Australian Institute of Company Directors

CYBER SECURITY COOPERATIVE RESEARCH CENTRE

SME and NFP Director Checklist

1. Set clear roles and responsibilities	Document where possible who has responsiblity for cyber security
	Appoint a cyber champion to promote cyber resilience and respond to questions
	Consider whether a director, or group of directors, should have a more active role in overseeing cyber security
	Collect data where possible on the effectiveness of cyber risk practices
2. Develop, implement and evolve a comprehensive cyber strategy	Utilise the ACSC Cyber Security Assessment Tool to identify the cyber security strengths of the organisation and understand areas for improvement
	Assess whether utilising reputable external providers will enhance cyber resilience over managing in-house
	Assess whether there is certain data (e.g. employee or customer data) that does not need to be collected
	Establish an Access Control System to determine who should have access to what
	Regularly repeat cyber securily training and awareness amongst all employees
	Promote strong email hygiene
3. Embed cyber security in existing risk management practices	Patch and update applications and anti-virus software
	Configure Microsoft Office macro settings (e.g. only macros from trusted locations enabled)
	User application hardening - limit interaction between internet applications and business systems
	Limit or restrict access to social media and external email accounts
	Restrict use of USBs or external hard drives
	Restrict operating system and software administrative privileges
	Implement multi-factor authentication
	Maintain offline backups of key data
	Ensure that departing employees or volunteers no longer have access to systems and passwords

4. Promote a culture of cyber resilience	Mandatory training and phishing testing for all employees and volunteers where appropriate
	Pick a staff member to be a 'cyber security leader' to promote strong cyber practices and respond to questions from other staff
	Subscribe to ACSC alerts to stay across emerging cyber threats
5. Plan for a significant cyber security incident	Prepare an incident response plan utilsing online templates if appropriate
	If practical conduct a simulation exercise or test various scenarios against the incident response plan
	Ensure physical back-ups of key data and systems are regularly updated and securely stored
	Maintain offline lists of who may assist in the event of a significant cyber security incident and which key stakeholders to communicate with

SME AND NFP RESOURCES

1. ACSC: **Cyber security for small and medium businesses**
2. ACSC 24/7 Hotline on 1300 CYBER1 (1300 292 371)
3. Council of Small Business Organisations of Australia: **Cyber Security Resources**
4. CSCRC: Smaller but Stronger: **Lifting SME Cyber Security in South Australia**

CCT-106-4_22