CYBER SECURITY
CHECKLIST

GET STARTED

BDO

Do you understand the cyber risks your business is facing? This checklist can deliver the insights your organisation needs to lower its cyber risk profile.

Any effort to create a cyber-resilient business has to be led by the board of directors, who recognise the growing complexity of the organisation's digital presence and are responding with an effective strategy to mitigate emerging cyber risks.

The end goal is to become a cyber-resilient organisation, one where cyber threats are well understood and measures exist to defend the organisation's digital assets against cyber incidents. To aid in this goal, we have developed this checklist to take you through the process of building a cyber-resilient organisation.

UNDERSTANDING YOUR CYBER RISK PROFILE

- ☐ Do you know what the biggest cyber risks are in your industry?
- ☐ Do you have an understanding of the cyber-criminals active in your industry and how it relates to your organisation?
- ☐ Do you know which cyber-criminals would benefit from having access to your information and systems?
- ☐ Do you know what information about your business is currently in the public domain?
- ☐ Have you considered how this information affects your risk profile and ability to respond to a cyber attack?
- ☐ Do you know what the costs will be for your organisation to respond to and recover from a serious cyber incident?

IDENTIFYING YOUR BUSINESS CRITICAL DIGITAL ASSETS

- ☐ Do you know what information and systems your business needs to keep operating?
- ☐ Do you know where your business critical information and data is located?
- ☐ Do you know who has access to it?
- ☐ Do you understand the risks associated with information held by your third party suppliers?
- ☐ Do you know how effective your digital assets are protected?
- ☐ Do you know what the impact and consequences will be to your business if these are compromised?
- ☐ Is this within your risk appetite?
- ☐ If not, are you considering additional measures or strategies to lower your risk exposure?

INTEGRATING CYBER WITH STRATEGY

- ☐ Do you consider cyber risks during your strategic planning process?
- ☐ Is cyber integrated into your corporate risk management framework?
- ☐ Have you established mechanisms to regularly review and assess changes in your cyber risk landscape?
- ☐ Do you have access to cyber threat intelligence information or collaborate on sharing threat information?
- ☐ If your organisation changes direction or moves into a new market, do you have a mechanism in place to address any new cyber risks?
- ☐ Do you have effective cyber security awareness training across all levels in your organisation?
- ☐ Have you considered cyber insurance as part of your cyber risk management strategy?

BUILDING A CYBER-RESILIENT ORGANISATION

- ☐ What is the current level of knowledge regarding cyber risks across the board of directors?
- ☐ How often does the Board discuss cyber security trends and risks and how this might impact your business and strategy?
- ☐ How effective is your internal capability to manage these increased cyber risks?
- ☐ Are you aware of changing privacy and data breach legislation and how this will affect the Board's cyber breach disclosure duties?
- ☐ Do you know what to do when you have been breached?
- ☐ Do you have mechanisms in place to identify and respond to cyber incidents?
- ☐ How regularly is your cyber incident response plan tested?

NEW SOUTH WALES
NORTHERN TERRITORY
QUEENSLAND
SOUTH AUSTRALIA
TASMANIA
VICTORIA
WESTERN AUSTRALIA

1300 138 991
www.bdo.com.au

Distinctively different – it's how we see you

AUDIT • TAX • ADVISORY

This publication has been carefully prepared, but it has been written in general terms and should be seen as broad guidance only. The publication cannot be relied upon to cover specific situations and you should not act, or refrain from acting, upon the information contained therein without obtaining specific professional advice. Please contact the BDO member firms in Australia to discuss these matters in the context of your particular circumstances. BDO Australia Ltd and each BDO member firm in Australia, their partners and/or directors, employees and agents do not accept or assume any liability or duty of care for any loss arising from any action taken or not taken by anyone in reliance on the information in this publication or for any decision based on it.

BDO refers to one or more of the independent member firms of BDO International Ltd, a UK company limited by guarantee. Each BDO member firm in Australia is a separate legal entity and has no liability for another entity's acts and omissions. Liability limited by a scheme approved under Professional Standards Legislation other than for the acts or omissions of financial services licensees.

BDO is the brand name for the BDO network and for each of the BDO member firms.

© 2016 BDO Australia Ltd. All rights reserved.