A Roadmap for Lawyers With Cybersecurity Paralysis

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

We understand why lawyers have cybersecurity paralysis. They don't understand cybersecurity, experts disagree on the best steps to take, the majority of cybersecurity measures involve spending time and money – and to top it off, the threats and defenses against those threats change daily. Here's a brief roadmap to where you should be going.

By the Numbers: Where We Stand Today

Thanks to the ABA's 2018 Legal Technology Survey Report, we have some solid numbers to ponder as we construct our roadmap. Looking strictly at the big picture statistics, these were the ones we found most significant.

- 23% of respondents reported that their firm had been breached at some point.
- Of those reporting that they had been breached, the percentage breached generally increased with firm size until you got to large firms - 14% were solos, 24% for firms with 2-9 and 20-49 attorneys, 42% with 50-99 attorneys, and 31% with 100+ attorneys.
- 60% reported that their firms had not experienced a data breach. It is important to note that it is extremely possible that many firms experienced a breach and never detected it.
- 9% of those breached notified clients and 14% notified law enforcement.
- Of those breached, 41% reported downtime/loss of billable hours, 40% reported consulting fees for remediation of the problems, 11% reported loss or destruction of files, and 27% reported replacement of hardware/software.
- 40% reported experiencing an infection with viruses/malware/spyware, with the greater number occurring in firms with 2-49 attorneys and the lowest in firms with 500+ attorneys.
- 34% reported having cyberinsurance coverage (the percentage is growing, but slowly).
- 24% reported using full-drive encryption, a low number in these days.
- 29% reported using encryption of email for confidential/privileged data sent to clients.

Without bombarding you with numbers, the smaller the firm, the less likely it was to have a policy covering document retention, acceptable computer use, remote access, social media, personal technology use and employee privacy.

Perhaps most startling to us was the fact that only 25% reported having an incident response plan, a critical cybersecurity component. Larger firms were more likely to have such a plan. In general, larger firms have a bigger attack surface, but they also have more resources to devote

to cybersecurity. We will focus in this article on solo/small/mid-size firms as we try to lay out a roadmap to cybersecurity.

Security Assessments Are Essential

You can't fix what you don't know is broken. That's a fact. We are now at a point in time where 11% of attorneys have received from a client or prospective client a request for a security assessment. 34% have received some sort of client security requirements document. While the survey didn't ask about assessments required by insurance companies in order to get cyberinsurance, we know from our own clients that these are becoming more prevalent.

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's wrong.

So 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.

What should you be looking for besides a reasonable price? References from colleagues (who have no dog in the hunt) are useful. Make sure the company has true cybersecurity certifications. IT certifications are not cybersecurity certifications. Also make sure the report will follow the guidelines of a reputable organization such as the Center for Internet Security.

What you want as an end result 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.

Train Your Employees!

Your most valuable asset (your employees) are also a great threat. They are often moving too fast and easily duped by phishing emails. Phishing emails often and successfully target law firm. Perform phishing simulations where employees receive carefully constructed emails specific to your firm. If they do not see the red flags and click on a link or attachment (or answer an email leading to a follow-up conversation asking for monies, gift cards etc.), you will see how much training – and retraining - is needed.

Training should be annual, mandatory and without mobile devices present. The partners should be there, leading by example. Believe it or not, training is not very expensive – again, stick with smaller companies with cybersecurity certifications. Don't use your in-house folks – they simply don't carry a big enough stick – outsiders are invariably a better solution. Again, it's a good idea to get referrals from colleagues. You want trainers who can both educate and entertain. If they

cannot keep the attention of your employees, you are probably throwing money down a rat hole.

Happily, we are seeing more and more firms of all sizes investing in training. It might surprise you, but the employees generally enjoy the training and feel more confident in their ability to spot phishing emails, recognize social engineering attacks, etc. This is an excellent way of creating a culture of cybersecurity.

The Power of Policies

Policies in law firms tend to be static. There is a big push to get some policies in place and then nothing happens – sometimes for years. But policies are invaluable in all sorts of ways. They set the expectations of your employees. If employees disobey them, they will expect consequences, up to and including termination, depending on the severity of the violation.

As the world invariably changes (think of the policies that sufficed twenty years ago!), all policies should be reviewed yearly and revised as needed. Train employees on them every year – they will invariably forget portions of policies that are very important.

