CNA

We can show you more.®

PROFESSIONAL COUNSEL℠

ADVICE AND INSIGHT INTO THE PRACTICE OF LAW®

Safe and Secure:
Cyber Security Practices for Law Firms

A CNA PROFESSIONAL COUNSEL GUIDE FOR LAWYERS AND LAW FIRMS

Due to the unprecedented number of data breaches at major corporations, 2014 was called "The Year of the Data Breach." Based upon recent news reports, one might believe that such breaches are confined to the healthcare and financial sectors. Data breaches within law firms are rarely reported in mainstream news outlets, and those law firms affected by data breaches usually prefer not to publicize the breaches. This general underreporting of data breaches within the profession has led many lawyers to greatly underestimate their own data security risks. As a result of this misplaced sense of security, many law firms have failed to take necessary steps to improve their data security. This is one situation where "no news" is not necessarily "good news."

While data breaches may not be as common for law firms as in some other industries, they remain a significant and growing threat. Law firms suffer data breaches not only from hacker intrusions, but also from many other sources and causes. Those law firms that choose to ignore this risk do so at their peril. Implementing adequate data security is not only a sound business practice, but also a legal and ethical duty for lawyers. Fortunately, law firms may avoid the vast majority of breaches by implementing data security measures that are neither unduly expensive nor obtrusive.[1]

The Growing Data Security and Privacy Threat for Law Firms

Clearly, data breaches at law firms are on the rise. In 2011, the FBI met with representatives from 200 of the largest U.S. law firms to warn them that law firms represent a major target of hackers. Why? Law firms hold vast collections of sensitive client documents – data of significant value to hackers. Ample cause for concern arises as security experts working with law firms report that law firm hacking is pervasive. Mandiant, a security consulting firm, estimated that 80 percent of the 100 largest firms had a malicious computer breach in 2011.[2] In most of these cases, the law firms either had failed to discover the breach on their own, or had discovered the breach several months after its occurrence. Indeed, security experts commonly note that there are two types of law firms: those that know they have been hacked, and those that don't *yet* know it!

Beyond the risk of a hacking incident, law firms are vulnerable to data breaches from within the law firm. According to CNA claim data, a lost or stolen laptop or device is the *most frequent* cause of a data breach claim.[3] The growth of smartphones, tablets and other devices in the legal profession has notably amplified the security risks for law firms. Many law firms now have "Bring Your Own Device" (BYOD) policies that enable lawyers to access their law firms' networks and download client data onto their devices. While BYOD policies undoubtedly make smart business sense, law firms must appreciate the risks associated with permitting the unrestricted use of outside devices. Currently, most law firms do not require *any* security on outside devices, such as mandatory password protection, encryption, or remote wiping capability.[4] As a result, not only is data on the device vulnerable to a potential breach if the device is lost or stolen, but the firm's network itself may be exposed to harmful malware and viruses present on the device.

Rogue employees represent another vulnerability regarding law firm data. Although this situation may be rare, there have been examples of lawyers or other law firm staff misappropriating or misusing confidential client data.[5] In a recent case, a law firm brought litigation against a former partner of the firm who had downloaded Dropbox software onto the firm's network in order to continue accessing client files through the cloud provider after his departure. [6] Firms should, therefore, consider adopting security mechanisms such as data loss protection ("DLP") systems, also known as data leak prevention systems, to help detect and prevent the potential unauthorized transmittal of confidential information by employees. DLP systems ensure that end users do not send sensitive or critical information outside the corporate network. Such systems classify and protect confidential and critical information so that unauthorized end users cannot accidentally or maliciously share data whose disclosure could place the organization at risk. For example, if an employee tried to upload a corporate file to a consumer cloud storage service such as Dropbox, the employee would be denied permission.

