CNA

We can show you more.®

CYBER-SAVVY LAWYERS:

Smart Cyber Practices In Law Firms

TABLE OF CONTENTS

Introduction
pg. 2

Evolving Legal Implications
pg. 3

8 Tips for Securing Your Data
pg. 5

Benefits and Risks of Using the Cloud
pg. 8

4 Things You Must Do After a Data Breach
pg. 10

Social Media Conduct
pg. 11

Conclusion
pg. 13

Your Cyber Self-Assessment
pg. 14

INTRODUCTION

This guide offers a comprehensive synopsis of what cyber means to you as a lawyer. From implementing cybersecurity measures to handling the event of a data breach, the following information can help you protect your data and stay out of court – all while serving your clients.

Cyber is synonymous with electronic, digital, virtual and online.

> In today's market, much of your **day-to-day business endeavors** are likely executed on a cyber platform.

You receive an email from a client; you have a conference call after lunch; you make a wire funds transfer; you research legal precedents online.

Cybersecurity, as you can assume, refers to the state of being protected against criminal or unauthorized use of any data or information traveling through a cyber outlet, including, but not limited to: physical electronic devices, email, the cloud, Internet, and shared drives and networks. When it comes to warding off hackers, you've likely heard of encryption, firewalls, spyware and the power of a strong password. While these security measures certainly compose one wall of defense, they cannot offer comprehensive protection.

As a lawyer, cyber protection is critical. Within your files, you possess clients' personal identifiable information (PII). This means that hackers are more likely to target you or your firm to get their hands on that kind of information. PII's generally include someone's full name in conjunction with:

- Social security number
- Driver's license number
- State issued ID number
- Financial account number
- Credit or debit card number
- Personal ID or password (i.e., for accessing a network containing financial account or health information)

But it's not just cybersecurity practices you need to consider. How do you conduct yourself on social media? Did you know that certain posts, even on your personal account, can violate confidentiality, ethics, or state or federal privacy and data security laws?

While what you post and share on social media is within your control, there is no surefire way to defend against a cyber attack. From this guide you can take away: cyber-related legal precedents; advanced cybersecurity practices; risks and benefits of cloud computing; social media risks and etiquette; and steps to take after a data breach. We'll send you off with a self-assessment to take back to your office, firm and/or employees to get started in cyber-securing your practice.

EVOLVING LEGAL IMPLICATIONS

If you haven't set up safeguards in your firm, whether you haven't had time or funding, this is now one of your highest priorities. State privacy laws are setting a higher minimum standard for businesses with custody of confidential client information. In other words, protecting client information is the law.

Until recently, the landscape of privacy laws included two types. First, there were breach notification laws at the state level. These laws set forth requirements for notifying clients and mitigating damages in connection with disclosure of personal private information. Second, there were federal "duty to safeguard" laws that generally applied only to certain industries, for instance, the HIPPA Privacy Rule in healthcare. Under ABA Model Rule of Professional Conduct 1.15, lawyers have obligations of safeguarding, accounting and delivery when holding the money or property of others.[1] However, most state bar associations have not yet directly addressed whether a lawyer is liable when a third party not employed or supervised by the lawyer steals client funds.

Consider **this scenario:**

A sophisticated hacking scam the FBI refers to as "Business E-mail Compromise" targets lawyers who process client funds from their attorney trust accounts. Typically, the hacker impersonates the intended recipient of a payment via email. For example, the email can come from a nearly identical email address to your well-known client's email address, aside from a missing letter or additional number that you're likely to not notice at a glance. The hacker would ask you to transfer funds at your earliest convenience, manipulating you into wiring client funds to a fraudulent bank account. After the funds are fraudulently transferred, you may be obligated to replace the lost client funds.

1 See In re Mayeaux, 762 So.2d 1072 (La. 2000)("lawyer's mistake, good faith, or lack of conscious wrongdoing does not negate an infraction of the rule"); Att'y Grievance Comm'n v. Stolarz, 842 A.2d 42 (Md. 2004)("an unintentional violation…is still a violation of the attorney's affirmative duties imposed by the rule"); Restatement (Third) of the Law Governing Lawyers §5 cmt. (d)(2000).