Many policies involve cybersecurity but they have different names, which can be confusing. The most common, by whatever name, are:

- Acceptable use policy
- Social media policy
- Remote access policy
- BYOD (Bring Your Own Device) policies
- Access control policies (passwords, multifactor authentication, biometric authentication, etc.)
- Backup policy
- Vendor access policy
- Retention and destruction of data policy (let us interject here that minimizing the data you retain is free – and greatly reduces your risk)
- Disaster recovery policy
- Encryption policy
- Reporting lost or stolen device policy
- Employee privacy (which may mean the absence of privacy on your network)

The Critical Incident Response Plan

If you don't have an incident response plan and you then suffer a breach, you will invariably be running around in headless chicken mode. We have borne witness to this reaction many times – you don't want to be in that mode.

The way to avoid it is to have a good incident response. The elements of such a plan are not all that complicated. Here are the essentials:

- Contact information for your regional FBI office
- Contact information for a data breach lawyer
- Contact information for the attorney who will oversee the breach response and any others in the firm who may be involved
- Contact information for a digital forensic company (to investigate and remediate the breach)
- Contact information for your insurance company (you may be required to report a breach/incident in a given period of time or lose benefits)
- Contact information for your bank (in case you need to warn them to be wary of suspicious transactions - banks are accustomed to this)
- Contact information for a public relations firm (small firms are less likely to use these services)
- Who needs to be informed? Clients? Vendors? The state attorney general? Make sure to have a copy of your state's data breach notification law kept with the plan.
- Plans for preservation of information to assist in the breach investigation such as gathering all logged data and taking impacted devices off-line
- Steps to resume operation

You should do annual reviews of the plan, including (at least) tabletop exercises where you go through various scenarios, adding and subtracting issues and problems (managing partner is climbing a mountain in Asia and inaccessible, the electric grid is down, etc.).

The Right Technology at the Right Price

So . . . you're not a mega law firm and you are budget conscious. No worries, it's a big club. So here is our basic technology advice with this stern warning: No technology is invincible.

Let's start with some simple and free advice. Make sure you apply all patches and updates as they become available. Failure to patch leaves you vulnerable to a security incident. Trust us, the bad guys are constantly scouring the Internet looking for those that are vulnerable to a known hack.

Obviously, you need some sort of endpoint protection. This means there should be some sort of security software installed on all your computers, servers and mobile devices. In the old days it was called anti-virus software, but today's endpoint protection is really a security suite that contains such things as a firewall, anti-malware protection, anti-virus, encryption, etc. Endpoint protection is a good start, but you really need some vision into events happening at the endpoints. According to a report by Sophos and market research company Vanson Bourne, one in five IT managers didn't know how an attacker got in, even after discovering the threat. This has given rise to Endpoint Detection and Response (EDR) tools to provide vision into security events.

Another important concern is edge protection. This is where you would install some sort of firewall appliance. One of our favorite products (no we don't get any commissions) is the

Meraki product line by Cisco. The Meraki is a combination firewall, intrusion detection system (IDS), intrusion prevention system (IPS) and wireless access point (AP). The device itself is only a few hundred dollars and the annual subscription for the software is only a few hundred dollars as well. Best of all, the subscription includes continuing updates to your protection as new threats are discovered – and they happen automatically – you don't have do a thing or spend another dime. You may recognize the combined functions from the old days of unified threat management (UTM) devices. You don't see the UTM term used these days, but effectively that's what devices like Meraki are.

Another area to focus on is mobile device management (MDM). It is no secret that we are a mobile society and our smartphones are really powerful computers that can also make phone calls. Larger firms will invest in MDM solutions such as Airwatch, Mobileiron or Microsoft's Intune. We would suggest that the solo and small firm lawyer look to the built-in controls contained in Active Sync. If you have your own Exchange server or use Exchange Online with Office 365, Active Sync is a free feature that can enforce device encryption, enforce lock codes and even remotely wipe the device.

Final Thoughts

As we write this the week after coming back from speaking at ABA TECHSHOW®, we are reminded that much of the cybersecurity advice above was echoed there. One of our favorite slides had the words "Store Less. Delete More." That might have been the best, most succinct advice we heard during the conference. Words to live by!

Sharon D. Nelson, Esq. 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 a co-author of 17 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 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.