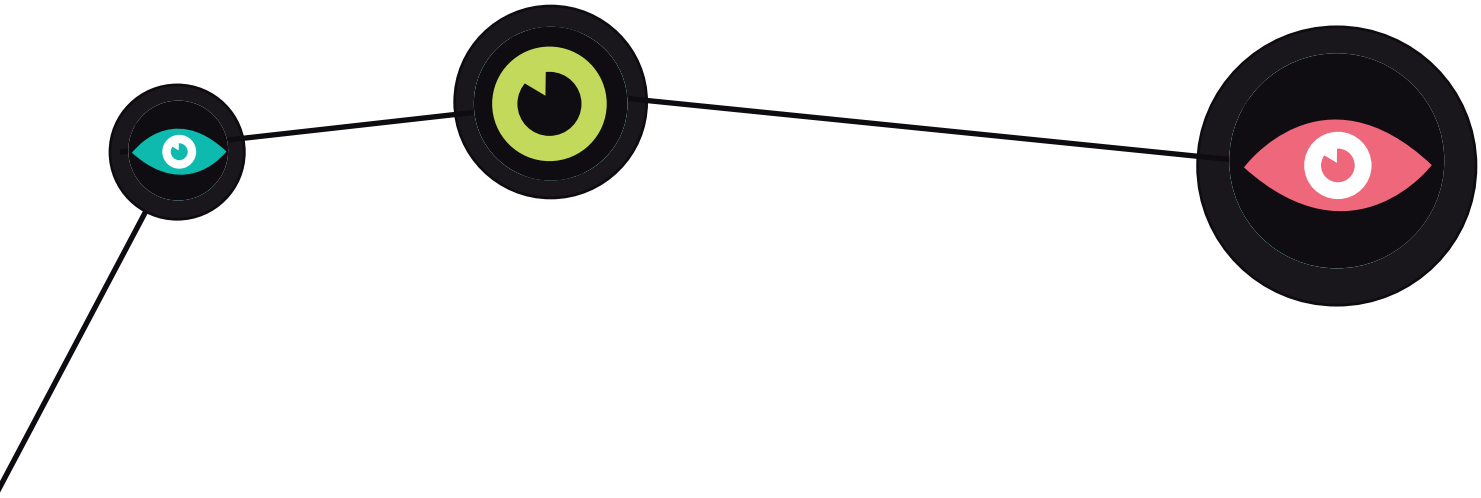
What Law Firms Can Do To Protect Themselves Online

ANDRES HERNANDEZ



The lifeblood of a law firm is the information—often incredibly sensitive information—that flows through it. Clients expect lawyers to keep their confidential information from falling into the wrong hands, and law firms that cannot do this will soon find themselves out of business. Even beyond the goal of maintaining security to keep clients happy, lawyers have a legal and ethical duty to protect this information and can face severe repercussions if they are not able to do so.

Unfortunately, for all the good that it has brought to law firms, the digital age has also invited in a host of additional risks that can leave data vulnerable in ways that you may not even realize. Cybercriminals are realizing this in increasing numbers. According to cybersecurity firm Mandiant, 80 of the 100 largest law firms in the country have been hacked since 2011, and 14 percent of respondents to an American Bar Survey in 2014 said that their firms had been the targets of cyberattacks that year alone.

Why are law firms such an attractive target? Two reasons.

1. They have incredibly sensitive information, often from a number of large businesses in a wide array of industries. Attackers use this information in a variety of ways: Sometimes they ransom it back to companies; other times, they sell it to whichever competitor is willing to offer the most money; and on certain occasions, they may simply release information to the public that the company in question would rather keep private.
2. Overwhelmingly law firms are behind the curve when it comes to digital security. In the most recent study from the International Legal Technology Association (ILTA), conducted in 2013, firms were expected to have "woken up" to the issue, but they were still doing shockingly little.