The North Carolina State Bar was the first to address this third-party-theft issue in an October 2015 ethics opinion.[2] According to the Opinion,

> Lawyers are **required to use reasonable care to prevent third parties** from gaining access to client funds held in the trust account.[3]

As a result, a duty is imposed upon you to implement reasonable security measures, such as calling the intended recipient of funds at the phone number listed in your file to confirm his or her e-mail address.[4]

In addition, you have affirmative duties to "educate [yourself] regularly as to the security risks of online banking; to actively maintain end-user security at the law firm through safety practices such as strong password policies and procedures, the use of encryption and security software and the hiring of an information technology consultant to advise the lawyer or firm employees; and to insure that all staff members who assist with the management of the trust account receive training on and abide by the security measures adopted by the firm."[5]

The costs of employing cybersecurity surely outweigh the costs of a data breach or loss of client funds. In general, safeguarding client data doesn't have to be expensive. For small businesses using one or more standalone personal computers, off-the-shelf software is available providing firewalls, antivirus, spam and spyware protection and encryption. The cost per computer to install and maintain this software is typically a few hundred dollars, and the cost of installing and maintaining this protection in a small computer network is rapidly coming down. Unified Threat Management appliances are firewall routers designed to provide these protections across a small network, typically at a cost of $1,000 or less.

Remember, security measures such as these make up just one wall of defense. Additional safeguards further secure your data and reputation, and some methods don't cost a penny.

2 See FEO 6, The North Carolina State Bar, October 23, 2015.
3 Id.
4 Id.
5 See 2011 FEO 7, The North Carolina State Bar, 2011; 2015 FEO 6, The North Carolina State Bar, October 23, 2015.

8 TIPS FOR SECURING YOUR DATA

While spam filters, anti-spyware, software-based firewalls and virus scanning are essential risk management tools, there are additional ways to help you shrink your security gaps.

1 Encrypt, Encrypt, Encrypt

According to a 2013 American Bar Association survey, all forms of encryption – including file encryption, e-mail encryption and full-disk encryption – are the security features used *least* often by law firms.[6] This data is surprising as encryption represents a relatively simple and effective risk management tool. Furthermore, lost or stolen laptops and devices are a top cause of law firm data breaches. If a computer or device is encrypted, even if the laptop or device is lost or stolen, the information will not be accessible.

2 Use Caution in the Cloud

+

Reportedly, **the cloud is used by 64 percent of lawyers** in their practices.[7]

When you store firm and client information in the cloud, it is essentially stored off site, possibly in another country, where it may be subject to international search and seizure laws.

Most bar associations that have published opinions on the ethics of cloud computing found that working in the cloud is ethical if appropriate precautions are taken.[8] At a minimum, you must use due diligence in selecting a cloud provider by asking the right questions. Does the cloud provider employ adequate security to protect the data? Will the data be stored internationally? If so, will it be subject to search and seizure? You also should know what data you're placing in the cloud, and whether that data is subject to state or federal privacy laws. Have the clients provided their written consent to place information in the cloud? Will the information in the cloud be encrypted? Law firms should use only a cloud provider that can provide reasonable assurance that the data will be protected. We'll further discuss the benefits and risks of the cloud in the next section.

3 Beware of BYOD

While advantageous for many reasons, Bring Your Own Device (BYOD) policies are risky if appropriate security measures are not taken. Firms should have a specific BYOD policy in place regulating how those devices are to be used, and giving the law firm ultimate control over the devices. Company data on the devices should be both encrypted and password protected. Law firms also should install mobile device management (MDM) software that can remotely "wipe" the employee's device if the firm employee leaves the company. Law firms may consider installing a remote location-tracking "app" on the device if the device does not already have such software installed.

6 Joshua Poje, "Security Snapshot: Threats and Opportunities," ABA TechReport 2014, Legal Technology Resource Center.
7 Alan Cohen, "Survey: Data Security is Tech Chiefs' Top Worry," The American Lawyer, (Oct. 29, 2014).
8 See, e.g., Oregon Bar Ethics Opinion 2011-188 (November 2011); Pennsylvania Formal Opinion 2011-200; North Carolina 2011 Formal Opinion 6 (January 27, 2012); New York State Bar Ethics Opinion 842 (Sept. 10, 2010); Alabama Ethics Opinion 2010-02; Washington State Bar Advisory Opinion 2215 (2012).

4 Vet Your Vendors

You likely frequently outsource work such as e-discovery, legal research, copying, IT and other non-legal services to third-party vendors. As recent data breaches have demonstrated, third-party vendors are becoming a vulnerable point of attack at which hackers can strike.

