Australian Institute of Company Directors

CYBER SECURITY COOPERATIVE RESEARCH CENTRE

A CONCISE SNAPSHOT:

Cyber Security Governance Principles

PRINCIPLE 1:

Set clear roles and responsibilities

KEY POINTS

1. Defining clear roles and responsibilities is a foundational component of building effective cyber resilience
2. Comprehensive and clear board reporting, including engagement with management and updates on emerging trends, is a key mechanism by which a board can assess the resilience of the organisation
3. External experts can play a role in providing advice and assurance to directors and identify areas for improvement

GOVERNANCE RED FLAGS

1. Cyber risk and cyber strategy not featuring regularly on board agendas
2. Board not annually reviewing skills to ensure that directors have a minimum understanding of cyber security risk
3. Board reporting on cyber risk is hard to digest and features excessive jargon with a reliance on technical solutions
4. Limited or no external review or assurance of cyber risk controls and strategy
5. No clear lines of management responsibility for cyber security

PRINCIPLE 2:

Develop, implement and evolve a comprehensive cyber strategy

KEY POINTS

1. A cyber strategy, proactively overseen by the board, can be a business enabler by identifying opportunities for the organisation to build cyber resilience
2. Identifying the key digital assets and data of an organisation, including who has access to these assets, is core to understanding and enhancing cyber capability
3. A robust cyber strategy will account for the importance, and potential risks, associated with key third-party suppliers

GOVERNANCE RED FLAGS

1. Lack of formal documentation of the organisation's approach to cyber security
2. Limited understanding of the location of key digital assets and data, who has access and how they are protected
3. The cyber strategy and risk controls are not subject to internal and external evaluation and periodic refinement relative to evolving threats
4. Lack of data governance framework to guide how data is collected, held, protected and ultimately destroyed

PRINCIPLE 3:
Embed cyber security in existing risk management practices

KEY POINTS

1. Cyber risk is still an operational risk that fits within an organisation's existing approach to risk management
2. While cyber risk cannot be reduced to zero there are a number of accessible and low-cost controls that all organisations can utilise to mitigate the risk
3. The board should regularly assess the effectiveness of cyber controls to account for a changing threat environment, technological developments and the organisation's capabilities

GOVERNANCE RED FLAGS

1. Cyber risk and cyber strategy not reflected in existing risk management frameworks
2. High management confidence that cyber risk controls are effective without regular external validation
3. Over reliance on the cyber security controls of key service providers, such as cloud software providers
4. Cyber security controls and processes of potential vendors are not assessed in the procurement process for key goods and services
5. Prolonged vacancies in key cyber management roles

PRINCIPLE 4:
Promote a culture of cyber resilience

KEY POINTS

1. A truly cyber resilient culture begins at the board and must flow through the organisation and extend to key suppliers
2. Regular, engaging and relevant training is a key tool to promote a cyber resilient culture, including specific training for directors
3. Incentivise and promote strong cyber security practices, including participating in phishing testing and penetration exercises

GOVERNANCE RED FLAGS

1. Board and executives do not undertake cyber security education nor participate in testing
2. Cyber security is not reflected in the role statements and KPIs of key leaders
3. Communication from leaders does not reinforce the importance of cyber resilience to staff (cyber is seen as an issue only for frontline staff to manage)
4. There is a culture of 'exceptions' or workarounds for board and management with respect to cyber hygiene and resilience

PRINCIPLE 5:
Plan for a significant cyber security incident

KEY POINTS

1. Directors and management should proactively plan for a significant cyber incident
2. Simulation exercises and scenario testing are key tools for the board and senior management to understand and refine roles and responsibilities
3. A clear and transparent approach to communications with key stakeholders in a significant cyber incident is critical in mitigating reputational damage and allowing for an effective recovery

GOVERNANCE RED FLAGS

1. The board and senior staff have not undertaken scenario testing or incident simulations to test the Response Plan
2. Likely scenarios and consequences are undocumented with lessons from simulations not being captured
3. It is not clear how communications with key stakeholders will be managed in the event of an incident
4. No post incident review with board and management

Top 10 director questions

Roles and responsibilities

1. Does the board understand cyber risks well enough to oversee and challenge?
2. Who has primary responsibility for cyber security in our management team?

Cyber strategy

3. Do we understand our current cyber security capability and have a plan to enhance this capability?
4. How does our approach to enhancing cyber security support our broader organisational strategy and strategic initiatives?

Cyber security risk management

5. Where, and with whom, are our key digital assets and data located?
6. How regularly does management present to the board or risk committee on the effectiveness of cyber risk controls?

Cyber resilient culture

7. Is cyber security training mandatory across the organisation and is it differentiated by area or role?
8. Does the board and senior management reinforce the importance of cyber security and collective responsibility?

Cyber incident planning

9. Do we have a cyber incident response plan, including a comprehensive communications strategy, informed by simulation exercises and testing?
10. Can we access external support if necessary to assist with a significant cyber security incident?

Comprehensive guidance for directors is contained in the *Cyber Security Governance Principles* from the AICD and the CSCRC

ACKNOWLEDGEMENT OF COUNTRY

The Australian Institute of Company Directors acknowledges the First Nations people across this Country. We acknowledge the Traditional Custodians of the Lands on which our organisation is located and where we conduct our business. We pay our respects to the Elders, past and present, and recognise those who continue to promote and protect First Nations cultures. The Australian Institute of Company Directors is committed to honouring First Nations peoples' unique cultural and spiritual relationships to the Skies, Lands, Waters, and Seas, and their rich contribution to society. We acknowledge the past and stand together for our future.

ABOUT CSCRC

The CSCRC develops cyber security capability and capacity to help keep Australia safe. We do this by developing innovative, real-world research and cultivating outstanding talent to solve pressing cyber security challenges for the nation.

ABOUT AICD

The Australian Institute of Company Directors is committed to strengthening society through world-class governance. We aim to be the independent and trusted voice of governance, building the capability of a community of leaders for the benefit of society. Our membership includes directors and senior leaders from business, government and not-for-profit sectors.

DISCLAIMER

The material in this publication does not constitute legal, accounting or other professional advice. While reasonable care has been taken in its preparation, the AICD and CSCRC do not make any express or implied representations or warranties as to the completeness, reliability or accuracy of the material in this publication. This publication should not be used or relied upon as a substitute for professional advice or as a basis for formulating business decisions. To the extent permitted by law, the AICD and CSCRC exclude all liability for any loss or damage arising out of the use of the material in the publication. Any links to third-party websites are provided for convenience only and do not represent endorsement, sponsorship or approval of those third parties, any products and services offered by third parties, or as to the accuracy or currency of the information included in third-party websites. The opinions of those quoted do not necessarily represent the view of the AICD and CSCRC. All details were accurate at the time of printing. The AICD and CSCRC reserve the right to make changes without notice, where necessary.

COPYRIGHT

For more information about Cyber Security Governance Principles | Version 2 November 2024, please contact:

E: policy@aicd.com.au

JOIN OUR SOCIAL COMMUNITY

aicd.com.au

CCT1571_24