- 90 percent weren't using any laptop tracking technology.
- 76 percent still weren't using two-factor identification.
- 72 percent weren't using encrypted USB drives.
- 64 percent didn't automatically encrypt content-based emails.
- 64 percent had no intrusion-prevention tools.
- 61 percent had no intrusion-detection tools.
- 56 percent didn't encrypt laptops.

While another two years have passed since this study, giving law firms ample time to improve on their security, it should be noted that the largest improvement from the ILTA's previous, 2011 study showed only a 12 percent reduction in that two-year period. In several areas, firms made no improvement or even got worse.

Law Firms Need To Understand the Threat Before They Can Fight It

Part of the problem may be that many law firms still do not understand the potential threat that they face, or they believe that they are small or private enough that hackers simply won't notice them. Sadly, this is not the case. A number of today's cyberterrorists even specialize in going after small and medium-size businesses, with law firms a particularly lucrative target.

How exactly can law firms get hit?

Spear phishing. This is essentially the more advanced version of the email virus that most of us are familiar with. It is called spear phishing because the people and organizations that employ this technique tend to aim it at a specific target and engage in research before sending out emails. This research makes their emails seem incredibly legitimate, encouraging people on the receiving end to open them. Once the email is opened, a virus or other malware is automatically uploaded to your system.

Ransomware. This is a specific type of malware designed to lock your computer systems and encrypt your data. It comes with a "ransom note" demanding that you pay money if you want to be able to access your data again. Ransomware can come via an email attachment or be downloaded from the Web by masquerading as any number of things. This particular type of cyberattack has become prevalent enough for law firms that it was actually featured in an episode of the TV show *The Good Wife* this past season.

Fake apps. When an application becomes popular, it's almost a requirement for knockoffs and fakes to show up in the app stores. Not only does this make it difficult for people to know which application is the real deal, many of the fakes carry with them vicious malware designed to sneak onto your system and take over. This one is particularly dangerous for law firms that allow their employees to use their smartphones or tablets for work, because attackers would then have access to anything that the infected device can see.

Malicious social network links. Because the vast majority of people now know to watch out for email viruses, cybercriminals have migrated their attacks over to social media sites. Some of these may

come in the form of codecs that you need to download to watch videos, while others appear in messages that seem to be from friends you trust. This is another one for law firms to watch out for, because employees access their social media accounts from work computers all the time, and it only takes one person making one mistake to get infected.

Obviously, these are just a few of the ways attackers can try to worm their way into your system. Law firms with minimal security may even have to deal with direct attacks, in which criminals simply hack into their network from the outside and access any information they want.

Specific Security Measures Your Firm Should Employ To Protect Itself Online

What can you do to protect against these kinds of threats? All law firms are different, and the security controls that work for one firm may not be enough for another—or may not offer the right kind of protection. Thankfully, a number of options are available no matter what your needs are, including:

Create a strong password policy. Did you know that passwords with fewer than eight characters can be cracked in just a few minutes? Or that passwords are often the first—and last—line of defense against hackers? While it's true that any password can be hacked, given enough time and resources, all of them are definitely not created equal. Make sure your employees:

