they had received a client security requirements document or guidelines, again mostly large firms.

It continues to worry us that these percentages are so low. Only once have we done a security assessment for a law firm without finding any critical vulnerabilities.

Final Words

Though we say it all the time, we'll repeat ourselves here. There is no silver bullet in the cybersecurity world. If a vendor tells you they can make you 100% secure, run the other way. We need to get many of the percentages cited above to be higher. Time to roll up your sleeves and get to work.

Lastly, because there is no silver bullet, don't forget to make sure that you have adequate cyberinsurance – that is a risk management tool since danger always lurks, your technology efforts notwithstanding!

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*.

Michael C. Maschke *is the CEO/Director of Cybersecurity 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*.