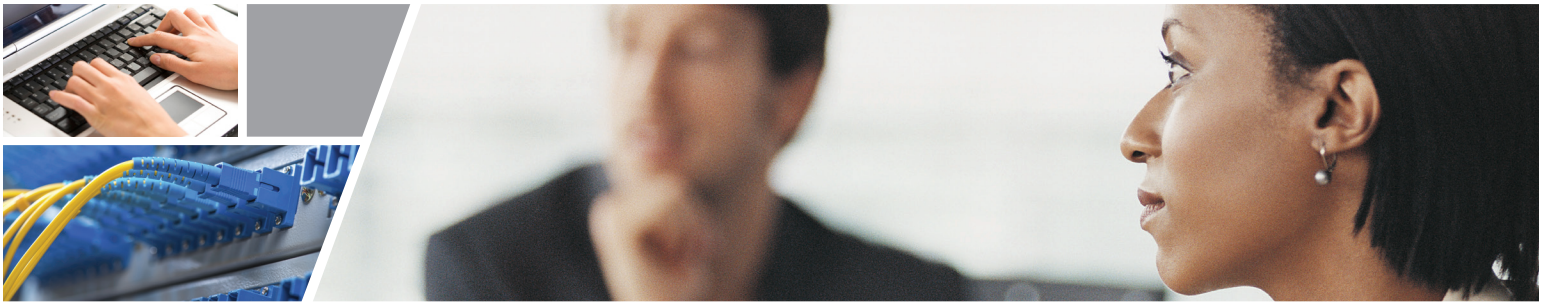
8 Tips for Cyber Security Practices in Law Firms

CNA
We can show you more.®



PROFESSIONAL SERVICES

Most firms already employ common data security tools such as spam filters, anti-spyware, software-based firewalls, and virus scanning on both PCs and in email. These are indeed essential risk management tools, but lawyers and law firms should not assume that installing these security features results in comprehensive protection. These eight tips will help you take the necessary steps to shrink 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.[1] 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.[2] 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.[3] 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.

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.

4. Vet Your Vendors

Lawyers 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,

1 Joshua Poje, "Security Snapshot: Threats and Opportunities," ABA TechReport 2014, Legal Technology Resource Center.
2 Alan Cohen, "Survey: Data Security is Tech Chiefs' Top Worry," The American Lawyer, (Oct. 29, 2014).
3 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).

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% 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") 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.

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. Employers 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. 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.

Conclusion

In short, data security represents a real and growing concern for law firms. Excellent data security is increasingly becoming a criterion 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 sensitive data. Failing to provide such security could have serious legal, financial and reputational consequences. Implementing cyber security practices is the first step in lessening your risk of being hacked. But it's important to have cyber liability coverage to help lessen your financial losses should the worst occur.

To learn more about how to keep your business protected, visit CNA.com.