5. RISK MANAGEMENT – 'DIRECTORS OBLIGATIONS ON CYBER RISK'

Under the Corporations Act, directors are required to have particular regard around their duty of care, due diligence and continuous disclosure obligations when running a company. This applies to directors involved in running a private, as well as a public organisation. Such obligations extend to all aspects of a business, including a business's IT infrastructure and security.

Directors are no longer able to push the responsibility of cyber compliance on to the IT department or to a third party IT service provider. It is a director's duty to be involved in managing and understanding the real risk associated with cyber security, along with ensuring a strong compliance regime exists that addresses cyber security within the business. Failure to discharge such duties can expose directors to claims from shareholders, along with investigations from regulators such as the Australian Security & Investment Commission (ASIC) and the Office of the Australian Information Commissioner (OAIC).

Australian Government agencies, not for profit organisations and all businesses with revenue greater than $3m have responsibilities under the *Privacy Act 1988.* Even those small businesses with less than $3m of revenue but who collect health information, sell and/or purchase personal information for a benefit have obligations under the Act. It is becoming more common for small businesses to 'Opt In' to the Privacy Act and therefore send a clear message to their clients that they are committed to strong privacy practices. In recent times the Australian Privacy Principals have been updated through the *Privacy Amendment (Enhancing Privacy Protection) Act 2012* (Cth). Australian Privacy Principal (APP) 11 requires entities governed by the Act to *take reasonable steps to protect personal information it holds from:*

(a) Misuse, interference and loss; and
(b) From unauthorised access, modification and disclosure.

Significant penalties may apply for breaches of the Privacy Act, including fines of up to $340,000 for individuals and $1.7m for organisations. With this in mind, directors of companies need to start understanding the following about their business.

- Who is responsible for cyber security within the organisation? Is there a dedicated Information Security Officer? Do the Board of Directors have oversight around cyber security? For SME businesses, does the director(s) understand how IT is managed within the business? If it is outsourced, do they understand the terms and conditions in place with the outsource providers?

- Does the company have policies in place that identify external and internal threats to the organisation? How does the organisation deal with mobile device security and off site access to systems?

- Does the company have an incident response plan in place and how effective is this plan? Does it specifically deal with IT downtime caused by malicious threats and accidental human errors? Has the plan been tried and tested and is it distributed to key members within the organisation?

- What insurance does the organisation carry to deal with cyber breaches? What are the limits? Are there specific exclusions which may remove cover for the organisation in certain ways? Is it a full cyber policy, or an *add on* policy? Does it provide access to a strong incident response team who can support an organisation when an incident occurs?

With obligations on directors increasing at a rapid rate, cyber risk management should now be at the forefront of all directors' minds.