Lawyers have specific ethical duties under ABA Model Rules of Professional Conduct 5.1 and 5.3 to ensure that their vendors' conduct is compatible with professional obligations, including the duty of confidentiality under Rule 1.6. According to ABA Formal Opinion 08-451, an outsourcing lawyer must "act competently to safeguard information relating to client representation against inadvertent or unauthorized disclosure" by the individuals to whom the lawyer has outsourced the work. Therefore, you must assess whether your vendors are storing, transporting or analyzing confidential data. If so, written and signed contracts should address the various relevant security issues, including ensuring that the information is properly stored and secured to prevent unauthorized access. Finally, law firms should carefully and thoroughly review the vendor's contract for indemnification clauses, limitations on liability and guidance as to the party who will be expected to pay in the event of a data breach.

5 Staff Training is Key

Educating staff on confidentiality issues and avoiding a data breach can greatly reduce the risk of a data breach in your firm. They should receive instruction on the policies and practices the law firm expects them to follow, including Internet usage policies and social media policies. For example, targeted or untargeted malware and/or viruses are a major cause of data breaches, which can be transmitted to the firm's network when firm employees click on a link in an e-mail. It's important for employees to understand that spam filtering and anti-virus will never be 100 percent effective in stopping malware. Regular training for employees about these and other "do's and don'ts" can help avoid a large number of potential data breaches within law firms.

6 Be Wireless Savvy

Strong wireless protocols should be observed in order to prevent unauthorized guests from accessing firm data. Also, you must exercise caution when working over unsecured networks using laptops, smart phones and tablets. Free networks, including those found in airports, hotels and coffee shops, are frequently unsecured. A virtual private network (VPN) encrypts any data sent or received, and makes it more difficult to intercept. Another alternative involves purchase of a mobile Wi-Fi hotspot, which is a small, transportable Wi-Fi router that provides a personal and private Wi-Fi cloud to which you can securely connect your device.

7 Have a Password Policy

Enforcing a uniform password policy for all lawyers in the firm is one of the most effective – and inexpensive – programs a law firm can pursue to protect its sensitive data. Employees should be required to select a complex password with a combination of letters, numbers and symbols. The password should be a minimum of 12 characters, and contain upper- and lower-case letters and numbers. Consider even using a phrase or more than one word in the password. Passwords should be changed regularly and not repeated. Password managers can help attorneys create, track and store secure passwords. The limited risk associated with using a password manager is greatly outweighed by the benefit of having a strong password in place.

8 If All Else Fails, Be Prepared

Even law firms with the best security protection available remain at risk of a data breach or another disaster. Therefore, law firms should prepare for the possibility of a disaster by having a business recovery plan in place and test it at least annually. In addition, routinely back up your data and maintain a copy at an off-site, secure location. Given the potentially devastating impact of a data breach, cyber liability insurance coverage could mean the difference between a law firm surviving a data breach relatively unscathed, or not surviving at all. Cyber liability coverage can help a law firm cover the costs related to a data breach, including privacy breach notification expenses, litigation, loss of income, regulatory fines and penalties and other expenses.

Implementing cyber security practices is the first step in lessening your risk of being hacked, especially as new data sharing technologies emerge, such as the cloud.

BENEFITS AND RISKS OF USING THE CLOUD

Numerous companies are now offering cloud-based services focused specifically on the needs of law firms, and market various benefits in seeking to move law practice management functions to their cloud.[9] These benefits include the following:

1 Reduced Cost/Reduced Capital Expenditures

By using cloud computing, you'd no longer need computers with large storage capacity, external hard drives, or servers to store all of their data. Instead, this information would be stored in the cloud and would be accessible from any computer, tablet or other device with access to the Internet.

2 Scalability/Flexibility

Financially speaking, you'd only pay for your actual usage of the service. For example, if your firm needs access for 10 users, you'd pay for 10 users. If, within six months, your firm has downsized and only needs six users, you'd only pay for six users. Alternatively, if within one year your firm has experienced growth and needs 15 users, your firm can pay for access for 15 users.

3 Accessibility of Data Across Different Devices

Cloud computing and storage also eliminate the need to create multiple versions of the same document on multiple devices. If a document was stored in the cloud, you could draft a document on your work computer and then update the same document from your personal tablet or laptop from home.

4 Sharing/Collaboration

The arguably most compelling feature of storing documents in the cloud is the ability to collaborate on those documents. For example, when you assist a client in responding to written discovery, those documents must be reviewed by the client. Often, the method to assist the client requires emailing revised versions of the document back-and-forth and saving those emails (and attachments) in your email program and in the client file. By utilizing the cloud service, you can simply save the document to a shared folder and provide the client with secured password access to the folder containing the document.