- *Use at least 15 characters.* That's the number that experts recommend. Long passwords are not invulnerable, but they do tend to be a lot harder to crack, especially if the attackers in question are employing a brute-force program that checks all possible password combinations. Simply adding a few more characters can be the difference between your password getting cracked in a few seconds or minutes to literally years. A 15-character password may seem like a pain, but it's a lot better than having to deal with the fallout of a security breach.
- *Don't use the same password.* Yes, it's difficult to remember a bunch of different passwords, but going with one password for everything just isn't smart. We know this, but it's easy to convince yourself that you're the exception—especially if the one password you come up with is a really good one that seems like it couldn't be broken. Here's the problem with that logic: Cybercriminals don't necessarily need to crack your password to gain access to it. A common technique they employ is to go after sites with low levels of security and steal passwords and email addresses. Armed with this information, they can track you down and attempt to log in to your work accounts.
- *Stay away from common phrases.* Many people think that they are being clever by choosing a completely random, everyday phrase and using it as their password. For example, something like "holdthedoor" seems pretty innocuous, right? Who could possibly guess that your password would be "holdthedoor" unless that's something that you go around saying frequently? Unfortunately, hackers employ programs that systematically go through common phrases like this to rule them out, so your super-safe "random" password could actually be easier to crack than one that's personal to you but uses some of the other tips here.
- *Switch passwords frequently.* This is another one that everyone knows but many people do everything in their power to avoid or put off. Force employees to change passwords regularly. Why? Because cybercriminals are known to hold on to passwords for months or even years before trying to use them so they can prevent getting caught. This is a strategy that shouldn't work, because we all know to change our passwords, but human nature puts us at risk.
- *Mix character types.* You've probably been asked to create passwords with at least one uppercase and lowercase letter or to add a number. Many sites are now doing this because it makes passwords more complex and therefore harder to crack. Special characters such as #, ^, and ! also go a long way toward making passwords harder to hack or guess. While you're at it, you can warn your employees of common issues to avoid, such as simply adding a number to the end of your password. Overwhelmingly, when people are asked to include a number, they put it at the end of the password, and hackers now account for this.
- *Don't just use the dictionary.* Another common technique is to flip through the dictionary, point to a word at random, and choose it as your password. But just like with common phrases, hackers have programs that systematically go through dictionary words to check them as passwords. Even replacing certain letters with symbols ("a" with "@," "E" with "3," and so on) won't protect you from more sophisticated attacks, because many programs are designed to check for these combinations as well.
- *Combine random (or seemingly random) words.* While security is all well and good, it can be incredibly difficult to remember a password if it's 15 characters long and more or less consists of gibberish. A good way to combat this while still creating an effective password is to combine several words together that seem random. For example, you could use the names of your last three bosses and then add punctuation: 3ThompsonMeiersWilson$. It's more than 15 characters, it has upper- and lowercase letters, a number, and a special character, and it should be

a lot easier to remember than something generated randomly. Even the 3 and the $ have meaning: three bosses who paid you money.

- *Utilize two-factor authentication.* Have you ever attempted to log in to a site or recover a password and are told that a special code needs to be sent to your email account or mobile phone? That's two-factor authentication, and it can go a long way toward keeping cybercriminals out of your system because of the extras steps required and the information that they would need to possess.

Do your due diligence with cloud vendors. The cloud is a necessary (and often incredibly helpful) part of doing business as a lawyer in the 21st century. It can enable you to access important information anywhere, increase efficiency, cut back on downtime, and generally just make your life easier. However, it also means that you're putting valuable information out there in the ether, and that can be a terrifying thought. Every company says that it's secure, but how do you know? What do you look for? Here's a sample of questions that you should ask when doing your due diligence with a potential cloud vendor.

- Does your application meet the functional requirements of our law firm?
- Will the firm need to change current organization workflows in order to use your app? How much?
- What is your privacy policy?
- How many customers do you have?
- What level of encryption do you offer?
- Is it possible to customize who has access to what parts of the application based on their role or even the individual?
- Can you provide me with case studies, references, and assessments done by third parties?
- What security measures do you use to authenticate users?
- Does your application integrate with other applications? Which ones? How does this integration work?
- May I see your Service Level Agreement (SLA)? You want to see an uptime guarantee included that is anywhere from 99.9 to 99.999 percent.
- What kind of compensation do you offer if you can't meet the uptime guarantee? Is it automatically offered, or does it need to be requested?
- Are any independent security vendors brought in to vet how secure your product is?
- What are your data ownership terms? How does this work with metadata I generate while using your application?
- Are you compliant with all of the regulations that apply to our firm?
- Is Application Protocol Interface (API) access offered? Does this cost extra?
- Can you provide me with your physical location and phone number?
- What is your disaster recovery strategy? How often do you test it?
- Are data fields customizable? What field types exist? Can more fields be added?
- Do you use geographically distributed data centers for applications and data? How many? Where are they?
- How does security work at your data center(s)? How many people will have access to my data? How are those people vetted before they receive access?
- How frequently do you upgrade the application? How will my use of the application be impacted during this time?
- How many backup copies of data do you create? How often is data backed up?

