Cybersecurity Basics

by Sharon D. Nelson and John W. Simek

Cybersecurity is a hot topic these days, but what does it mean to practicing lawyers today? Essentially, cybersecurity is the protection of your information systems from theft or damage. For an attorney, that means making sure your client's information stays confidential. Today, that includes taking steps to protect yourself from experiencing a data breach.

Are lawyers doing enough to safeguard law firm and client information? Our opinion is that many are not. Here are a few reasons we hold that opinion.

- The FBI reported at a legal technology conference in 2013 that they are seeing hundreds of law firms being increasingly targeted by hackers.
- Mandiant, now part of InfoSec giant FireEye, reported that 7% of the breaches it investigated in 2014 involved law firms.
- Another report noted that 80% of the largest 100 law firms, by revenue, had been hacked between 2011 and 2015.
- At a meeting of large firm information security experts from D.C., most admitted that they had been breached – and that they were aware from their colleagues that others had been breached as well.
- Even with the dismal record of reporting law firm data breaches, we still learn of them in the press and informally – and we will detail some of them for you.

While data breaches can happen despite reasonable (or even stronger) security, the frequency of law firm data breaches and reports on how some of them have occurred suggest that many attorneys have not been employing reasonable safeguards. Why do many otherwise competent lawyers fail so miserably in protecting firm and client data? Here are some of the reasons.

- Ignorance—they simply need education – and many of them don't know they need education.

- The "it can't happen here" mentality is flatly wrong. Since the FBI issued an advisory in 2009 warning that law firms were specifically being targeted by identity thieves and by those performing business espionage, it has continued to meet with large firms to preach the gospel of information security. We were, in earlier days, worried about cybercriminals, China and other state-sponsored hackers, which continue to be major threats. Thanks to Edward Snowden, we now know that we also need to worry about surveillance by our own government.

- According to press reports, lawyers and law firms are considered "soft targets"; they have high value information that's well organized and frequently have weak security – although we are happy to report that, at least at large firms, cybersecurity is now a pretty high priority.

- Though there are many low cost/free measures that solo and small firm lawyers can take to protect sensitive data, true information security, including hardware, software, training, etc. is expensive. Protecting the security of client data can present a big burden for solos and small law firms. This does not take away a lawyer's ethical duty, however, and it is one reason the authors lecture so often on computer security. Once a lawyer sees the most common vulnerabilities, he or she can take remedial steps—or engage an IT consultant to do those things that are beyond the lawyer's skill.

- The need for vigilance never stops. You cannot secure your data once and think you're finished; the rules of information security change on close to a daily basis. Certainly, someone in the firm needs to keep up with changes regularly or the firm needs to engage a security consultant to do periodic reviews. While the necessary frequency of security assessments depends on the size of the firm, the sensitivity of the information and identified threats, it is our judgment that mandatory assessments should be conducted at least annually. And clients are beginning to demand self-audits or third-party audits of law firm security. Sensei has never seen a client who passed such an audit on the first go-round. In fact, they don't even understand the audit questions, which doesn't bode well for the results.

Detect and respond

In a more innocent time, we really thought we could keep the barbarians outside the walls that guard our data. Alas, those days are gone. For years, the emphasis was on preventing villains – cybercriminals, state-sponsored agents, business espionage spies and hackers – out. We went from fairly simple anti-virus software to sophisticated anti-virus software and, finally, to enterprise anti-malware software security suites.

The products got better and better and better. Sadly, what we learned is that all the would-be intruders were not only matching the good guys step for step, they were outpacing them.

It took a surprisingly long time for everyone to "get it" – but in the end, we realized that if the bad guys are smart enough and target a particular entity, they are going to successfully scale the walls we built to keep them out. And with that realization, "detect, respond and recover" became the new watchwords in cybersecurity.

Mind you, we are still trying to keep the bad guys out – that is our first line of defense. But now that we know that our first line of defense is a Maginot Line for sophisticated attackers, we have moved forward in our thinking.

The NIST Cybersecurity Framework

In February of 2014, we had begun moving forward toward securing our data and the physical infrastructure protecting it when the National Institute of Standards and Technology released Cybersecurity Framework Version 1.0.

The framework provides a structure that organizations, regulators and customers can use to create, guide, assess or improve comprehensive cybersecurity programs. This came as a result of Executive Order 12636, issued in February of 2013, which called for "the development of a voluntary, risk-based Cybersecurity Framework—a set of existing standards, guidelines and practices to help organizations manage cyber risks. The resulting framework, created through public-private collaboration, provides a common language to address and manage cyber risk in a cost-effective way based on business needs, without placing additional regulatory requirements on businesses."

The framework allows organizations—regardless of size, degree of cyber risk or cybersecurity sophistication—to apply the principles and best practices of risk management to improve the security and resilience of critical infrastructure.

The document is called "Version 1.0" because, much like our Constitution, it is supposed to be a "living" document which will be updated to reflect new technology and new threats - and to incorporate "lessons learned."

Here is where you find the magic words of the document, "identify, protect, detect, respond and recover" that should shape any law firm's cybersecurity program.

