Cybersecurity Assessments for Law Firms: How Not to Screw Them Up

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

Should You Have a Cybersecurity Assessment Every Year?

Absolutely. A fair number of firms perform cybersecurity assessments twice a year. For most firms, we'll settle for once a year. It is also true that most cyberinsurance companies will also settle for once-a-year assessments. The biggest firms may do it twice a year (or more), but most of you reading this are probably doing just fine with yearly assessments.

We have lived through 2023 – in which we saw more law firm breaches than ever before. And we saw (horrifyingly) a stream of class action lawsuits filed against breached law firms. So yes, we need to pay attention to cybersecurity assessments – not put them off or skip a year for budgetary reasons. While we often hear that budgets don't allow for a cybersecurity assessment, if you get breached, your budget is going all to hell. Better to spend the money and avoid the breach.

Do you need a penetration test which takes longer and is much more expensive? If you're big enough, yes. But for solos, small and midsize firms, a cybersecurity assessment is generally considered to be reasonable. Penetration tests are very expensive, complex and include an authorized simulated attack performed on your network(s) to evaluate security weaknesses. Testers act as attackers, simulating a variety of attacks. We could write an article on penetration testing alone but suffice it to say that most law firms will be ethically compliant with a yearly cybersecurity assessment.

Can You Use Your Own Internal IT/Cybersecurity Team to Do an Assessment?

That is one of the stupidest questions we've ever heard and, sadly, we hear it a lot. In fact, employees tend to encourage management to let them do the testing. Why? The unvarnished answer is that they are afraid that weaknesses in the network will be revealed, and they will be blamed.

Here's the horrifying truth: In over 25 years of business, only ONCE have we done a cybersecurity assessment without finding a critical vulnerability. Just once. Kudos to that law firm for a job well done by great employees with the full support of management.

However, normally our reports contain a sizeable list of vulnerabilities, critical, high, medium and low. As IBM says, critical vulnerabilities should be prioritized for immediate

remediation. High vulnerabilities should be reviewed and remediated wherever possible. Medium vulnerabilities pose minimal risk to data security – fix them when you can or when the budget allows. Low vulnerabilities are more cautionary or informational.

How Do You Find a Qualified Cybersecurity Assessment Provider?

One thing you are looking for is a long list of cybersecurity certifications. Assessments need to be done by highly qualified experts. Clearly, they are often costly, especially if they are large entities. For most law firms, the better alternative is smaller firms with a lot of certifications and references from other law firms that you can check with.

It is very useful to seek out your friends in other law firms as a first step. They have no vested interest. Ask questions of your friends – did the experts get along well with the in-house IT/cybersecurity folks? Did they offer a flat fee cost? What was it? (We prefer flat fee pricing based on the number of devices to be assessed). Were their reports thorough and not written in technical jargon? Did they clearly prioritize the recommendations? Did they offer a cost estimation for remediation of the vulnerabilities?

Be Wary of Cybersecurity Assessment Providers Who Work for Cyberinsurance Companies

We are seeing a very disturbing trend in the cyberinsurance market. Insurance carriers are partnering with managed security and IT providers to gain more insight into your data and infrastructure. They offer lower premium rates if you use their partners. The justification is that the carrier has a much better idea of its risk exposure when they have firsthand knowledge about your data and infrastructure. The problem is that they have firsthand knowledge about your data and infrastructure.

You install agents within your environment that monitor status and activity. In other words, they have “eyes” into your data, your client data, vulnerabilities and pretty much everything about your firm’s operation. No thank you.

You Hold Your Cybersecurity Assessment in Your Hands: Now What?

Assuming you had a reasonably priced but expert firm do the assessment, you now have a perfect roadmap in your hands. If the project remediation costs don’t seem reasonable, you can always choose another firm. But if the firm’s employees did well in working with your employees, that’s a very good sign. They are likely to work well with your employees in remediating the vulnerabilities.

Don’t put this off – that happens way too often. Get those critical vulnerabilities squared away and give serious thought to how and when you can take care of the High and Medium vulnerabilities. Getting management buy-in can be a royal pain, so be ready with the stats of breached law firms, the costs to deal with the breach and the terrible publication

relations disaster – no law firm in today's legal environment can escape having to report a breach, often to multiple entities.

Final Words

P.T. Barnum once said, "There's no such thing as bad publicity." Where law firm data breaches are concerned, let us assure you that P.T. Barnum was wrong.

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