Costs of a Data Breach

Understandably, the potential financial damage from a data breach keeps many managing partners up at night. As of 2013, the average cost of a data breach in the United States was $5.4 million, including crisis management services, forensic investigations, legal counsel, breach notification expenses and credit monitoring for individuals whose data has been breached.[7] Thus, the future survival of a law firm following a data breach may depend upon whether or not the firm has sufficient financial resources to overcome such a crisis.

The reputational impact of a data breach on a law firm also represents a matter of critical importance to a law firm. The firm's reputation is arguably its most important and valuable asset. A data breach thus raises questions and concerns as to the adequacy of its data security protocols and can lead to the loss of client business. From an enterprise risk management perspective, law firms have much at stake concerning data security and every incentive to make data security a top priority.

Source of the Lawyers' Duty to Protect Client Data

Data security is not simply a smart risk management step for law firms, though. Specific legal and ethical obligations also require law firms to provide data security for their information and that of their clients. Various federal laws impose affirmative obligations on law firms to protect certain categories of information in their possession, such as the Health Insurance Portability and Accountability Act of 1996 (HIPAA), the Fair and Accurate Credit Transactions Act of 2003 (FACTA), the Gramm-Leach Bliley Act (GLBA), and others. Numerous states have also imposed affirmative obligations on businesses, including law firms, to protect personally identifying information (PII) in their possession, including Social Security numbers, drivers' licenses, account numbers and health information.

In addition, law firms increasingly are subject to various notification obligations under state law, in the event of a breach. As of 2014, at least 47 states had enacted legislation requiring any private or governmental entities to notify individuals of security breaches of information involving PII. Failure to comply with the aforementioned state and federal laws can result in enforcement actions, civil suits, or civil monetary penalties.

Unlike most other industries, lawyers also have ethical obligations to maintain data security. These ethical duties arise primarily under Rules 1.1 and 1.6 of the ABA Model Rules of Professional Conduct. A violation of these ethical rules can give rise to a disciplinary action or a malpractice lawsuit against a lawyer and/or a law firm. For example, ABA Model Rule 1.6, subsection (a) provides that:

> "[A] Lawyer shall not reveal information relating to the representation of a client unless the client gives informed consent, the disclosure is impliedly authorized to carry out the representation, or it falls within one of the exceptions under subsection (b)."

Most states have adopted ABA Model Rule 1.6(a) or similar wording. Moreover, recent revisions to ABA Model Rule of Professional Conduct 1.6 added the following additional affirmative obligation for lawyers:

> "(c) A lawyer shall make **reasonable efforts** to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client." *(Emphasis Added)*

A number of states have since adopted this new language into their rules of professional conduct. Therefore, under this new ethical obligation, lawyers may now be required to make "reasonable efforts" to prevent the disclosure or access of client information. What efforts are considered reasonable? While there is no simple answer to this question, the comments to ABA Model Rule 1.6 state that various factors will be considered in determining the reasonableness of the lawyer's efforts, including the sensitivity of the information, the likelihood of disclosure if additional safeguards are not employed, the cost of employing additional safeguards, the difficulty of implementing the safeguards, and the extent to which the safeguards adversely affect the lawyer's ability to represent clients.[8]

Furthermore, under Rule 1.1 of the ABA Model Rules of Professional Conduct, lawyers are required to provide a competent representation to a client. Comment 8 to this Rule requires lawyers to "keep abreast of changes in the law and its practice, *including the benefits and risks associated with relevant technology*" in order to provide a competent representation. A number of states have now adopted this or similar language as well. So, lawyers also may be obligated to become and remain conversant with relevant technology in order to meet their ethical duties to clients, including their duty of confidentiality.

Apart from the legal and ethical requirements, strong business incentives abide regarding the maintenance of data security as well. Law firms are now frequently facing security audits from clients, especially from corporate clients in the financial services and healthcare industries. In a recent survey, 54% of mid-sized and large law firms responded that their risk and security practices had been audited by a client.[9] Thus, the quality of a law firm's data security can become a competitive advantage – or disadvantage – relative to revenue and profitability.

