As someone who read (and reviewed http://researchcenter.paloaltonetworks.com/2015/10/the-cybersecurity-canon-locked-down-information-security-for-lawyers/) the first edition, I was delighted to find the second edition even more readable and relevant. There shouldn't be any doubt today regarding the need for lawyers to be competent about how to protect their Client's confidential information—*Locked Down: Practical Information Security for Lawyers*, 2nd Edition enables them to understand the basics of end-to-end information management covering (in depth, in some instances) policies, physical security, authentication, encryption, mobility, network security, remote access, cloud computing, outsourcing (3rd party vendors), social media, cyberinsurance and much more. Conveniently, the Appendices contain the most important cyber collateral (e.g., NIST Framework, relevant ABA Model Rules, Checklists, Sample Security Policies, etc.) so minimal outside resources need to be consulted to use the book as a blueprint for how to be secure.

While the book is written for lawyers (and all lawyers should read it), it is important for all professionals supporting legal services to also read it to understand the role they play in the ecosystem. For example, the chapter on Secure Disposal and Digital Copiers should put lawyers on notice that all people working for them that touch digital (or otherwise) Client information have a hand in ensuring it is properly managed/secured. This may mean hiring consultants with more in-depth knowledge to ensure devices, etc. are properly configured and data flows are mapped and managed (full-lifecycle). The chapter on The Internet of Everything drives home the point that soon absolutely everything will be "connected" making vigilance about proper information management (including information security) all the more important. The chapter on Cloud Computing provides a terrific overview of the issues to be considered (pp. 222-223 cover "reasonable care") in this context. Given how mobile everyone is today, the chapters on Networks: Wired and Wireless and Remote Access should have readers running to their own devices (including home routers) and/or their IT staff/consultants to ensure everything is appropriately configured and working.

Having read hundreds of relevant articles and books over the years, this is the best (most straightforward and appropriately detailed) book on the subject. If you remove the lawyer-specific (mostly ethical) requirements, it stands as a general book on cybersecurity for any business. Every corporate counsel should read this book, both to ensure their own house is in order and to work with all their 3rd Party legal services vendors, particularly law firms. Cybersecurity is so important that every law firm employee should be properly trained (based on their roles) and certainly every law firm IT and Records/Information Governance professional should read and live the content of the book. I stand by my October 22, 2015 prediction that when a law firm is sued by a client because of a data breach, *Locked Down* may one day be "entered into evidence to demonstrate the 'reasonable care' law firms should be taking with respect to security." That day may come soon.

PS-Encryption, encryption, encryption is a mantra rightly reinforced by the authors throughout the chapters that I hope gets into (and stays) in the subconscious of every reader.

Christina Ayiotis, Esq., CRM

Co-Chair, Georgetown Cybersecurity Law Institute