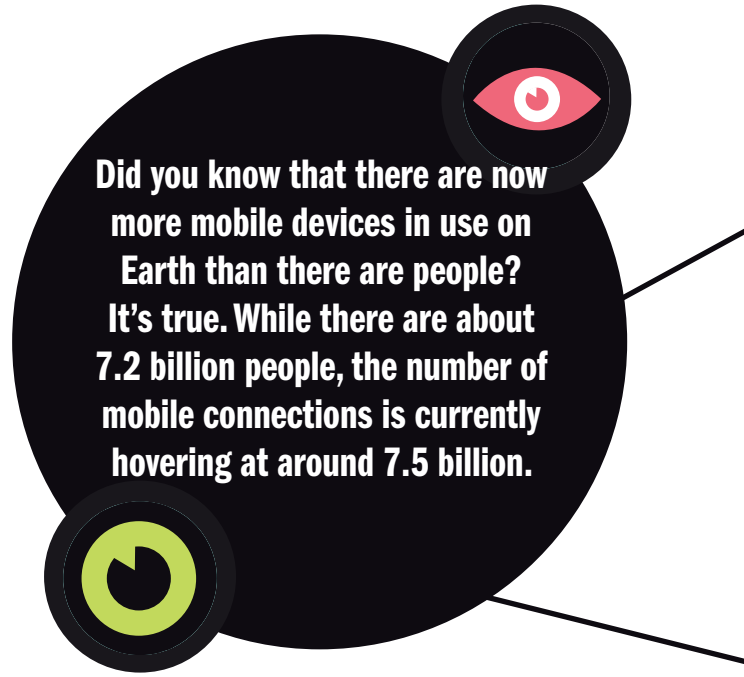
Take the time to get answers to all your questions before committing to a cloud vendor.

Come up with a BYOD (Bring Your Own Device) policy. Did you know that there are now more mobile devices in use on Earth than there are people? It's true. While there are about 7.2 billion people, the number of mobile connections is currently hovering at around 7.5 billion. Moreover, almost two-thirds of Americans have a smartphone, and most of them never want to be more than a few feet from it. Admittedly, that last part doesn't have any statistical basis, but it certainly feels true, doesn't it?

With so many people carrying around their own personal computer in their pocket, it should come as little surprise that many prefer to use it for work rather than being assigned a company-provided device. After all, they're comfortable with their device. Why learn something new if they don't have to?

Law firms have largely acknowledged this and allowed their employees to bring in their own devices and use them. This is understandable; what isn't understandable, though, is the fact that so few firms have enacted security policies for how these outside devices can be used and what kinds of protections they need to have. If you are going to allow employees to use their own devices for firm business, it is imperative that you do this. Some no-brainers include:

- *Make it clear what devices are allowed.* It seems like this should be obvious, but it's never wise to assume. If your security works well with smartphones but not with tablets, or if you are compatible with Android devices but not iOS, make it clear in your policy.



- *Company data must only be sent through corporate email.* This one is pretty self-explanatory.
- *Require mandatory password protection.* You've got a specific password policy for firm-owned devices, right? Well, that same policy needs to be extended to cover employee-owned devices. They need to have a password on their mobile equipment, and it needs to adhere to firm standards, or they can't use it for work.
- *Demand encryption.* All employee mobile devices used to access firm data need to be encrypted to the standards of the firm. Additionally, passwords must be stored in an encrypted password store.
- *Assert your right to wipe.* If an employee's device is lost or stolen, you need to be able to wipe the data so you don't suffer a breach. Make it clear in your policy that you reserve the right to do this, because you'll be getting rid of all of their personal data as well as anything that pertains to the firm. One way to soften this blow is to offer information to employees on how they can back up and restore their personal data once the device is replaced.

