Security Assessments and Pen Tests for Law Firms

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

The Perfect Storm is Headed Your Way

The way law firms operate has undergone a drastic change over the past year, in both the physical and digital worlds. We saw law firm employees working remotely, a heavier reliance on cloud-based technology solutions and services and firms operating on a reduced budget through the economic crisis caused by the pandemic. Some law firms have thrived, while some have floundered with an inability to pivot and adapt quickly.

The new norm has created an operating environment that hackers once could only dream of. What has been proven over the past year is that cybercrime rises during times of crisis and law firms are still slow to respond. Ransomware is the number one cybersecurity threat that we now face. The perfect storm has been created and is heading towards your firm if it hasn't arrived already.

What exactly do we mean? Users are now accessing confidential client files from their kitchen or home office through personal computers, tablets, and outdated Wi-Fi that has not had the configuration updated since the Internet Service Provider installed it. Employer-provided systems are not universal, even among the largest of firms. Users are now responsible for keeping their software and operating system patched with critical updates.

Two-factor authentication, which Microsoft states will stop 99.9% of account takeover attacks, remains unused – even though it is provided at no cost with your Microsoft 365 subscription. Encryption of laptops, while commonly discussed, is hardly implemented. Our country was shut down abruptly; this prevented most firms from carefully planning and evaluating the new cybersecurity landscape. They faced immediate changes in the way they worked. Plain and simple, they were not prepared.

Law firms recognize that there are security problems within their networks. Many just don't know where to start to identify and fix them. Others accept the risks of taking no action.

All is not lost. There are steps that law firms can take now to get control of the situation, to identify where the problems exist and remediate them. The first step is realizing that something needs to be done. The next step is finding where the problems exist, and that is accomplished through a security assessment.

Security Assessments Are Essential

You can't fix what you don't know is broken. We are now at a point in time where attorneys are receiving from a client or prospective client a request for an independent security assessment or proof of having one recently been performed. Many are also receiving a request to provide a client or prospective client with their firm cybersecurity measures, along with any documentation or guidelines. Law firms inquiring about cyberinsurance are often required to have an assessment performed to become eligible for coverage. Assessments are becoming THE way to prove (and document) that you take cybersecurity seriously.

Even if no one requires you to do an assessment, you absolutely need one – and it should be done at least annually. Why don't firms have an assessment done? Mostly because lawyers fear the costs of the assessments – and the costs they may incur in fixing what is wrong.

Let us try to allay some fears. While it's true that large law firms will generally seek out large (and therefore expensive) cybersecurity firms, it is equally true that there are many smaller cybersecurity firms with reasonable fixed-fee prices for doing an assessment and giving you a report identifying your vulnerabilities. Typically, the price is based on the number of endpoints involved in the assessment, including such things as mobile devices, computers, servers, network, and storage devices. And yes, even printers. You need to make sure the cost of the report deliverable is included, as well as time for discussion of its contents. The proposal should be clear, concise, and understandable. Do not proceed unless you know what you are getting for the cost. It wouldn't be uncommon for a security assessment of a small firm with 25 endpoints to cost $5,000 or less.

What should you be looking for besides a reasonable price? References from colleagues (who have no dog in the hunt) are useful along with references from previous clients. Are they experienced and have they performed assessments before? Make sure the company has current cybersecurity certifications. IT certifications are not cybersecurity certifications. Look for reputable certifications such as the Certified Information Systems Security Professional (CISSP), Certified Ethical Hacker (CEH), GIAC® Penetration Tester (GPEN), and PenTest+. Also, make sure the report will follow the guidelines of a reputable organization such as the Center for Internet Security.

It's worth pointing out that assessments can take a few weeks to complete, depending on the scope of the project and the number of endpoints. You will want to know when the assessment will start and end, including if any after-hour or weekend work is required to minimize the impact on critical systems. The drafting of the report can take several days depending on the level of detail provided. Before starting an engagement, vendors will ask you for network diagrams, asset inventory lists, a listing of software and licensing agreements, Administrator user names and passwords to network devices, servers, and other security devices. To expedite the engagement, it will be helpful to have this information readily available.