+ While there are **many advantages to cloud computing**, there are also **inherent risks.**

It's important to address all foreseeable risks and ethical issues with your cloud vendor prior to contracting for its services. A cloud vendor is a company, often referred to as a cloud service provider (CSP), which offers cloud computing services – typically Infrastructure as a Service (IaaS), Software as a Service (SaaS) or Platform as a Service (PaaS). Also, consider risks unique to your specific area(s) of legal practice, as well as unique to your state's laws and rules of professional conduct. One of the best means of addressing those risks with your cloud vendor is in the Service Level Agreement (SLA). Many of these SLAs are less than one page and address only the "uptime" of the cloud provider. "Uptime" is a term indicating that the cloud vendor guarantees that the attorney will have uninterrupted access to information in the cloud. Most cloud vendors guarantee approximately 99.999 percent uptime.[10]

9 Non-exclusive list of cloud vendors: Appirio, Citrix, Clio, Dialawg, HoudiniESQ, IntraLinks, Livia, Merrill Lextranet, MyCase, Next Point, Rocket Matter, Thomson Elite, Total Attorneys, LLC

10 See also the term "FIVE NINES", which refers to a provider offering 99.999% uptime. It is the "gold standard" in utility service industries. See Cloud Computing Opinion: The Goal of "Five Nines" – 99.999% Availability is Meaningless, Ajax World Magazine, Sept. 15, 2008 at http://ca.sys-con.com/node/674934.

Below are eight risk control techniques for managing the inherent risks of cloud computing:

- **Investigate your vendor.** What is the vendor's business model? Is the vendor financially stable? Who are some representative clients? If the cloud vendor is reputable, the vendor typically will have relationships with other corporations in data-sensitive industries and, ideally, other law firms.
- **Determine ownership of data.** Attorneys should confirm that the law firm will be the sole owner of data and that the vendor has no ownership or other rights to the data.
- **Determine confidentiality of data.** Attorneys should confirm that the vendor will assume responsibility and legal liability for confidentiality of data.
- **Know the location of data storage.** Attorneys should confirm the location of data storage. Attorneys should review the choice of law provision in concert with laws that may govern the situs of data storage.
- **Know how the system usage logged/accessed.** Can the law firm define and control different levels of access to certain files for various employees/clients? Accessibility and support of two-factor authentication can be important if the firm must apply different security and access for lawyers and support staff.
- **Have an exit strategy: return of data/deletion upon termination.** Attorneys should confirm that the vendor will return data to the firm in a usable format. For example, if the law firm stored Microsoft Word documents with the vendor, is the data returned in that format or another format that is unusable to the law firm? In addition, confirm that the vendor will ensure that upon return of data, it is permanently deleted from the vendor's servers.
- **Confirm vendor's full acceptance of liability.** Confirm that there are no limitations on the vendor's liability.
- **Obtain the client's consent to the use of cloud storage.** Attorneys should explain to the client that the firm uses cloud storage in the practice. In addition, attorneys should always obtain the written consent of the client to the use of cloud storage of client files and documents. The consent should be in writing and signed by the client.

+

While cloud computing can be attractive for many reasons, **do not participate simply to adopt the latest technology.**

In fact, cloud computing might not be beneficial for all law practices, depending upon the needs. Before you reach out to a cloud vendor, conduct a reasonable review of the current model of your law practice management and evaluate whether a move to the cloud would be beneficial.

4 THINGS YOU MUST DO AFTER A DATA BREACH

Today's digital landscape lends itself to more opportunities for hackers to access your data. Unfortunately, even if you and your firm have taken all precautions, a data breach may still occur. If you've been breached or suspect your information system has been targeted and client information is exposed, a rapid assessment and mitigation of damage is imperative, as outlined below:

Evaluate the severity and scope of the incident.

If a laptop computer or other portable device is lost or stolen, identify the data that may have been exposed, and determine whether these materials are encrypted. Consider engaging forensic information technology experts to define the scope of the problem. In addition, if the possibility of identifying theft or other criminal action is present, inform appropriate law enforcement agencies of the situation.

Notify appropriate law enforcement or other governmental authorities and potentially affected clients.

Most states now mandate notification of both governmental and/or legal authorities and of those whose confidential data may have been exposed. Firms that have experienced a data security breach also may be required to pay for credit monitoring services for potential victims. Some breach of data security laws require firms to warn affected persons of the risk of identity theft and fraud within a stipulated timeframe.

