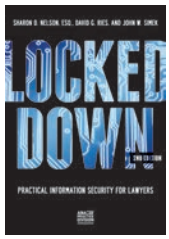
Locked Down:

Practical information security for lawyers, 2nd edition

Sharon D. Nelson, David G. Ries and John W. Simek



The first edition of *Locked Down: Information Security for Lawyers* was published in 2012. It introduced law firms to the increasing importance of having proper cybersecurity for client and firm data. At the time, that concept was still new to a lot of firms and often not taken as seriously as it should have been. In the years since, there have been high profile breaches at companies like Target®, Ebay®, Yahoo® and Panamanian law firm Mossack Fonseca. Law firms in Ontario have been hacked and ransomware infections have become much more common. On a daily basis firms across Ontario are targeted by phishing scams and bad cheque frauds.

Fortunately, most firms now understand the scope of the danger and are making efforts to improve all aspects of their cybersecurity, from employee training to firewalls. The second edition of *Locked Down*, now titled *Practical Information Security for Lawyers* was published in 2016 and offers a roadmap for firms trying to figure out steps to better protect themselves and their clients. The authors, Sharon D. Nelson, David G. Ries and John W. Simek, have backgrounds in the practice of law and information security.

The new edition begins by reminding lawyers why they are considered ripe targets by hackers: the money in their trust accounts and the valuable information about their clients. The law firm of a big corporation is also considered an easier target than the company itself. To paraphrase an expert quoted in the book, "why hack Boeing when it's simpler to hack Boeing's law firm?" To drive the point home, real-life stories of security breaches are included that would keep many firm administrators up at night.

The nature of cyber-attacks has evolved since the first edition was published. For example, phishing attempts are no longer obviously fake emails claiming to be from your bank. They have become more sophisticated and individually targeted, and can appear to come from senior members of your own firm. On the other hand, many of the security vulnerabilities are the same as they've always been: weak passwords, unsafe storage and remote access habits, and outdated software.

Each chapter examines a particular vulnerability. Some could be considered 'front end' issues, such as email, laptops, mobile devices, and desktops. Many hackers find these to be the weakest link because they depend on employees' diligence in following proper security procedures. Other chapters look at the 'back end' of a firm's IT network: storage, servers, backup systems, and wireless encryption.

It's also important to predict what could become security problems in the near future, so the authors devote time to the "internet of things," cloud computing, the expansion of social media, and even drones – imagine a drone hovering outside an office high-rise trying to detect your WiFi signal. Hackers are always adapting their methods to new technologies, so the work of securing your information is never truly done.

There is also a discussion of a lawyer's professional obligation to keep client data secure. In this book, it's in the context of the American Bar Association's *Rules of Professional Conduct* and opinions from American state bar associations. Ontario lawyers will want to refer to the Law Society of Upper Canada's *Technology Practice Guideline* (lsuc.on.ca/with.aspx?id=2147491197). Not only do lawyers have an ethical responsibility to protect client data from cyber breaches, but clients are increasingly demanding to know that a firm's network is secure.

It's beyond the scope of a single book to address every aspect of cybersecurity, and the authors make it clear that their goal is primarily to help lawyers understand the concepts and issues. It is then up to firms to hire their own experts in this field to tailor cyber solutions to their own needs. While immediate steps can be taken in some areas (such as strengthening passwords or improved staff training on security protocols), an expert will be required to address more technical subjects like backup systems, encryption, and firewalls. The book will help the average lawyer understand *why* these issues are critically important.

The practicePRO Lending Library has more than 100 books on a wide variety of law practice management topics. Ontario lawyers can borrow books in person or via email. A full catalogue of books is available online (practicepro.ca/library). Books can be borrowed for three weeks. LawPRO ships loaned books to you at its expense, and you return books at your expense. ■

Tim Lemieux is Claims Prevention and Stakeholder Relations Coordinator at LawPRO.