



CYBER RISK MANAGEMENT CHECKLIST

✓ Payment processes and email fraud

- Before accepting and acting upon directions for payment that are provided by email, your organisation verifies the payment details by phone (not using the phone number included in the same email as the directions for payment).
- You inform your customers and suppliers in writing that you will never send them an email changing your bank account details.
- You advise your customers and suppliers in writing to contact you urgently if they receive an email from your organisation purporting to change payment details.
- You regularly check your email set up to ensure that there are no unexpected redirection rules in place (in Outlook, you can check this on the Home screen under Rules, then Manage Rules & Alerts).

✓ Software and virus protection

- You have a process in place to ensure that new software patches are applied to your operating system and software.
- You have antivirus protection in place and is it kept up to date.

✓ Data storage and back-ups

- You complete daily data back-ups.
- You check at least monthly that your back-ups are readily accessible and able to be used/not corrupted upon retrieval.
- Where data is backed up in the cloud, do you know what authentication procedures are required by the cloud provider to ensure that unauthorised users are not able to access your organisations data.

✓ Staff risk-awareness and training

- You have incorporated cyber risk awareness in your staff policies and training.
- Your organisation has a “BYO device” security policy for staff members who are able to access work files on non-company devices such as smart phones, tablets or home computers.
- You have advised all your staff members in writing of the importance of using passwords that are unique to the workplace only.
- You and your staff automatically/regularly change your passwords every few weeks.
- You have discussed with staff the risks associated with using free or unsecured WiFi, importing material onto the organisations computer network through a USB drive, and taking confidential material outside the workplace via USB, mobile phone or laptop.
- You have discussed with staff the risks associated with using free or unsecured WiFi, importing material onto the practice’s computer network through a USB drive, and taking confidential material outside the workplace via USB, mobile phone or laptop.
- Cyber risk awareness included in your induction material for new staff.

✓ Data security breaches and privacy protection

- You have considered whether the Mandatory Breach Reporting regime under the *Privacy Act 1988* (Cth) applies to your law organisation.
- Your policies and procedures note the importance of reporting relevant data breaches.

✓ Planning ahead

- You have an emergency response plan for what to do in the event of a cyber-attack.
- The plan includes seeking crisis assistance from your organisation’s IT consultant with their contact details recorded for immediate response.