# A practical guide to help lawyers be cybersafe

LPLC has developed a **Cyber Security Guide** covering five key areas to help time-poor and information-overloaded lawyers understand the risks and act to make their practice safer.

The guide has been designed for sole practitioners and small to medium firms as this is where most of the cyber claims occur, however it is equally relevant as a resource for larger firms.

We know anecdotally that there are many sticking points to implementing greater cyber security measures. Practitioners tell us that they are stretched and don't know where to start when it comes to taking steps to protect their practice.

Our Cyber Security Guide aims to support practitioners to take the first, essential steps in five crucial areas:

1 Secure your technology

2 Establish policies and procedures

3 Create a culture of cyber risk awareness

4 Warn clients about cyber risks

5 Have an incident response plan for prompt action
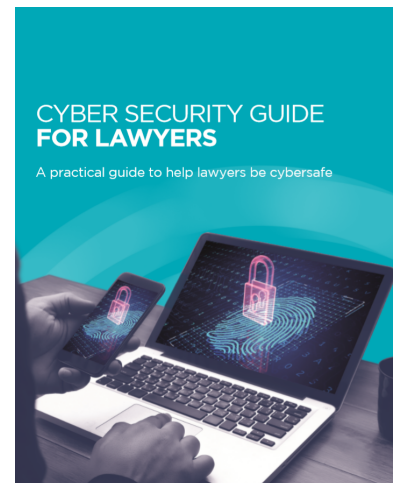
The guide explains briefly why each key area is important, sets out what to do and how to do it. It has been produced in a checklist format and includes links to valuable resources and information for those who want more detail.

Cyber fraud is a pervasive threat to the business operation and reputation of lawyers and law firms. Cyber security is not just an IT issue. It is an essential part of today's legal practice and everyone in the firm has a critical role in preventing cyber-crime.

Awareness plus action is the key. Our Cyber Security Guide for Lawyers provides essential information and practical measures to put firms on the pathway to greater cyber security.

The complete guide and individual checklists can be viewed/downloaded/printed at **lplc.com.au/cyberguide**.

Visit our **cyber security resource page** for a number of additional cyber security resources.

Subscribe