Opportunities to Advance Law Firm Security

Most firms already employ the most common data security tools such as spam filters, anti-spyware, software-based firewalls, as well as virus scanning on both PCs and in email.[10] These are indeed essential risk management tools, but law firms should not assume that installing these security features results in comprehensive protection. They should remain vigilant regarding other significant vulnerabilties that exist, and take the necessary steps to close these 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.[11] This data is surprising as encryption represents a relatively simple and effective risk management tool. As discussed above, lost or stolen laptops and devices are a top cause of law firm data breaches. The use of full disk encryption on laptops and other devices can help mitigate this risk. 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 now used by 64% of lawyers in their practices.[12] Working in the cloud has many potential advantages for law firms, including cost savings, scalability, increased mobility, and a host of other benefits. However, cloud technology has its own inherent exposures if one is not careful. When a lawyer stores firm and client information in the cloud, that information 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 have found that working in the cloud is ethical if appropriate precautions are taken.[13] At a minimum, lawyers 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? Lawyers also should know what data they are 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. For more information, see CNA's article, "Caution in the Cumulus: Lawyers' Professional & Ethical Risks and Obligations Using the "Cloud" in Their Practice."

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 software that can remotely "wipe" the employee's device if the firm employee leaves the company. Law firms also may consider installing a remote location-tracking "app" on the device if the device does not already have such software installed. If the device is misplaced, the app may be able to help locate it and prevent a data breach from occurring.

4. Vet Your Vendors

Approximately 40% of law firms currently outsource some non-lawyer functions.[14] Lawyers frequently outsource work such as e-discovery, legal research, copying, IT and other non-legal services to third party vendors. Interestingly, the legal outsourcing industry is growing at a pace of 28% a year or more.[15] As recent data breaches have demonstrated, third party vendors are becoming a vulnerable point of attack at which hackers can strike. For example, in March 2014, the W-2 information, as well as other information of 441 current and former employees of a large international law firm had been breached when a vendor's database was accessed through acquisition of a client's login credentials. The law firm notified the Maryland Attorney General of this breach.[16]

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, law firms must assess whether their vendors are storing, transporting or analyzing confidential data. If so, contracts should address the various relevant security issues, including ensuring that the information is properly stored and secured to prevent unauthorized access. For example, the law firm should confirm that vendors employ password protection, encryption and antivirus software. Written confidentiality agreements are also advisable in outsourcing relationships. 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

The importance of employee training cannot be overemphasized. Educating staff on confidentiality issues and avoiding a data breach can serve to reduce the risk of a data breach in your firm. Law firm employees should understand the importance of protecting law firm data and their critical role in maintaining its security. They also 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. Periodic 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

Advances in wireless technology have made it possible for law firms to better serve their clients by allowing their lawyers to work remotely from anywhere in the world. However, without the proper precautions, working remotely can represent a risky practice.

Strong wireless protocols should be observed in order to prevent unauthorized guests from accessing firm data. The most common types of wireless security protocols are Wired Equivalent Privacy ("WEP"), Wi-fi Protected Access ("WPA") and Wi-fi Protected Access Version 2 ("WPA2"). Transacting business wirelessly with WEP represents an extremely weak security standard with many well-known security flaws.[17] The password WEP uses can often be penetrated in just a few minutes. It is preferable for law firms to instead use WPA2, which is the most secure wireless security protocol currently available, due to the addition of AES, an encryption device that encrypts the network with a 256 bit key. Not only will WPA2 prevent uninvited intruders, but its wireless security protocols will then encrypt private data as it is being transmitted over the airwaves.

Second, lawyers 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. Avoid reviewing or sending any confidential data over an open wireless network. If available, use the firm's virtual private network ("VPN"), which will encrypt any data sent or received and make 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. By taking such small but important steps, lawyers can significantly reduce their risks when working remotely.

