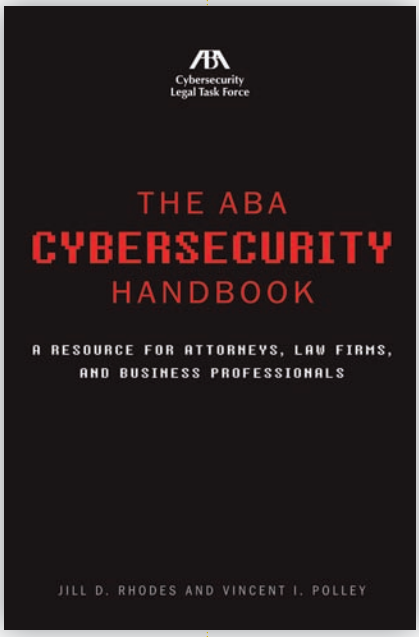
BACK STORY

BOOK REVIEW:
THE ABA CYBERSECURITY HANDBOOK

BY MICHAEL SAUNDERS, ESQ.

With high-profile cyber attacks and data breaches occurring with alarming regularity, it comes as no surprise that in August, the American Bar Association (ABA) adopted Resolution 109. The one-sentence resolution "... encourages all private and public sector organizations to develop, implement, and maintain an appropriate cybersecurity program that complies with applicable ethical and legal obligations and is tailored to the nature and scope of the organization and the data and systems to be protected."[1]



Lawyers and law firms are uniquely situated with respect to cybersecurity, since they are entrusted with highly confidential information, such as information on mergers and other deals that might be attractive to hackers. Also, lawyers and law firms are uniquely situated with respect to cybersecurity, since lawyer ethics rules involving competency and confidentiality are implicated in protecting a client's confidential information. Therefore, the importance and value of lawyers and law firms having cybersecurity programs, such as those encouraged by ABA Resolution 109, is clear, but where should lawyers and law firms begin in instituting such programs?

Reading the ABA's Cybersecurity Handbook would be one practical first step towards instituting a cybersecurity program and gaining greater awareness of cybersecurity issues as they pertain to lawyers. The book, edited by lawyers and cybersecurity experts Jill Rhodes and Vince Polley, features chapters written by nearly 30 authors, including Rhodes and Polley, and is appropriate for lawyers in all areas of practice..

The handbook could have easily devolved into overly technical and convoluted jargon, but instead presents a highly readable, refreshing practical treatment of the subject of cybersecurity as it applies to the needs of those in the legal profession. The book contains informative chapters covering many topics including: understanding cyber and data security risks and best practices, data security and a lawyer's legal and ethical obligations to clients, and best practices for incident response and cyber liability insurance coverage. In addition, the handbook has useful appendices covering federal and state laws pertaining to data security. Perhaps most helpful is that each chapter of the book concludes with actionable ways for lawyers to manage cybersecurity risks.

Nevada Lawyer magazine recently had an opportunity to speak with the handbook's editors, Vince Polley and Jill Rhodes. They shared some practical cybersecurity recommendations for *Nevada Lawyer* readers. As an initial key step, Polley suggested firms appoint someone in management with specific responsibility over cybersecurity, find IT experts either in the firm or outside the firm and address the cybersecurity "low-hanging fruit," such as ensuring data is encrypted and being careful about using public wi-fi. Rhodes advised "knowing your data." She said, "Know what data the firm or your organization actually has and is working with, understand what its sensitivity is or may not be, and know how your people are using that data." She also recommended examining the risks surrounding the usage of that data and considering what policies and practices the organization has in place to protect that data. Finally, she stressed the importance of cybersecurity education, a key theme of the handbook.

Despite a lawyer's or law firm's best efforts to manage cybersecurity risks, the possibility of a data breach is very real. Given that possibility, Polley and Rhodes were asked what should be done in the event of such a breach. Polley advised taking a proactive approach. He said, "You have to do your data breach planning long in advance of the breach, or your response is going to be inadequate." In the event of a data breach, Rhodes suggested first calling the personnel with authority over cybersecurity issues (i.e. the organization's privacy officer, IT security person, and/or managing partner) and discussing the breach. She recommended determining 1) the nature of the disclosure, 2) how much information was disclosed and 3) whether or not the disclosure is still ongoing. Finally, she said the organization should determine what the impact of the disclosure is likely to be and what is to be the appropriate response.

During the interview, Rhodes and Polley both agreed that ignorance of cybersecurity risks is the greatest cybersecurity threat facing lawyers and law firms. In the case of cybersecurity threat awareness, ignorance is inexcusable, particularly when there are excellent resources, such as the ABA Cybersecurity Handbook, readily available. As the saying goes, knowledge is power, and arming yourself with the knowledge that the handbook has to offer would without a doubt represent a powerful first step toward managing your firm's cybersecurity risks. ■

AUTHOR'S BIOGRAPHY is available on page 5.

1. http://www.americanbar.org/content/dam/aba/images/abanews/2014am_hodres/109.pdf