KANE RUSSELL COLEMAN LOGAN

One Mission. Your Mission.

Recent ABA Ethics Opinion Forces the Legal Profession to Increase Email Security

News / May 31, 2017 / Amy Taylor

How do lawyers and their firms manage and safeguard the information with which they have been entrusted while continuing to inform and communicate with their clients? In an ethics opinion issued earlier this month, the American Bar Association stated that under the professional rules of conduct, attorneys have a confidentiality obligation to take reasonable measures to ensure that unencrypted emails containing client information are safe from cyber threats. This recent ABA opinion suggests that attorneys provide a protocol to determine precisely what those measures should be. It revisits a 1999 opinion that stated attorneys could use unencrypted email for routine client communication because at that time, unencrypted email posed no greater risk of interception or disclosure than any other non-electronic forms of communication.

So what does this opinion really mean for lawyers and their firms? If unencrypted emails are no longer the appropriate form of communication, what is? The recent ABA opinion provides a nice road map in answer to the question and acknowledges that what constitutes reasonable measures will change according to a wide variety of factors. It urges attorneys and their firms to develop processes to address cybersecurity on a case-by-case basis.

The recent ABA opinion offers good guidelines for developing what it calls a "fact-based analysis" which includes a lawyer-conducted threat assessment, an understanding of how client information is relayed and stored, an education about electronic security measures, an assessment of the most appropriate protection steps, the creation of codes or labels for confidential client data, the provision of information security training for lawyers and their staff, and the performance of due diligence with the firm's third-party vendors who handle every aspect of document copying, coding, culling and collection. Much of these tasks must necessarily be handled by attorneys themselves with advice and education from IT staff or trusted IT advisors but ultimately, lawyers can no longer hide behind their IT staff or third-parties should a breach occur. They must be proactive and thoughtful about their education, assessment and prevention. However, the ABA's opinion raises several questions regarding implementation:

1. What role do the 50 state bars play in this new normal? State bars traditionally play a pivotal role in disciplinary proceedings. Does the obligation to provide reasonable measures now mean that state bars must address the disciplinary process when/if there is a breach?
2. How do lawyers and law firms conduct an IT threat assessment?
3. How do lawyers and law firms educate themselves on how client information is elayed/stored/managed? How do they evaluate their electronic security measures and determine the most appropriate protective steps for the information they hold?
4. Are the current available document management systems capable of labelling and protecting confidential client data or are firms now duty-bound to assure that their document management systems are the most robust available?
5. What role does electronic cloud storage bear in this new climate?

6. What malpractice products are available to attorneys and their firms for protection in the event of a breach?
7. What does all this mean for the lawyers and their staff who bring their personal laptops, tablets and phones to work each day?

Regardless, this new opinion will require an abundance of thought and time as law firms navigate this information-sensitive climate.