How Law Firms Should Strengthen Cybersecurity to Protect Themselves and Clients

By Amy Terry Sheehan and Jill Abitbol
The Cybersecurity Law Report

Law firms store a wealth of sensitive and confidential information electronically, making them prime targets for hackers. Not only does weak data security affect business development and client retention for firms, but can result in legal and ethical violations as well. How can firms meet clients' increasing data expectations? How can clients determine how robust their current and potential firms' systems are? What mistakes are law firms making? John Simek, vice president and co-founder of cybersecurity and digital forensics firm Sensei Enterprises, Inc., answered these and other questions about law firm data security in a conversation with The Cybersecurity Law Report. See also "Sample Questions for Companies to Ask to Assess Their Law Firms' Cybersecurity Environment" (Jun. 17, 2015).

CSLR: What are the specific cybersecurity threats that law firms currently face?

Simek: Probably the most prevalent threats that we're seeing now, and not necessarily targeted ones, involve ransomware. At the end of last year, in the northern Virginia area alone, there were four law firms that got hit with ransomware attacks in just one month.

The key is for firms to make sure that their backups are engineered properly to recover from a ransomware infection. Then they are in a position to restore their data without

having to pay the ransom. Of those four law firms that were hit with ransomware at the end of last year, two were engineered correctly and two were not.

[See "How to Prevent and Manage Ransomware Attacks" Part One (Jul. 15, 2015); Part Two (Jul. 29, 2015).]

CSLR: What do you recommend to firms that have not yet proactively engineered proper backups?

Simek: I tell solo practices and small firms, which tend to use external hard drives for backup, to disconnect that device after they've done their backup. That way, in the event their system gets infected, it won't impact their backup. If their external drive is still connected to their computer, and their computer gets infected, their backup is going to get infected too. It's a very simple thing. There's no cost to doing that. It's just a procedural piece.

I recommend hardware-based backup solutions for mid to larger firms. Hardware-based, also called agent-based, backup is not seen as a drive letter or a network share. The data is moved via software to the backup device.

CSLR: Do you recommend that firms use cloud backups?

Simek: Cloud backups are good as well. The key in cloud backups, and particularly for attorneys because of their ethical duties to protect the confidentiality of the data, is to select a cloud solution where the firm can control the encryption key. Not all backup solutions and cloud solutions will allow users to do that.

Carbonite, which is used by a lot of solo to mid-sized firms, allows users to define the encryption key themselves. Some cloud providers do not want users to do that because they fear that if the user forgets the encryption key, their backups will be useless. Although that is certainly a possibility, if a firm is planning to use a cloud-based backup, it will want a

provider that allows it that control.

OneDrive, for example, does not allow users to define what that encryption key is. So that means that Microsoft can decode data stored in the cloud if it wanted. With Apple iCloud, Apple also can decode backup content. Apple actually can read iMessages and related content, even though it's stored encrypted.

From an attorney's perspective, the ability to define the encryption key is a crucial differentiator, and something they should look for in a cloud solution.

[See "Implementing an Effective Cloud Service Provider Compliance Program" (Nov. 25, 2015).]

CSLR: In addition to the backups, what other steps should law firms currently be taking to address security threats?

Simek: Training employees is crucial. Phishing attacks, such as emails where someone is trying to get an employee to wire money to a foreign bank, make up a large percentage of threats. The solution there – and firms tend not to want to do this – is to train employees. The people are the problem. An email message that has a malicious attachment or a malicious link in it won't have any adverse effect unless someone clicks on it.

Firms have to educate their employees because all of the technology in the world is not going to prevent an attack. Threat actors may be smarter than the current security technology. They may be using malware that nobody has ever seen before, and your firm may be the first kid on the block to get it.

Threat actors can also get information from court filings, which are public record. Somebody can jump on Pacer and find out the name of the case and the attorney of record. They can then send an email message that purports to come from the

attorney of record using a bogus email address or a fake domain and say “Here’s an updated complaint in such and such a case.” The receiving attorney will recognize the email and click on the attachment. Through training, firms can teach employees how to recognize and prevent these types of situations.

[See “Designing, Implementing and Assessing an Effective Employee Cybersecurity Training Program (Part Two of Three)” (Mar. 2, 2016).]

CSLR: What about firms that are reluctant to invest in training because it is non-billable?

Simek: Well, it can cost them so much more to clean up and recover from an infection, even if it’s reputational damage, than it would to educate their employees.

We see the larger firms now starting to invest more money in preventing threats. They’re beginning to see the value of what that training can do.

Some firms have gone so far, and I think this is good, as to test their employees by sending intentional phishing messages to see how many people click on what. Employees are then scored and the firm uses those scores to evaluate whether certain employees need one-on-one education.

CSLR: Are there any other important security measures that firms should be taking?

Simek: Patching vulnerabilities and updating are two important measures. The number one reason that firms get compromised is they are not applying patches. When you don’t patch your operating systems or your software, you’re susceptible. It doesn’t cost much to do that.

The second reason is use of outdated software. Firms don’t want to spend money to update and this makes them vulnerable

to attacks. They're still running Windows XP, which is not supported. They're still running Internet Explorer. Internet Explorer 10 and below are no longer supported. I don't know if a lot of law firms know that yet. There was an article several years in *The New York Law Journal* that said that continued use of Windows XP is unethical. So, firms have to upgrade their software and they have to spend money to do that.

CSLR: What should clients expect from a law firm and would you say that client expectations are a driver for change?

Simek: Client expectations are definitely a driver. Law firms would be reluctant to spend money on security unless clients were expecting it. The firms that are more advanced with security and related certifications will even use that as marketing plug.