"Identify and protect" was where we started in the early days of cybersecurity – and while those words are still important, "detect and respond" have surged forward as a new focus – along with, of course, recovering from security breaches – no easy task. It is especially tough if you don't know you've been breached – and the average victim has been breached for seven months or more before the breach is discovered!

What Does "Detect and Respond" Mean for Law Firms?

It means rethinking how you approach security of your data. Now that you know that you can't keep a determined intruder out, you know you need to detect them once they've penetrated your network. So you need technology and software that will help you detect that you've had what is called, in polite circles, "a cybersecurity event" – translate that to "a breach."

As you can imagine, you want to know of these "events" as soon as possible so you can take action. Today, there are technology solutions that identify "anomalies" in your network (things that are outside the norm) or that look for executables that are unknown but are behaving like malware or some other form of cyberattack. While some of the solutions may be beyond the need or the budget of solos and very small firms, you don't have to be very large to start considering heading down this road – the risks of not doing so are simply too great. The good news is that there are technical solutions that are very affordable and would be a good starting point for the solo and small firm attorneys.

Some of the solutions include data loss prevention (DLP) software and appliances, intrusion detection systems (IDS), intrusion prevention systems (IPS), electronic content management systems (ECMs) and Security Event Management systems (SEMS). When you meet with someone who can explain the various solutions to you, brew a pot of expresso – you're going to need to be highly focused to understand how one solution differs from another – this is really cutting edge technology that changes from month to month (if not day to day).

For the solo and small firms, we recommend that you start by investigating intrusion detection systems. An intrusion detection system watches network and system activity and alerts you if there appears to be some malicious activity. It begins by creating a baseline of network traffic. Any suspicious activity outside of the configured parameters (e.g. 10% additional network bandwidth utilization) causes an alert, which is typically an e-mail message to an administrator. One of our favorite IDS products is Meraki by Cisco. It is subscription based and only costs a few hundred dollars a year. The hardware itself is a few hundred dollars and then you only have to deal with annual subscriptions after that. The system is cloud based and updates are automatically delivered and installed. The updates are based on the activity seen by all the Meraki devices in the Cisco network. In other words, you take advantage of having fixes applied based on malicious activity that someone else may have experienced. Need to say, Cisco is a very trusted brand.

As for your response to your incident, that may vary. After the initial panic, you will want your in-house or outside technology consultants (and you are likely to need digital forensics technologists, who are more familiar with data breach investigations) to take a look at the situation and see what they can determine. They can also, once they understand what has happened, figure out how to “plug the hole” and otherwise mitigate the breach. Remediation of whatever caused the breach is key.

Hopefully, you already have an incident response policy and plan in place, no matter how big or small you are. For all but the smallest firms, there should also be an incident response team in place to implement the plan. At a minimum, you should have already identified who will be involved along with their appropriate role.

In all probability, you will want to call a lawyer familiar with data breach laws who can advise you on complying with any of the 47 state data breach notification laws. And if there is data protected by federal law (such as HIPAA data), you’ll need advice on that front too.

Finally, one of the first pieces of advice you are likely to be given is to call the FBI. While that is anathema to most law firms, it is the appropriate course of action. Remember that the FBI makes no public statements about these investigations and doesn’t show up in flak jackets or otherwise make a public display of your “cybersecurity event.” You can determine which FBI office to call by performing a Google search for “FBI regional offices” and entering your zip code.

The ABA Cybersecurity Resolution

The ABA has weighed in on cybersecurity concerns, always a sign that the states may follow. On August 12, 2014, the ABA House of Delegates passed, without opposition, a cybersecurity resolution, Resolution 109, which reads as follows:

RESOLVED, *That the American Bar Association encourages private and public sector organizations to develop, implement, and maintain an appropriate cybersecurity program that complies with applicable ethical and legal obligations, and is tailored to the nature and scope of the organization, and the data and systems to be protected.*

You might be forgiven for thinking as you read the resolution, “Wow, that really says a whole bunch of nothing.” And you’d be right – it is really a cautionary resolution intended to raise awareness.

There is a back story to the resolution, which was much larger in its original format. The original resolution appeared to command all law firms, large and small, to come up with a cybersecurity program that met national and international standards.

This met with fierce opposition from a number of ABA entities, including our own Law Practice Division and the GP/Solo Division. The resolution was submitted by the ABA Cybersecurity Legal Task Force and the Section of Science & Technology Law.

In answer to the controversy, the language of the Resolution (which stands on its own and is not governed by the accompanying Report) was watered down to the tepid version above. At the behest of other entities, language in the Report was also changed to make it clear that the Resolution was not attempting to make a change in lawyers' ethical duties and to add language recognizing that smaller firms could not be expected to adopt a program that made no sense considering their size and budget constraints.

Clearly, for small firms, the international and national standards cited in the Report appeared fearsome. There are standards for smaller firms like the NIST standard mentioned above.