What you want from the assessment is to know what critical vulnerabilities you have so those can be fixed right away. After that, the report will identify medium and low risks. Address medium risks as soon as you can. The idea is to plan a timeline, often constructed around budget constraints or impact on productivity. The low risks should of course be addressed, but they don't carry the level of concern that critical and medium risks do. Some of the risks can be addressed by your technology provider, whether in-house or outsourced.

Remember that a vulnerability assessment is not the same thing as a penetration test. Pen tests are exercises where the tester acts as if they are attackers trying to infiltrate your network, exploit any discovered vulnerabilities, and compromise your data. In other words, they act like an attacker would act. We recommend that firms start with a vulnerability assessment as they are much more affordable and will provide a baseline of your security posture. Pen tests are much more expensive and could be considered later if warranted.

Pen Testing Explained

Let's get started with penetration testing. For most solo/small law firms, this is probably overkill unless you have major league clients or extremely high-value data. In pen testing, you are asking a company to pretend they are the "bad guys" and attack you – it is scary stuff and tends to be expensive. The company will generally require a "get out of jail" free agreement, saying that they are not liable for any damages resulting from a successful compromise of your network. There are different types of pen test engagements and one (the white box test described below) that is a little less costly. Pen tests can take a few weeks up to several months to complete, depending on the scope of the engagement and the type of test agreed upon.

As stated, there are different types of pen tests – white box, black box, and hybrid (sometimes called gray box). In a white box engagement, the vendor works hand-in-hand with the client in exploiting the systems. The client will provide the vendor with information about their network including Internet Protocol address ranges, types of hardware, and software. Often in a white box pen test, the client will set up an Administrator account for the vendor to use during the exploit process. The vendor may even be allowed to place a "pen test laptop" on the local network to attempt the exploits, thereby speeding up the process. These engagements often cost less than a black box pen test, take less time to complete, and are nearly as effective in identifying successful attack vectors into your network as a black box pen test. A white box pen test of a single network with less than a hundred endpoints can run up to $20,000 or more from start to finish.

In a black box pen test, the vendor is provided with no information or detail about the client network – including the number of endpoints, types of services or applications, or the number of physical or logical locations. The vendor is left on their own to perform the reconnaissance and discovery, attempting to break into the client's network just like a hacker does. A black box test is a more realistic attack because it takes the stance of a non-informed potential attacker. It simulates a very realistic scenario, helping a business be on its highest guard. These types of pen tests can take months to complete and can be extremely expensive depending on the scope of the engagement. We've seen these types of engagements cost upwards of $100,000 or more depending on the size of the company.

A hybrid pen test engagement is a combination of the two, in terms of requirements, the information provided to the vendor, cost, and timing. These aren't as common but it's helpful to be aware that these engagements do exist and can be more thorough than a white box but less expensive than a black box engagement.

Parting pearls of wisdom

Now that you have information and guidance on both security assessments and pen tests, it's time to take action. Reach out to other firms that you trust for recommendations and referrals for these services. The time to act was before the crisis, but it's not too late. Especially if you're one of the lucky firms that hasn't experienced a security incident since the start of the pandemic. Trust us, we've seen and heard it all – from ransomware outbreaks crippling networks and destroying client data to millions of dollars being wired to fraudulent accounts – all with devastating outcomes for the unfortunate law firms.

Vulnerabilities are constantly changing and require security assessments to be performed at least annually. These engagements identify vulnerabilities in your information systems including software, computers, mobile devices, network devices, along with their configurations, and provide steps to

address them. Immediately fix the most critical vulnerabilities and create a plan to address the medium and low vulnerabilities. Once you complete this process and fix the problems, the security posture of your network will increase to a level it has never seen before.

Lastly a parting warning – there is no silver bullet when it comes to cybersecurity and protecting your systems. There is no 100% foolproof solution – and run from any vendor who says that there is. But there are steps that you can take to be proactive (such as a security assessment) and to batten down the hatches. Don't be foolish and think it won't happen to my firm – we're too small. All law firms have a bullseye on their figurative back – if you are lucky enough to have escaped serious harm thus far, your luck may run out without preventive actions on your part.

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 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*.