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. Optimally, a password should be random, but at a minimum, it should not be a popular password or one that can be easily guessed. Rather, firm 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. The Georgia Institute of Technology reported that any eight character password can be cracked in less than two hours but that it would take approximately 17,000 years to crack a strong 12-character password.[18] The firm should also require passwords to be changed regularly and not repeated. It may be helpful to use a password manager to keep track of different passwords. Password managers can help attorneys create and store secure passwords. Examples of password managers that security experts have recommended are 1Password, LastPass and KeePass. The limited risk associated with using a password manager is greatly outweighed by the benefit of having a strong password in place. Employees should receive annual training on the basics of secure passwords and their importance.

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. About one in five law firms reported that their law firms had experienced a disaster in 2013.[19] Therefore, law firms should prepare for the possibility of a disaster by having a business recovery plan in place. This can help the firm quickly rebound from disasters such as data breaches, hard drive failures, or computer malfunctions. Alarmingly, in a recent survey, only about 53% of law firms reported that their firms had a business continuity plan.[20] In addition, firms should routinely back up their data and maintain a copy at an off-site location. Many law firms currently do not have adequate back-up procedures in place. The American Bar Association has a plethora of excellent disaster planning resources available to assist law firms.[21]

9. Consider Cyber Liability Insurance Coverage

Given the potentially devastating financial 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. CNA, as the market leader in lawyers insurance, has industry experience that lawyers can rely on for all of their insurance needs.

10. Use of Cybersecurity Frameworks and Standards

In developing a comprehensive cybersecurity risk management plan, law firms may find it instructive to examine certain accepted frameworks and standards, including International Organization for Standardization (ISO) 27001 and the National Institute of Standards and Technology (NIST) Special Publication (SP) 800. Obtaining the ISO 27001 certification may have the added benefit of placing law firms in a better security posture when responding to client security questionnaires or undergoing security audits. Such certifications may be more appropriate for larger law firms than smaller ones, however, given the significant cost and effort required to obtain and maintain them. Ultimately, obtaining a certification should not be viewed as the final step in the implementation of a cybersecurity risk management plan. An effective cybersecurity risk management program requires continuous monitoring, updating and enforcement. It may be helpful for law firms to retain a security expert to assist them in developing and managing a cybersecurity program that is appropriate for them.

Conclusion

In short, data security represents a real and growing concern for law firms. Excellent data security is increasingly becoming a criteria for clients in selecting legal counsel. In addition, various ethical and legal duties require law firms to make reasonable efforts to provide adequate security for their sensitive data. Failing to provide such security could have serious legal, financial, and reputational consequences. Opportunities exist currently for law firms to improve their data security practices, which will improve their chances of avoiding a potential data breach. Additional CNA risk control resources are available on the CNA website at **www.cna.com**.

Data Breach Checklist

Data Breach Response

- ☐ Confirm an actual breach.
- ☐ Designate an in-house lead to manage the firm's breach response.
- ☐ Record details about the discovery of the breach, including the date and time when the breach was discovered, as well as the date and time when response efforts begin.
- ☐ Preserve any evidence/secure the premises around the area where the data breach occurred.
- ☐ Stop additional data loss. Take affected machines offline but do not turn them off or start probing into the computer until your forensics team arrives. Lock-down systems (ie. change passwords and encryption keys).
- ☐ Restrict information until legal counsel is involved – keep it on a need-to know basis only.
- ☐ Start a preliminary investigation into the incident.
- ☐ Document everything known thus far about the breach.
- ☐ Review cyber liability insurance coverage, if any in place.
- ☐ Report the breach to your insurance carrier.
- ☐ Hire an attorney specializing in cybersecurity and law firm defense.
- ☐ Employ vendors such as forensics, data breach resolution, and PR firms.
- ☐ Investigate the scope of the breach to determine types of information compromised and number of affected individuals.
- ☐ Attempt to retrieve lost or otherwise compromised data.
- ☐ As soon as possible, identify any disclosure obligations to clients and individuals affected by the breach or agencies and other authorities.
- ☐ Consider the need to notify law enforcement.
- ☐ Determine what and how to tell clients, employees and the public.
- ☐ Arrange for credit monitoring or other protection service for affected individuals.
- ☐ Mail / e-mail notifications.
- ☐ Make a public announcement, and launch a website for the breach.
- ☐ Respond to inquiries.
- ☐ Fix the issue(s) that caused the breach.
- ☐ Document when and how the breach was contained.
- ☐ Cooperate with regulatory and government inquiries.

