How Does A Law Firm Find a Good Cybersecurity Company?

by Sharon D. Nelson, Esq. and John W. Simek

Thanks to our friend and colleague Courtney Kennaday, the Director of South Carolina's Practice Management Advisor Program, for suggesting the topic of this article. As she accurately noted, information security companies "are springing up like weeds." She also asked, "How's a lawyer to know who is good? What should they be looking for in the company's resume?"

Excellent questions Courtney. We hear law firms bemoaning the difficulties of finding reputable (and affordable) cybersecurity companies all the time. Since our company, Sensei Enterprises, Inc., provides those services, hopefully we have some insights to guide law firms in their selection.

Managed security services is an ongoing effort, generally addressed with a long term contract, and not addressed here. That would require an article of its own. We're talking about companies that investigate data breaches and provide security assessments and implement recommendations from those assessments. Let's start with the first question we hear all the time.

Why Do I Need a Cybersecurity Firm?

Almost all law firms have an IT consultant, whether an outside consultant or in-house employee. All too often, lawyers believe that information technology wholly embraces information security. It does not. While there is a lot of crossover between the two fields, most IT providers are aware of basic security best practices – they are not actually cybersecurity specialists – though they may feel that they are!

As technology has gotten more and more complex, it has become critical to have access to folks who do a "deep dive" into security. A security specialist who is all textbook and has no practical experience with IT is no good to you. All the certifications in the world are no substitute for experience.

As we go to press, 25 states have now ratified some version of the ABA 2012 changes to the Model Rules of Professional Conduct, which require technology competence and mandate that a lawyer "shall make reasonable efforts to prevent the inadvertent disclosure of, or unauthorized access to, information relating to the representation of a client."

Between the enhanced ethical duties and the flood of data breaches throughout all businesses, law firms have recently recognized the need to focus on keeping client data secure. Hence the proliferation of cybersecurity firms. But as Courtney asked, "How's a lawyer to know who is good?"

The Big Dogs

If you run with the big dogs (AM Law 200), you are probably going to select a large provider of information security services. They cost more, but they offer a large range of services and a depth of knowledge and industry certifications. Among those we see most often are Mandiant (a division of FireEye), Dell SecureWorks, RSA, IBM Security and Root9b.

The Rest of the Pack

We know that the vast majority of lawyers reading this article will be from solo, small or mid-sized practices. The jaw-dropping prices of the large cybersecurity firms are well beyond your reach. But take heart, there are plenty of smaller businesses that provide information security at a price point you can live with. So what are you looking for when you search for this kind of help?

Recommendation, Recommendations, Recommendations

We can't stress this too strongly. Talk to other lawyers and law firms. Who have they used and liked? Did their pricing seem fair considering the work done? What services did they provide? Did they meet their deadlines? What kind of certifications did they have? Were they professional and responsive? If they provided a security assessment, was their deliverable a good report? Did they also make recommendations for remediating security vulnerabilities with pricing? Any negative feedback? Did they play well with your IT folks? This is pretty critical because your IT folks are going to feel threatened the moment they learn that cybersecurity experts are being brought aboard. Good experts will expect a certain amount of tension and know how to defuse it and emerge with a "we're all on the same team" mentality.

References

Any good information security company will be ready with references. Our advice is to be a bit wary. These will be cherry-picked happy customers. You can ask them all the questions above and your instincts about whether the information you're given may be accurate, but we still prefer reaching out to other law firms as referenced above. We've seen too many folks do an Internet search for a cybersecurity company (and of course the company looks awesome on their website) and the references do check out – but then they are disappointed by poor work, a failure to be responsive, escalating costs, etc.

Better, we think, to follow the Beatles' advice and get by with a little help from your friends.

Certifications

You might think that the certifications held by cybersecurity experts would be a real measurement of their skills, but not always. There are certifications you can essentially buy (no testing), certifications with easy tests or open book tests, certifications which aren't true certifications (for instance, a 'certification' that you attended a course) and certifications which are bookish rather than practical.

Real experts get their hands dirty fast. They want to delve into the inner recesses of your network after looking at your network diagram (you have one, right?). You may not understand what they say – the good ones translate cyberspeak into English pretty well – but it's usually clear when you ask a question

and they answer immediately and confidently that you probably have someone who knows what they are doing. If you ask a supposed expert how to engineer your backup to guard against ransomware and they fumble for an answer (and you can learn the answer on the Internet yourself), you'll know pretty quickly who you don't want to hire.

Here's a list of some of the information security certifications that we think are most valuable in evaluating a company's credentials – along with a brief statement of what the certification provides:

CISSP (Certified Information Systems Security Professional) – an independent vendor neutral certification from the International Information System Security Certification Consortium, also known as $(ISC)^2$. It is globally recognized and covers competence in eight domains including:

- Security and Risk Management
- Asset Security
- Security Engineering
- Communications and Network Security
- Identity and Access Management
- Security Assessment and Testing
- Security Operations
- Software Development Security

The certification requires a passing grade of 700 to 1000 points from a test comprised of 250 questions. You must have at least five years of security work experience (one year may be waived for a college degree) to qualify as an exam candidate. Ongoing education is also required to keep the CISSP current and valid.

CEH (Certified Ethical Hacker) – a certification that assesses the security of a computer system by using penetration testing techniques. The CEH is administered by EC-Council. Similar to the CISSP, the CEH requires two years of information security experience before being eligible to take the exam. The experience requirement is waived if the candidate attends official EC-Council training at an Accredited Training Center, via the iClass platform, or at an approved academic institution. Penetration testing is one technique to help assess security vulnerabilities.