We are starting to see clients hand prospective or current firms an IT security assessment, or some sort of questionnaire, and ask them to complete and submit it as a condition of their provision of legal services to the company. Depending on the client or the firm, the client may require an independent third-party audit.

So yes, definitely, it's the clients that are driving change and enforcing it primarily through these audits.

[See "Designing and Implementing a Three-Step Cybersecurity Framework for Assessing and Vetting Third Parties" Part One (Apr. 8, 2015); Part Two (Apr. 22, 2015).]

CSLR: Are companies treating law firms like any other third-party vendor in terms of the security audit or vetting questionnaire?

Simek: It depends, I think, on the industry and who the client is. The questionnaire or audit can be very targeted, and maybe even more stringent, for law firms because the data that companies are giving to the law firm may be extremely

valuable. This is not payroll data. This is not somebody that's just cranking out W2s for the company, for instance. This is patent information, merger and acquisition information and other confidential data. Depending on the value of the information, the client may be a lot harder on the law firm than they would on some other third-party provider.

CSLR: How does the completed questionnaire or audit get used by the client and/or the law firm?

Simek: The results of the audit might demonstrate to the law firm that it is deficient in certain areas of security and it might then communicate its plan to remedy those deficiencies to the client. Especially if it's a larger client, firms want to do what they can to keep them.

CSLR: What certifications should law firms have in place?

Simek: I think it depends on the size. Big firms are obtaining ISO [International Standards Organization] 27001 certification, which costs a lot of money and takes a lot of time. The mid to smaller firms are not going to be able to afford to do that but there are other things that they can do, like self-certification. NIST [National Institute of Standards and Technology] has small business standards that firms can follow, which will at least help assess their infrastructure, and whether they have any weaknesses and whether the assistance of a third-party is needed.

CSLR: Is data security handled differently depending on practice area?

Simek: It can be. It depends on the value of the data. Whether it is a law firm or a corporation, a risk assessment needs to be conducted to determine the value of the data being held and the risk of losing it. That information will define how much the firm is going to spend or what efforts the firm is going to make to protect the information or mitigate risk.

CSLR: When is it appropriate for lawyers to use encryption in their communications?

Simek: We're at the stage now where every lawyer should at least have encryption capability, which includes the ability to encrypt communications and the ability to encrypt data at rest (for instance, when putting data on a flash drive).

Encrypted communication is easier today than it used to be. There are now many services that actually manage the encryption communication mechanism. Voltage and Zix are two such services. It can be as simple as clicking on a button in Outlook that says "Encrypt and Send."

To save money, we advise smaller firms that only need to communicate in encrypted form once in a while to put the confidential information into a Word document, and then password protect that Word document. The password protection encrypts it. This can also be done using Adobe Acrobat or a WinZip file. The confidential information can then be sent as an attachment, and a separate communication would be used to transmit the password.

Firms that receive medical information or PII that falls under HIPAA may use Zix, but they can have the filter set to recognize any medical information or PII content, and then the service will automatically encrypt that message to send it.

CSLR: Are clients being more selective about the data that they're giving to the law firms in the first place?

Simek: Not really. They're not withholding the data. They're just asking and making sure that the law firm is prepared to receive it and to properly protect it. Absent that assurance, there's the likelihood the client will find another law firm.

CSLR: What types of remote access or mobile device policies should law firms have in place?

Simek: For anything related to the data the firm holds or the firm's infrastructure, employees should know what is expected of them, what they should do, what they are allowed to do, and within what boundaries. This would require policies on remote access, computer usage, social media, internet usage, email, bring your own device, bring your own network and bring your own cloud.

The necessary policies are unique for every firm depending on the type of practice and type of attorneys. There is no template. To be effective, the policies need to be customized for every firm.

[See "How to Reduce the Cybersecurity Risks of Bring Your Own Device Policies" Part One (Oct. 14, 2015); Part Two (Nov. 11, 2015).]

CSLR: What is the biggest challenge you face when you are asked to respond to an incident?

Simek: Capturing data. The number one thing that we run into when we respond to these things is that there is minimal logging, if any, going on. Nobody had the foresight to configure their devices or their systems to capture information on an ongoing basis. That's a killer for the investigations.

CSLR: Why are lawyers or firms not configuring their devices or systems to capture information?

Simek: Because the default is not to. All these devices, systems and applications have the ability to capture information but it's not turned on by default.

CSLR: In the event of a security incident, when and how should a law firm contact its clients?

Simek: You just hit on a real touchy nerve. If you ask a lawyer or a managing partner, they'll say they never want to

tell the clients. However, 47 states have data breach notification laws. The unfortunate part is that most lawyers don't want to conform to them, even if they're legally bound to. They're also ethically bound to notify clients of a data breach.

But whenever a law firm gets breached, the argument I always get is "Well, but we don't know with 100% certainty what data was accessed." Yeah, that's true. You don't know with 100% certainty, but you've got a pretty good idea. And in some cases, when there is notification of clients, the clients aren't anxious for the breach to be made public.

In some instances, the client will insist on contract terms that set forth the number of days or hours within which they should be notified of an incident.

[See "Synthesizing Breach Notification Laws in the U.S. and Across the Globe" (Mar. 2, 2016).]

CSLR: Have clients and law firms been able to get to a place where both sides are comfortable on the data security issue?

Simek: It has been a wake-up call for a lot of firms. We are seeing firms use client surveys and audits to detect and remedy security deficiencies. By doing that, they are maintaining client relationships.