6 Steps to a Successful Cybersecurity Strategy: For the Highly Targeted Law Firm

AVALONCyber

CYBERSECURITY IS A RISK

In March 2016, the Wall Street Journal broke the news that some of the biggest, most prestigious New York City law firms had been hacked, including Cravath and Weil Gotshal.[1] The cybersecurity situation for law firms has become so serious lately that in the ABA Journal article one big firm partner warned his fellow lawyers to: "start with the assumption that you will face one or more cyber breaches."[2] Indeed, in reporting on the attacks on top law firms, the WSJ further reported that it was just "one of several recent cyber-related incidents that have affected the legal industry." A 2015 ABA survey found that 23% of law firms of more than 100 lawyers admitted to data breaches.[3]

A further danger for law firms is that, unlike physical theft, data can be stolen, copied or just viewed in place without leaving obvious traces of a crime. The FBI was reported to be investigating the March 2016 big firm data breach for potential theft of Mergers and Acquisitions materials that could be used in insider trading, but, no-one involved at the time knew what, if any, data had been taken or even accessed. That's not surprising; according to the Verizon Risk Team 2016 Data Breach Investigations Report

1 Nicole Hong and Robin Sidel, "Hackers Breach Law Firms, Including Cravath and Weil Gotshal," The Wall Street Journal, March 29, 2016
2 Jason Tashea, "Experts advise new tactics to fight data breaches," ABA Journal, August 1, 2016
3 Gabe Friedman, "ABA Survey: Data Breaches Rising at Large Firms," Bloomberg Law, September 23, 2015

of over 100,000 incidents, 92% of data breaches in 2015 were discovered weeks or months later not by the target but by law enforcement, a compromised client or other third party. Only 8% of the time was the breach discovered by the internal IT team. They're just not looking!

And so it is also not surprising that the press, especially the legal technology press, has seized upon these scary statistics to publish scary stories:

- **As Cyber Fears Rise, Smaller Firms Struggle to Cope** - "…the price of effective security may be putting smaller firms at a disadvantage…clients are now going so far as to audit firms' security setups…"[4]
- **Smaller Firms May Risk Losing Clients Over Cybersecurity Fears** - "… more clients threaten to abandon firms that don't meet their data-privacy standards…it's a factor that in-house counsel are taking into account as many of them whittle down their rosters of outside law firms."[5]
- **Will Cybersecurity Costs Force Small Firms to Merge?** - (Spoiler alert: for one small firm, yes) "…the costs and worries about protecting client data had become overwhelming…'It was getting to the point where I couldn't sleep at night…'"[6]

92% of data breaches in 2015 were discovered weeks or months later not by the target, but by a third party

Be afraid, be…well, actually don't be afraid. Be smart.

So, how should you deal with this scary new risk as a lawyer? You could simply panic. We recently attended a conference on cybersecurity for lawyers where one of the lawyers in the audience told the other attending lawyers to stock up on bitcoins, so that they would have plenty of that infamously untraceable online currency on hand to pay the hackers who will inevitably steal or hold hostage their confidential client data. We suppose that this "advice" at least shows some level of understanding and acknowledgment of the problem; it's not the "stick your head in the sand" like a proverbial ostrich[7] approach. More like a "chicken running around with its head cutoff" type approach, if we were to stick with the avian theme. We wouldn't advise either approach and, the good news is, not only don't you have to, you are already on the path to doing the right thing.

Avalon has worked with lawyers for over a decade. Some of us are lawyers.

---

4 Rebecca Cohen and Lizzy McLellan, "As Cyber Fears Rise, Smaller Firms Struggle to Cope" Law Technology News, August 16, 2016

5 Lizzy McLellan, "Smaller Firms May Risk Losing Clients Over Cybersecurity Fears," Law.com, August 9, 2016

6 Lizzy McLellan, "Will Cybersecurity Costs Force Small Firms to Merge?" Law.com, July 25, 2016

7 Ostriches don't actually do this, and neither should lawyers when it comes to confronting cybersecurity risks

Some of us are married to lawyers. All of us understand and appreciate lawyers. And lawyers understand—and know how to deal with—risk.

Clients come to lawyers to get help identifying, managing, and mitigating risks. Whether it is the risk of a lawsuit, the risk of a new regulation, or the risk in a contract, clients come to lawyers because the lawyers are the best at dealing with those risks. Lawyers don't panic over risk, they solve it.

Cybersecurity is just another risk.

So solve it.