GSE (GIAC Security Expert) – a very rigorous two part exam administered by GIAC (Global Information Assurance Certification), an entity that specializes in technical and practical certification. Part 1 of the GSE is a multiple choice exam. Part 2 is a 2-day lab exam consisting of hands-on exercises.

EnCE (EnCase Certified Examiner) – a digital forensics certification administered by Guidance Software. Forensic examinations are used to attempt to determine what data may have been compromised and how the breach may have occurred. Other forensic certifications such as the **CCE (Certified Computer Examiner)** and the **GCFE (GIAC Certified Forensic Examiner)** are also commonly seen in the cybersecurity world.

There are certainly other reputable security certifications, but these are some of the ones we see most often and they are highly respected within the industry.

People Skills

You want someone you can understand. You want someone who doesn't "speak from high" making you feel like an idiot. You want someone who will work well with senior partners as easily as staff, and who will make friends with your IT support staff.

A telephone call to interview an expert is a good thing. Better yet, see if they will agree to an initial meeting. Most companies are happy to offer a free consultation for an hour or so. We wouldn't hire anyone who wasn't willing to do that. And don't let them send a sales person. You don't need charm and snake oil from someone who doesn't understand security. You want one of their experts who would actually be working with you. In the course of an hour, you'll probably have a good sense of whether this is someone you'll be comfortable working with and whether they are a good match in all other respects as well. It is worth the time – in part because cybersecurity isn't cheap and this is a bad place to make a mistake.

Does location matter?

Location doesn't matter a whit to larger law firms because they can afford travel expenses associated with a remote expert. With respect to smaller firms, the answer is more variable. Without going into granular detail, your expert is not going to need to spend a lot of time on your site. What the expert needs to do onsite is to perform such tasks as assessment of physical devices and equipment, collect logs and configuration files, review physical security, connect test equipment to the internal network, etc. This will generally only take a day. Almost any size firm can afford the travel expenses associated with an expert within driving range. Someone who has to fly in will add that cost plus reasonable meals and a night's hotel stay in most cases.

Solos and very small firms will prefer someone more local for cost reasons. However, if you have really found an expert you trust and you have the monies to engage them, we think the modest expenses involved with a one-day visit are well worth it. Of course, you should also consider whether you will want the expert back to discuss the final report and its recommendations – some laws firm do, but others are satisfied with a video conference. It truly is amazing how technology has made selecting remote experts far less costly as the vast majority of the work can be done remotely.

Costs

There is not a lot of transparency in information security pricing yet, something we hope will change over time. But you can force the hands of companies. If they don't have flat fee pricing based on number of users (or devices), tell them that you will only sign a contract with a company that offers flat fee pricing or certainly a not-to-exceed amount.

Be sure you define the scope of work correctly. But if you are reacting to a data breach, this advice goes out the window. You'll have to trust someone because the expert has no idea what he/she is walking into after a data breach (see the paragraph on recommendations above). You should have a digital forensics expert (these are often cybersecurity experts as well) in mind in the event of a breach. Better to be proactive because you'll be in full-blown panic mode if there's a breach.

But let's assume you are trying to secure your crown jewels (your confidential data) with no breach in play. Now you are looking for a security assessment – and then remediation. We see folks all the time

who want them both in one contract but that's not possible. Experts have to do an assessment before they know what needs to be remediated.

Understand, if you are comparing companies, what is in the scope. They should not be looking at servers only, but at all mobile devices. Is an assessment of physical security included? What about the review of security policies? Are the objectives to be met clearly stated in the scope of work?

So . . . you get a flat fee for the assessment. From smaller companies, this will not be a massive outlay. And of course you may get several flat fee quotes (but do remember that it is indeed often true that you get what you pay for). We think your gut feel after your meeting with the expert may guide you on how significant the monetary difference is. You have that Goldilocks "just right" feeling when you meet the right expert.

Once you get your assessment report back, it will normally come with recommendations – and any smart company is going to offer a proposal with pricing as well. This is where sticker shock may come in. Here's how to help yourself a bit. Make sure the report identifies, in order, critical vulnerabilities, serious vulnerabilities, and low to moderate vulnerabilities. Have the price listed for each remediation action to be taken (including equipment and labor). This will allow you to address the most serious problems first, as your budget allows – but if you've got truly major problems, you may consider dipping into a line of credit. Hopefully you won't find yourself in that situation, but there are firms who hover on the edge of disaster without ready funds to cure their problems.

And you know what? Once you have the report and that company's pricing, if you think it's way off base, take it to another cybersecurity company. If you did not choose wisely in the first instance, another company may find the recommendations or the prices to be out of line. Needless to say, you have to be careful of companies who simply want to bash someone else's work and then lowball their own pricing to get in the door. Even if company #2 gives you a good flat fee quote, be wary of the tone taken to someone else's work – is it respectful? Also, be watchful for signs that the level of protection is being lowered as a tradeoff for lower costs.

Final Thoughts

Go get those recommendations from friends. Have we said this already? Nonetheless, it bears repeating. If your friends have had a really good experience with a company, the chances are that they won't steer you wrong.

The kicker is that you'll have to go this process more than once. In April of 2016, *Legal TechNews* had a headline that read "Through Human and Conventional Openings, Successful Breaches Happening at Dizzying Speeds." That headline was spot on.

The means of attacking law firms morph from day to day, as do the defenses to such attacks. You can never set up your cybersecurity, think you're done and walk away. There is no "set it and forget it" in fast moving field. As a cost of running a law firm, cybersecurity is here to stay.

The authors are the President and Vice President of Sensei Enterprises, Inc., a legal technology, information security and digital forensics firm based in Fairfax, VA. 703-359-0700 (phone) www.senseient.com