Consult with legal counsel regarding applicable notification laws and how to manage media coverage of the breach.

Consider going beyond minimal legal compliance. Notification of federal and state regulators (i.e., state attorney general) may be appropriate in some cases. Because clients expect law firms to safeguard personal and financial information, a data breach can tarnish your firm's reputation. You can begin to repair trust and reduce further losses by offering to help clients obtain credit monitoring and identity theft case management services.

Immediately Back Up All Your Data

This should be done on a regular basis, but especially if you suspect a breach or experience an actual data breach. In some instances, it may be impossible to take this fourth step. Take ransomeware, for instance. This type of malicious software locks you out of your files and demands payment in order to restore access. There is a typical time limit of three to four days for payment to be made before the encryption key is destroyed, rendering your files unreadable – forever. If you're fortunate enough to have your files after a breach, immediately back them up in a secure, preferably off-site location like an external hard drive.

Any business can experience a data breach at any time. Should the worst occur, it's important to have cyber liability coverage.

+

According to the Ponemon Institute, **the average security breach costs organizations almost $200 for each record that's stolen, or about $5.5 million** for the typical company breach.

A claim that size could cripple a business without adequate insurance coverage.

SOCIAL MEDIA CONDUCT

Imagine a lawyer has just finished a grueling deposition preparation session with an uncooperative but important witness for her side of the case. Tired and a bit frustrated, Mary vents by updating her Facebook status while in the taxi on the way home:

"Absolutely drained after spending six hours prepping Mr. No-Clue for deposition. Who's in for dinner?"

In this post, Mary "tags" a few of her friends, among them Dave, who also happens to be a lawyer. But what will Mary do when Dave happens to be Facebook friends with the opposing counsel, who can see that Dave is tagged in Mary's post, and uses this serendipity as ammunition at cross-examination like this:

Mary, did you meet with the counsel to prepare for your testimony today?

Yes.

Are you aware that counsel has questioned your competence and the accuracy of your memory regarding the facts in this case?

Following an event such as this, professional liability coverage would undoubtedly become a necessity. But there are preventative steps lawyers can take to avoid such claims – as long as they remain diligent from behind their keyboards.

Social media, blogs and other interactive internet-based platforms allow lawyers to reach out broadly to colleagues, clients and potential clients. But, posting on personal social accounts doesn't exempt lawyers from confidentiality breaches, violations in ethics, or state or federal privacy and data security laws. Not to mention certain social actions could potentially mislead clients or fall short of the standard of care. Thus, while lawyers must keep pace with today's forms of communication, they also must consider the risks presented by new technologies and how to control those risks.

What follows is an examination of some of those risks and ways to help address them.

Social Media Potential Pitfalls

Participation on Facebook, Twitter and LinkedIn can be both socially and professionally beneficial. But, lawyers also risk breaching confidentiality or undermining relationships with courts, witnesses or clients through even the most seemingly innocuous status updates, comments, likes and shares.

The lawyer with the difficult deponent mentioned earlier not only is likely to be embarrassed before her client and the court, but also could face a professional liability claim when the witness refuses to cooperate in presenting essential facts at trial and the client's case is lost as a result.

A lawyer who uses social media to alert friends that he must cancel dinner with the post, "Unexpected meeting at XYZ Corp. equals long night of work ahead," may inadvertently tip someone off regarding XYZ's plans for a business transaction, potentially leading to violations of state or federal insider trading laws. This risk is exacerbated by the seemingly infinitely long reach of Internet posts, coupled with the lack of control over the message once it is posted online. Even if you delete a post after second-guessing its appropriateness, a dozen people have likely seen it within a matter of minutes.

And the post isn't limited to your followers and friends; the update is susceptible to being shared with friends of your friends, and their friends, over and over again. Similarly, lawyers or law firm employees who "friend" clients and communicate with them over public and semi-public media risk inadvertent waivers of privilege and unanticipated breaches of confidentiality.

Further, lawyers should not presume that the use of privacy settings on social media provides full protection of posted information from discovery in the event of litigation. The law continues to evolve in this area, and courts have taken differing positions on this.

