NON - PROFITS AND CHARITIES

ASKING ALL THE RIGHT QUESTIONS

EMPOWERING COMPANY DIRECTORS IN

CYBER SECURITY

GOVERNANCE

Understand your professional and personal obligations and learn how you can ensure your organisation is doing enough to combat cyber risks.

Introduction

In the rapidly evolving digital landscape of 2024, cyber security has emerged as a critical concern for organisations worldwide. Australian company directors are finding themselves with an increasing responsibility to comprehend, oversee, and guide cyber security efforts. This briefing document aims to provide essential insights into the evolving landscape of cyber security responsibility, supported by relevant survey data, and equip Australian company directors with the knowledge and questions necessary for effective governance.

The Evolving Landscape of Responsibility

As cyber threats grow in sophistication, the landscape of responsibility for cyber security is undergoing a paradigm shift. Traditionally considered the purview of IT departments, cyber security is now recognised as a board-level concern. Company directors are expected to be proactive in understanding, assessing, and mitigating cyber security risks to safeguard the organisation's assets, reputation, and stakeholder trust.

Australian Business Landscape

In Australia, regulatory frameworks such as the Notifiable Data Breaches (NDB) scheme underscore the importance of cyber security governance. The government's emphasis on cyber security aligns with the increasing expectations placed on company directors to ensure compliance and resilience against cyber threats and we should expect this pressure to increase proportionately to the risks.

Board Members' Role in cyber security

To address this gap in awareness and knowledge, company directors must recognise that cyber security is not solely a technical matter but a strategic business risk. Understanding the organisation's risk profile, data protection measures, and testing procedures are fundamental aspects of effective governance.

Asking the right questions…key questions for Australian Company Directors to ask their teams

Company directors are encouraged to use the following questions to help assess and enhance their organisation's cyber security posture:

Asking the Right Questions of Your IT Teams

1. Understanding Risk Profile

- *How do you, as a Director, understand the risk profile of our business systems?*
- *What is the most sensitive data that resides in the system?*
- *What is the primary and sub-function of the application and service?*
- *What functions can't be provided to the business without this system or service?*

2. Data Protection and Unauthorised Access or Theft:

- *What protections are in place to protect data from unauthorised access or theft?*
- *How would we know if our data has been stolen or accessed by unauthorised individuals or organisations?*

3. Testing and Preparedness:

- *How often is the cyber security of our systems and services tested?*
- *What is the process for assessing and addressing vulnerabilities identified during testing?*

By incorporating these questions, company directors can engage in strategic discussions with organisational leaders, fostering a deeper understanding of cyber security risks and measures. The goal is to empower company directors to actively contribute to the organisation's cyber security governance and resilience.

Isn't this the Chief Information Security Officer (CISO)'s job?

Considering the information presented above, it may be tempting to consider the task of cyber security to be solely the domain of your organisation's CISO.

However, even with a CISO in place, as we have outlined above, Directors still have a major role and responsibility to ensuring that their organisation is addressing cyber security risks and vulnerabilities. A good CISO will be appreciative of the support from more pro-actively involved Board Members. At a minimum, you will be signalling your support and awareness of this critical area.

Where to go for more help

We are not suggesting that Board Members need to become cyber security experts, but simply to take the opportunity to be proactively involved in ensuring their organisations are taking effective steps on their cyber security journey. However, where there is a need and/or interest, the link below provides a number of resources that may be helpful.

www.9thmind.com.au

"By 2026, 70% of boards will include one member with cybersecurity expertise.
For cybersecurity leaders to be recognized as business partners, they need to acknowledge board and enterprise risk appetite. This means not only showing how the cybersecurity program prevents unfavorable things from happening, but how it improves the enterprise's ability to take risks effectively. Gartner recommends CISOs get ahead of the change to promote and support cybersecurity to the board and establish a closer relationship to improve trust and support."

- **Gartner's Top Eight Cybersecurity Predictions for 2023-2024**

9TH MIND

ADVISORY

This briefing document was produced by 9th Mind Advisory. We are cyber security professionals who are passionate about helping organisations make pragmatic progress on their cyber security journeys. We work with Executive Leaders who often find themselves out of the loop concerning their organisation's actual cyber security position and we help them to ask the right questions of their organisation's leadership in order to facilitate progress.

You can contact us at: contact@9thmind.com.au | 1300 432 956 | www.9thmind.com.au