# Data Security
# Ask yourself some key questions

Cyber-assisted fraud, involving doctored emailed bank account details, has had a significant impact on law practices. In considering cyber threats generally, it is important not to overlook the broader issue of protecting private information.

Deciding on the appropriate level of cyber security for your practice can seem daunting, as there are many variables to consider. Making yourself aware of the type of data held by your practice and asking some simple, but important questions is a good start.

**What is the nature and value of your practice data?**

Understand what data is kept by your practice and what information you use in performing everyday functions. Ascertaining the value of your data and how often you use it, can help you to develop appropriate classification levels to ensure that your most sensitive data has the most robust protection. Data such as tax file records, identity documents, medical records and confidential commercial documents are particularly valuable to cyber criminals.

**Who has access to data held by the practice?**

Identify who has access to all levels of your data, including information held at online locations like:

- Files and folders
- Databases
- Online accounts
- Networks
- Mailboxes
- Any other key data storage tools
- Document sharing (e.g. OneDrive or Dropbox)

**Do you employ temps or contract-based staff?**

Who provides you with external services and do these people require access to your systems?

e.g. accountants, website hosts, suppliers or contractors, payroll companies, graphic designers etc.

**How is the data protected?**

Conduct an audit to determine all locations where data is stored and identify the security measures applicable to each location. Is the level of protection appropriate for the type of information being stored?

**What are your practice procedures and policies?**

Are your current procedures regarding data security and storage appropriate for the information being stored? Are your staff aware of the correct procedures and are they being followed?

**What are the current or emerging cyber threats in law practices?**

Cyber threats evolve continually. Stay up to date with current and emerging threats that may be relevant to your law practice. Educate your staff and encourage them to be on the alert.

**How would your practice respond to a cyber security emergency?**

A law practice must know how to respond in the event of a cyber incident. Speed is critical to containing the incident and protecting information and systems from further compromise.

Having a documented plan, regularly reviewed and updated, that sets out how to respond to an incident is an essential first step. The next step is ensuring that the people responsible for responding to a cyber incident are properly trained.

Importantly, the plan needs to be tested regularly to identify any gaps in protection. Learn from test results and address any issues that arise.

The answers to these key questions will provide a strong foundation for protecting your law practice against cyber threats.

Candice Perriman
Rick Education Manager