One more thing that we have learned at Avalon is that while good lawyers know how to use their skills to solve problems, great lawyers know how to combine their own skills with others' skills to solve problems even better. Great lawyers know how to team up with the expert they need to prove their theory of the case, to lobby the regulators, or to run the numbers in the contract. Cybersecurity is no different; the experts who you need on your team are out there —you just need to know where to look to find them.

Great news! You've already taken the first step towards solving your cybersecurity problems

The first step towards identifying, mitigating, and managing the risk from cybersecurity problems is to find the right experts to partner with—and if you're reading this (and read this far) you've already taken that first step. So now what?

The first step is to make sure, like every responsible business these days, that you've got anti-virus/malware software installed and updated regularly. But you can't stop there, because anti-virus software by itself just isn't enough anymore. Such software works by comparing the digital signature of potential malware against a system database of known threats. Even the software providers themselves have started to admit (quietly, behind the scenes) that they can't update their databases fast enough anymore.

The most sophisticated anti-virus systems get around this "keeping up with the Hacker Joneses" problem by being able to detect problematic behavior by programs, such as changing access rights, without needing an exact digital signature match. But even then the ubiquity of anti-virus software

works against it. Hackers can test new malware on systems with protection software loaded until it can sneak by without warning, and they always seem to have plenty of time to get it right. Thus, new threats can slip by even the most up-to-date systems.

To make certain that your law firm is fully secure, you need to take further steps—ones that might not be quite so obvious to those who aren't cybersecurity experts. A professional cybersecurity expert firm can help you with those next steps to create a cybersecurity strategy for your law firm:

1. **Assessment:** The first and necessary step in any cybersecurity strategy is to know where you stand now. Cybersecurity experts can analyze your current technology, processes, and personnel awareness and compliance with those processes. The experts should then be able to deliver the results in a comprehensible report that you, as an attorney and not an IT person, can understand quickly, thoroughly and with the risks articulated and ranked clearly.
2. **Mitigation plan:** Once your law firm's current cybersecurity state is identified, you can work with your team of experts to plan how to eliminate or manage the risks. The best experts will provide you with a detailed view of not just the risks, but also the various options for handling them—and the potential costs for each option. That gives you the control you need over the process to decide what next steps make best sense for your firm.
3. **Insurance preparation:** Some risks can be mitigated or eliminated at a reasonable cost, but others cannot, and for those it might make best sense to insure against them. Insurers now require that companies meet certain cybersecurity thresholds before offering coverage, and can require pre-coverage audits. An expert team can help your firm meet the required thresholds, pass any pre-coverage audits, and even potentially advise on the best coverage options and costs.
4. **24x7x365 Network monitoring:** Based upon the success of IT Managed Services, where IT outsourcing companies provide help desk and other support, cybersecurity companies are now offering Managed Security Services ("MSS"). If your company isn't big enough to hire full time network security engineers can use MSS providers to monitor your network and endpoint 24 hours a day, 7 days a week, 365 days a year. MSS providers can identify and block hackers before they cause the kind of trouble that makes headlines.
5. **Response plan:** Of course, no matter how many precautions you take, sometimes breaches simply happen. A cybersecurity breach can be a

Hackers can test new malware on systems with protection software loaded until it can sneak by without warning

disaster for any firm if you aren't prepared. An expert team can help you create an easy-to-follow incident response plan that you and your personnel can follow in the event of any problem —and which will make it far less likely for that problem to turn into a disaster.

6. **Incident response:** Finally, when an incident does happen, you need to implement the response plan fast. You need a team of experts who can help you investigate the incident, determine the cause, fix the problem, and take steps to prevent it from happening again —all before it impacts your firm, your clients, and your reputation.

About Avalon

Avalon has deep roots in digital investigations and is called upon regularly to help mitigate network breaches. Over the last several years, we have launched proactive cybersecurity services to prevent breaches. We have seen firsthand how hackers operate and can provide a unique perspective on our Cyber Security services. We regularly provide basic and deep security assessments as well as proactive network monitoring services, in addition to our policy assessment, writing, and Chief Information Officer (CIO) on-demand services. Many firms believe that they are protected by the managed services provider or their anti-virus software, but that is no longer sufficient. We can provide assessments and recommendations on safe guarding your firm's reputation, sensitive information, and your confidential data.

Now that you've found the right experts to help you negotiate the risks of cybersecurity, it's time to take action. Avalon can help with all of these risk identification and mitigation approaches. Call or email us today, or read our case study on how we helped one client recover from a major website security breach.

AVALON Cyber

QUESTIONS?

For more information on any of our services, please contact:

Ashley Hazlett
Director of Marketing
716.995.7777
ashley.hazlett@teamavalon.com