Australian Institute of Company Directors

CYBER SECURITY COOPERATIVE RESEARCH CENTRE

Snapshot of the Cyber Security Governance Principles

1. Set clear roles and responsibilities

Defining clear roles and responsibilities is a foundational component of building effective cyber resilience

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

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 periodically on board agendas
2. Chair and 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

2. Develop, implement and evolve a comprehensive cyber strategy

A cyber strategy, proactively overseen by the board, can be a business enabler by identifying opportunities for the organisation to build cyber resilience

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

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 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

3. Embed cyber security in existing risk management practices

Cyber risk is an operational risk that fits within an organisation's existing approach to risk management

While cyber risk cannot be reduced to zero there are a number of accessible and low-cost controls that all organisations can utilise

The board should regularly assess the effectiveness of cyber controls to account for a changing threat environment, technology developments and the organisation's capabilities

GOVERNANCE RED FLAGS:

1. Cyber risk 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 of potential vendors are not assessed in the procurement process for key goods and services
5. Prolonged vacancies in key cyber management roles

4. Promote a culture of cyber resilience

A cyber strategy, proactively overseen by the board, can be a business enabler by identifying opportunities for the organisation to build cyber resilience

Regular, engaging and relevant training is a key tool to promote a cyber resilient culture, including specific training for directors

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

5. Plan for a significant cyber security incident

Directors should proactively prepare and plan for a significant cyber incident

Simulation exercises and scenario testing are key tools for the board and senior management to understand roles and responsibilities

A clear and transparent approach to communications with all 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. Who has internal responsibility for the management and protection of our key digital assets and data? 4. Where, and with whom, are our key digital assets and data located?
Cyber risk management	5. Is cyber risk specifically identified in the organisation's risk management framework? 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. How is the effectiveness of training measured?
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?