Honan.
Insurance. Advice. Support.

CYBER RISK CHECKLIST

Understand Your Cyber Risk	Y/N
Are you aware of the impact and possible cost of a cyber/data breach on your organisation and how you would respond?	
Do you know the biggest cyber risks faced by your industry?	
Are you aware of the changes to legislation regarding mandatory notification of data/ network breaches and whether these impact on your business?	
Can you easily determine what information about your business is currently in the public domain, and how this affects your risk profile?	
Can you identify what information/data within your organisation might be targeted by cyber criminals and why?	
Does your business collect and store personally identifiable information? How many records are kept and is the information shared with third parties?	
Cyber Risk Strategy – *Important for Directors	**Y/N**
Are you aware of your Directors' obligations with respect to protection of your network data and notification of breaches or suspected breaches?	
Is network security integrated into your corporate risk management framework? ▪ Do you have a disaster recovery/incident responsez plan? ▪ Are security policies enforced and updated and do these match your business size? ▪ Is data ownership established and is it classified by its usage and sensitivity? ▪ Do you have a computer software and hardware asset inventory list?	
Does your organisation have written and implemented policies and procedures around privacy, handling sensitive information, usage of internet, email, portable devices, remote working, passwords, making payments?	
What is your review/audit process to ensure compliance with cyber risk policies and procedures?	
Is there adequate training in place to educate staff on cyber risk, privacy obligations, compliance with company policies and procedures, identification of suspicious activity and how to report this?	
Does the organisation hold a Cyber Liability Insurance policy as part of its risk management?	
Network Security Infrastructure - How resilient is your organisation?	**Y/N**
IT Department ▪ Do you outsource your IT? Fully/partially? Does this include your IT security? ▪ Have you ever performed security penetration testing of your network to identify vulnerabilities? ▪ Is all software updated when required? Is anti-virus software active for all users? ▪ Are you ensuring physical security of systems and facilities? ▪ Are file logs reviewed ensuring system backups with periodic data restores? ▪ Are issues, risks and potential breaches reported internally? Is there a procedure? ▪ Do you develop or manage applications that collect and store usernames and passwords?	