CYBER PRECEDENT

Strengthening the legal profession's defence against online threats

CHECKLIST: CYBER SECURITY ESSENTIALS

Use this easy checklist to see if your legal practice covers the basics of cyber security.

Issue	Description
Use strong usernames and passwords	• Make sure that all users have individuals accounts • Enforce strong passwords (min 15 character with mix of letters, numbers and symbols) • Have passwords changed on a regular basis
Install Anti-virus and malware protection	• Purchase business grade anti-virus and email filtering (don't use free versions) • Update the software regularly • Have it installed and monitored by a professional
Limited access to systems and files	• Only allow screened persons to view your data • Limit access to important files to employees on a need-to-know basis • Monitor access to sensitive client information
Regular back-up of data	• Regularly back-up all data (critical to any cyber security strategy) • Use both on-site and off-site back-up facilities • Ensure that you can easily access back-up data and restore it to your main system
Encrypt data	• Encrypt your data where possible. Encryption is another security layer that is extremely secure • Encrypt portal devices such as laptops and hard drives. Encrypted data is more difficult to hack
Keep system software up-to-date	• Keep system software up-to-date (older system software such as operating systems may have fundamental security flaws which are remedied through software "fixes" or "patches") • Keep all your system software patched. Install all updates on a regular basis and upgrade your software regularly to ensure that you are protected from vulnerabilities
Protect all devices	• Be sure to protect all devices that access the practice's system including laptops, mobile phones and tablets. Consider installing software allowing remote erasure of data in the event of theft or loss
Training	• Ensure all personnel are fully trained in cyber security measures. Many cyber-attacks are successful because a member of staff was not vigilant
Insurance	• Make sure you have adequate and appropriate insurance to cover you against cyber attacks
Audit your Service Providers	• Send the above list to the firm's outsourced IT service provider, if any, and all cloud service providers, to ensure that they are all taking the same precautions.

The Australian Signals Directorate has published further information about mitigating cyber intrusions, available at www.asd.gov.au/infosec/mitigationstrategies.htm

www.cyberprecedent.com.au

Law Council OF AUSTRALIA