Enact policies for dealing with lost or stolen devices. Attorneys have always taken their work home with them, but today this is easier (and more complicated) than ever before. Rather than smuggling out legal briefs, lawyers now are much more likely to grab their laptop, tablet, or smartphone. But what happens when one of these devices with sensitive information on it is lost or stolen? Did you know that data breaches most often occur due to a device being lost or stolen? Because of this, it is vital that your firm have clear policies on what to do if a piece of hardware goes missing, as well as have security methods in place to protect you even if this does happen. Here are just a few:

- *Location tracking.* If the device in question doesn't already have remote location-tracking software installed, firms should have this added. In this way, it may be possible to find a device that has been misplaced and prevent a data breach from happening.
- *Remote wiping capability.* No matter how much you try to keep sensitive materials from falling into the wrong hands, all of that can be for naught if someone with high-level access loses his or her laptop or other device. Even a strong password and encrypted device won't stop dedicated hackers forever. Once they break into the device, they'll be able to see whatever they want—unless you add remote wiping capability. This safety measure allows you to completely erase all data from the device in question so that even if criminals manage to break in, they'll discover that all their efforts have been for nothing.
- *Data loss protection systems.* Let's say your associate was doing some work at Starbucks and needed to refuel. It was busy, and he didn't want to lose his seat, so he left his stuff—just for a few seconds— to get an espresso. The device couldn't have been out of his sight for more than 20 seconds, but apparently that was enough time. When he returned, it was gone. He calls in to the firm immediately to report the theft, but even in that short amount of time, the crook in question somehow managed to take the sensitive information that he was looking at and transfer it to an external Dropbox account. The resulting data breach is a huge embarrassment, and the worst part is that it could have easily been prevented—and not just by the associate taking his device with him in the Starbucks line. All that the firm needed was a good DLP (data loss protection) system in place. DLP systems are designed to keep an eye on confidential information. If an employee attempts to transmit a file somewhere it shouldn't be going, the DLP would detect this and block it from happening. In other words, even with the associate's computer, the criminal wouldn't have been able to steal the files, because the DLP would have kept this from happening. Permission would have been denied.

Make your staff aware of social engineering. Even if you outfit your law firm with top-of-the-line network security and follow all of these other recommendations, it won't do much good when an employee makes a stupid mistake because he or she just didn't know any better. You need to train your staff what kinds of things to look out for: suspicious emails, phone calls, or social media messages; strange download requests; and so on.

Doing this, however, is easier said than done. Studies have shown that holding classes for your employees is a costly strategy that just doesn't work. Even if they pay attention and seem to understand what they need to do during the class, they won't retain the knowledge for long. Some things you can include:

- *Internal phishing.* Want your employees to learn how sneaky phishing emails can be? Utilize tools that allow you to send them fake phishing emails. Those who click on them will be notified that they opened an email that could have been dangerous and provided with further information to help raise their awareness.
- *Entertaining videos.* Formal classes don't work, but it can be effective to periodically send out short, humorous videos that highlight a particular security concern and what to do about it.
- *Hold contests.* People will be encouraged to learn and retain information better by competing with their peers to win prizes. Even those who don't participate can benefit from the increased awareness and repetition of important rules and concerns.

Ultimately, the most important thing you can do is actively work to improve your firm's security. Far too many firms seem content to hope that a data breach won't happen—but the truth is that it already may have. Most firms don't even know that they have been breached until the federal government contacts them to let them know that there's a problem.

Don't be one of those firms. Protect your clients and yourself by becoming proactive and staying ahead of the game. ⊙

Andres Hernandez is the co-founder and CEO of Wingman Legal Tech, a technology consulting firm that specializes in law firm technology. A Marine Corps veteran with a master's degree in Technology Management from National University, Hernandez has been leading an effort in the legal industry to adopt cloud technologies for leaner and more efficient law firms.