Post-Breach Response

- ☐ Identify and correct any deficiencies in the law firm's cybersecurity program
- ☐ Update technology controls, policies and procedures
- ☐ Make appropriate changes to privacy, security and response plans
- ☐ Conduct retraining of appropriate personnel

Endnotes

1. Verizon, 2012 DATA BREACH INVESTIGATIONS REPORT (April 2013), available for download at **http://www.verizonenterprise.com/DBIR/2013/**.
2. Lisa Ryan, "*Top Firms Aren't Prepared For Cyberattacks: Survey,*" Law 360, (Jan 15, 2015).
3. CNA Lawyers' Professional Liability claim data, Top Causes of Data Breaches, 2003- 2013.
4. Joshua Poje, "*Security Snapshot: Threats and Opportunities,*" ABA TechReport 2014, Legal Technology Resource Center.
5. Debra Cassens Weiss, "*Wilson Sonsini systems engineer pleads guilty to insider trading,*" A.B.A.J., (Nov. 14, 2014, 8:58 A.M. CST), **http://www.abajournal.com/news/article/wilson_sonsini_systems_engineer_pleads_guilty_to_insider_trading**.
6. Debra Cassens Weiss, "*Suit Claims Ex-Partner Installed Software Allowing Continued Access to Law Firm Files,*" A.B.A.J, (Feb. 13, 2012, 1:31 P.M. CST), **http://www.abajournal.com/news/article/suit_claims_ex-partner_installed_software_allowing_continued_access_to_law_/**.
7. Ponemon Institute, 2013 COST OF DATA BREACH STUDY (May 2013), available for download at **http://www.ponemon.org/library/2013-cost-of-data-breach-global-analysis**.
8. Comment 18 to ABA Model Rule of Professional Conduct 1.6.
9. Law Firm Risk Roundtable, 2014 LAW FIRM RISK SURVEY, US Edition.
10. *See* Poje, *supra* Note 4.
11. *See* Poje, *supra* Note 4.
12. Alan Cohen, "*Survey: Data Security is Tech Chiefs' Top Worry,*" The American Lawyer, (Oct. 29, 2014).
13. *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).
14. 2013 Law Firms in Transition, An Altman Weil Flash Survey.
15. Professors Mary Lacity and Leslie Willcocks, "Legal Process Outsourcing: LPO Provider Landscape," September 2012. **http://www.outsourcingunit.org/publications/LPOprovider.pdf**
16. **Http://ridethelightning.senseient.com/2014/03/**
17. *See* Sharon D. Nelson, David G. Ries, and John W. Simek, LOCKED DOWN: INFORMATION SECURITY FOR LAWYERS (ABA, 2012).
18. *See* John D. Sutter, "*How to create a 'super password'*", CNN (Aug. 20, 2010, 9:49 A.M.), **http://www.cnn.com/2010/TECH/innovation/08/20/super.passwords/index.html?hpt=Sbin.**
19. *See* Poje, *supra* Note 4.
20. *See* Poje, *supra* Note 4.
21. **Http://www.americanbar.org/groups/bar_services/resources/disasterrec.html**

CNA

For more information, please call us at 866-262-0540 or email us at lawyersrisk@cna.com.