The report states: "Small organizations, including small law firms and solo practitioners, can prioritize key cybersecurity activities and tailor them to address the specific needs that have been identified." For help with this, you might check out NIST Interagency Report 7621: *Small Business Information Security: The Fundamentals*." Written in 2009, it's a bit dated, but many fundamentals remain the same. As an example, target hardening is one of the sections. It would seem pretty obvious that you should be beefing up your security in order to reduce the chance of compromise, but most people just set it and forget it.

Cybersecurity worries

There are lots of cybersecurity worries to give you the willies in the wee hours of the morning. Here are a few of the most common ones we see.

<u>Ransomware</u> – We continue to see law firms struck by ransomware (one hit in our neck of the woods while we were proofing this article) which encrypts your data followed by a demand for payment – usually in bitcoins – to get your data back. Training your employees not to click on suspicious attachments or links in e-mail will help. They need to stay away from suspicious sites as well since ransomware can be installed by just "driving by" an infected website.

Overwhelmingly, from a technological standpoint, you can defeat ransomware by having a backup that is immune to it. This can mean, particularly for solo lawyers, that they backup to an external USB drive and then disconnect the backup from the network. If you leave it connected, the ransomware will encrypt your network AND your backup. For others, it means running an agent-based backup system rather than one which uses drive letters or network shares. Make sure your IT consultant has your backup engineered so that backups are protected – that way, even if you are attacked with ransomware, you can thumb your nose at the demands for money because you can restore your system from your backup (which means backups need to be made frequently to avoid any significant data loss – there should always be a good backup which is NOT connected to the network).

Employees – Employees are by nature rogues. In every study that's been made, they will ignore policies (assuming they exist) in order to do what they want to do. This often means they bring their own devices (BYOD) which may be infected when they connected to your network. They may also bring their own network (BYON) or bring their own cloud (BYOC). Certainly your policies should disallow these practices (in our judgment) or at least manage the risks by controlling what it is done by a combination of policies and technology.

They also steal your data or leave it on flash drives, their home devices, etc. This means you have "dark data" – data you don't know about and over which you have no control. This means you may miss data required in discovery because you don't know it exists. Your data may not be protected in compliance with federal or state laws and regulations. And you have no way to manage the data because you don't know it is there. Once again, a combination of policies and technology should be in place to prevent these issues.

Targeted Phishing – This is perhaps the greatest and most successful threat to law firm data. Someone has you in their sights – they often have done research on your law firm. They may know what cases you are involved it – and who your opponents are. They may know the managing partner's nickname. Everything they know about you they may use to get your click on something (say, an e-mail from an opponent referencing a specific case and saying "The next hearing in ___________ case has been rescheduled as per the attachment.") Many a lawyer has clicked on such attachments – or a link within an e-mail.

The best solution to protect yourself from targeting phishing is training – and more training – endlessly. One California firm had multiple target phishing attacks but survived them because attorneys and staff who receive such e-mails questioned their authenticity. Forget the loss of billable time. The loss of money, time and even clients due to a data breach can be far worse.

Interception of Confidential Information – Start with the proposition that everyone wants your data, including cybercriminals, hackers and nation states (including our own). Frankly, if they want your data and they have sophisticated tools, they will get it. So shame on you if you are not employing encryption (which is now cheap and easy) to protect confidential data via voice, text, and e-mail. Encryption, today, is a law firm's best friend. You may choose to use it always or in cases where it is warranted – but you surely should have the capability of encrypting.

Failure to Use Technology to Enforce Passwords Policies - First, let us say that you should use multi-factor authentication where available and use it to protect sensitive data. But failing that, we recognize that passwords are still king in solo/small/mid-size firms.

Therefore, have your IT consultant assist you in setting up policies that can be enforced by technology, requiring that network passwords be changed every 30 days, not reused for an extended period of time

– and mandating strong passwords, 14 or more characters in length, utilizing upper and lower cases letters, numbers and symbols. Passphrases are best. 1lovepracticingl@w2016! would do nicely.

How are you going to remember all of those unique 14+ character passwords? This is where a password manager is your friend. Password managers store the data in an encrypted "vault" that is accessed using a very strong master password. You put all your logon information into the software database where it is stored as encrypted data. Some password managers can store a wide variety of data and not just user name and password. Some will automatically fill in the login information without you typing a thing. Some can store additional information such as credit card numbers, passport information, prescriptions, frequent flyer numbers and any other desired information. Finally, when selecting a password manager, you'll need to decide if you want the encrypted password vault to be stored in the cloud on locally on your device. Either one is acceptable since the data is encrypted with a password you define.

One Last Shot Across the Bow

While it is true that "Detect and Respond" has set off a hue and cry, never forget that it is best for your law firm if you really can keep the barbarians outside the gates. We were reminded of this as we were writing this article - a news article appeared on our newsfeeds telling us that another law firm had suffered a data breach after a firm backup disk (apparently unencrypted) had been stolen from an employee's locked car trunk. The best defense we currently have to protect law firm data is encryption. "Detect and Respond" is a mantra you need to adopt but don't make the mistake of failing to adequately protect your data. Encryption is a law firm's best friend when it comes to risk management. If you haven't deployed encryption everywhere, now is the time. As a point of interest, Google is marching full steam ahead with its encrypt everything program. That's a good cue that you should be doing the same thing.

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