+ Social media risks are **not limited to those arising from a lawyer's sharing of information.**

Lawyers must also be careful when searching websites for information about witnesses and other parties. It is established and expected that lawyers can review public sites to gather such information. But, they may not do so surreptitiously: "pretexting" by instructing an investigator to "friend" a non-party witness in the hope of gaining access to potentially damaging information on the witness' protected social media profile would violate ethics rules prohibiting conduct involving dishonesty, fraud, deceit or misrepresentation. See, e.g., Phil. Bar Prof. Guidance Comm. Op. 2009-02. Evidence obtained this way would likely be rejected in court. On a related note, are you aware that when you look up someone on LinkedIn, they get a notification that you viewed their profile? This is good to keep in mind when researching a client or opposing councils' credentials. Do you want them to know you're looking into them?

Remember: Judges can and do look at social media updates to monitor compliance with directives and veracity of statements by criminal defendants, litigants and attorneys. In one situation, documented in the July 21, 2009 issue of ABA Journal Law News Now, a lawyer asked a judge for a continuance after the death of her father. The judge granted the request, but later reprimanded her after seeing pictures of the lawyer partying on the beach during the continuance period.

Any breach of candor to the tribunal can compromise a client's position before the court, with the jury or with the opposing party, raising the risk that a lawyer could face a claim for failing to provide adequate representation if the client is displeased with the outcome of the case.

Managing Social Media Risks

Ultimately, the most important risk control technique when using social media is to simply think before typing. It's important to recognize that, even with all the privacy settings turned on, nothing that gets posted online is 100 percent private. Most information related to a lawyer's work should not be shared publicly.

With that admonition in mind, risk control in the social media setting should focus on limiting access to information about any representation. Lawyers using social media tools should:

- Examine the security and privacy policy of any social media website before deciding to participate.
- Use available security and privacy protections to limit the reach and use of posts by others. This includes settings requiring prior approval of friend requests, or that provide users with alerts regarding who has chosen to follow updates or pages.

- Regularly revisit the security and privacy provisions of the site to monitor changes and react accordingly (Most social media channels notify users when their privacy policies or terms of service change).
- Set written rules for posting by office employees and professional staff on both personal and firm pages, clearly directing that only appropriately public information be shared. Consider applicable employment laws in formulating the rules. Monitor all posts on a regular basis, and inform employees of this in the rules.
- Monitor and adapt as the technology develops. The types of social media available on the Internet are expected to continue to evolve. The ability to post data instantaneously and in real time from handheld devices continues to raise new challenges for lawyers, for instance. When a new type of social media becomes available, consider the need to revise firm rules regarding their use.
- Be careful about what their social profiles reveal. On some sites, such as LinkedIn, participants can receive rankings or recommendations regarding expertise based on their participation in question-and-answer forums. In some jurisdictions, answering those questions could be a violation of ethics rules prohibiting specialization or certification statements. In any jurisdiction, answering such questions could cause a lawyer to be held to a higher standard of care when faced with a professional liability claim.

Often the most important risk control approach is to use thoughtfulness, caution and common sense. Establishing and enforcing a social media policy that emphasizes professional practices on social media to your employees is the first step in managing these risks in your firm. To better protect yourself and your firm, professional liability (errors and omissions) insurance can help cover the costs should you or one of your employees make a social media mistake.

CONCLUSION

Today's businesses operate in a connected world. While this has its advantages, the risks associated with client data exposure, theft or alteration cannot be taken lightly. Data breaches have become more common – and costly. Lawyers on social media need to consider unique consequences before they post. Establishing an effective social media policy, data security program and preparing a post-incident response plan can help protect both clients and your firm.

Talk to your insurance carrier about cyber liability and D&O liability coverages for your law firm's specific needs.

CNA
We can show you more.®

SMALL BUSINESS

YOUR CYBER SELF-ASSESSMENT

What type of PII do I possess?

- ❑ Social security number
- ❑ Driver's license number
- ❑ State issued ID number
- ❑ Financial account number
- ❑ Credit or debit card number
- ❑ Personal ID or password
- ❑ Other _____

What do my state laws say about third-party data breaches for a law firm?

_____

_____

_____

_____

_____

_____

Do my cybersecurity practices include the following?

- ❑ Encryption
- ❑ Password Policy
- ❑ Spyware/Firewall/Virus Scanning
- ❑ Wireless Connection Policy
- ❑ Consistent Data Backups
- ❑ Employee Training
- ❑ BYOD Policy
- ❑ Cloud Vendor SLA (if applicable)

Does my social media policy cover the following?

- ❑ Appropriate versus inappropriate types of posts/shares
- ❑ Compliant social media profiles (compare to state laws)
- ❑ An understanding of the social channels' privacy policies

To learn more, contact your independent agent.
Need an agent? Match with one today at www.cna.com.