PEAKSTONE™ GLOBAL
GOVERNANCE | TRUST | PERFORMANCE

The Governance of Cyber

Helping boards align their governance of cyber with leading practices

An agenda item for every board director

- Most organisations regardless of size or sector hold cyber risk as a "high" risk at the enterprise level.
- Many now take a stance of "when" and not "if" to the likelihood of a major cyber event in the short to medium term.
- Impacts of a cyber-security event are often material and reputationally damaging driven by data breach and/or supply chain disruption. There are many victim case studies.
- Given the dynamic nature of cyber threats; organisations must continuously evolve, enhance, monitor and report risk mitigation within a robust governance framework; ***The Governance of Cyber.***
- Boards recognise cyber security and cyber resilience must be towards the top of their governance priorities and every Board has ***three*** key cyber governance responsibilities:

  1. Oversight: assuming ultimate responsibility for governing cyber risk and therefore overseeing mitigation strategy, policies and activities.
  2. Staying informed: remaining cyber risk savvy; generally, and more specifically to the relevance of cyber to the organisation
  3. Setting the tone: setting and living the organisations values, risk culture and expectations regarding cyber resilience.

- Given the above context, all Boards should frequently and specifically assess how well their governance of cyber aligns with better practices.
- One critical element of cyber, not often discussed, is how Boards ensure Management is finding the balance between the performance of their information and technology and their conformance obligations.
- Ensuring that the 'performance' and 'conformance' are finding the right balance and priority is a critical oversight activity.

Aligning with cyber governance leading practices

- There is a lot of guidance available to Boards on cyber governance issued by big four accountants, lawyers, recruiting firms, training providers, professional bodies, regulatory bodies and others.
- At Peakstone Global (www.peakstoneglobal.com) we have reviewed much of this guidance from a board member's perspective.
- Overall, the principles based guidance issued by the Australian Institute of Company Directors (AICD) in partnership with the Cyber Security Cooperative Research Centre (CSCRC) provides an appropriate framework for Boards to use as a reference point for better cyber governance practices.*

- In short, this guidance, issued in October 2022 is independent, clear, comprehensive, current and pragmatic. It encourages boards to consider cyber governance through five principles:

1. Set clear roles and responsibilities
2. Develop, implement and evolve a comprehensive cyber strategy
3. Embed cyber security in existing risk management practices
4. Promote a culture of cyber resilience
5. Plan for a significant cyber security incident.

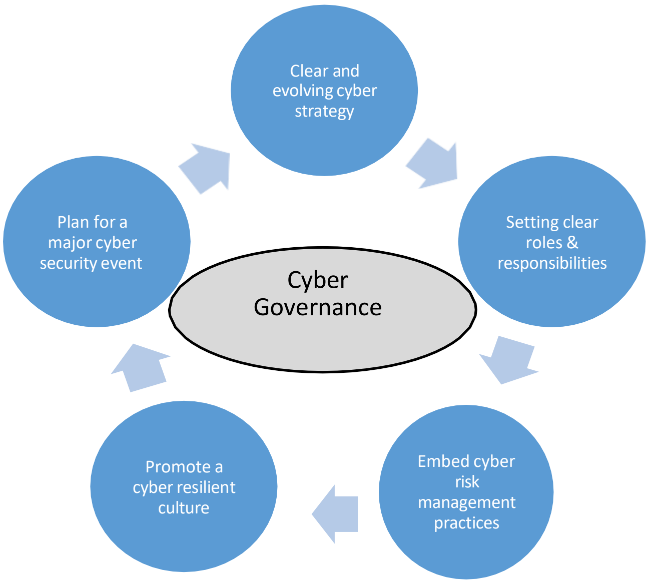
* A full copy of the guidance titled *Cyber Security Governance Principles* can be found at: https://www.aicd.com.au/risk-management/framework/cyber-security/cyber-security-governance-principles.html

Peakstone Global: Helping Organisations Elevate Cyber Governance Practices

Peakstone Global is a leading governance advisory firm. Our advisors work with Boards in all sectors to diagnose, design, deliver and embed improvements in governance processes for improved business outcomes.

Our board review services incorporate the governance of cyber at an elevated level. However due to the high profile of cyber risk for all Boards, our advisors have developed a tried and trusted approach to helping Boards assess alignment with better cyber governance practices. We use an approach built around the *Cyber Security Governance Principles* referred to above based on deep domain expertise and thought leadership in the governance of cyber.

We collaborate with board members and those within the organisation’s executive team with cyber risk management responsibilities to determine the current and desired state of alignment with each of the five key governance principles.


Clear and evolving cyber strategy
Setting clear roles & responsibilities
Embed cyber risk management practices
Promote a cyber resilient culture
Plan for a major cyber security event
Cyber Governance

Through short and targeted face to face discussions on each side of the Board / Management interface and a review of relevant documentation, we form and share an independent and balanced view on the “as is” and “to be” status of your cyber governance framework. For each key principle and overall, we will assess current alignment as “well aligned,” “generally aligned” or “misaligned.”

Taking account of your evolving approach to cyber security and cyber resilience, we will work with you to identify and action prioritised opportunities for improvement. These will be informed by our broader cyber governance experience from other companies.

Our deliverable will be discussed and agreed with board members and management and will provide a valuable assessment of the current state of cyber governance practices and a clear and aligned roadmap for further improvement.

Why Peakstone Global?

- We are leading advisors in board governance processes and practices with deep and broad international experience across all sectors.
- Our advisors have extensive experience working with Boards through the Board/ Management interface and specifically in matters relevant to cyber governance.
- Our cyber better practices assessment approach is proven and trusted.
- We are independent and free from conflicts of interest. For example, we will restrict our services to advising on the governance of cyber and as such our work stops there. Unlike some advisors we will not use our assessment of cyber governance better practices to serve as a gateway to additional work.

Key Peakstone Global Contacts

Our advisors Jason Wilk and Darren Taylor have significant international experience of the governance of cyber and better practices.

Since 1999, Jason has specialised in cyber. He headed cyber risk for several large financial institutions with Board level exposure. He co-founded and was the Managing Director of a boutique consulting firm specialising in the governance and management of technology and cyber security. He is the thought leader and course author for AICD cyber and technology courses including *Cyber for Directors*, *The Boards Role in Cyber* and the tailored variants of these courses. The learnings from delivering these courses since 2016 formed the underpinning for the creation of the *AICD Cyber Security Governance Principles*.

Darren is a risk and governance specialist with international experience (Europe / Australia/US). He was a Managing Director within Protiviti (global risk management consultancy) and Chief Audit Executive for a global S&P500 company. He has Project Management Office leadership experience of cybersecurity as an enterprise risk and has reported on cyber risk management and resilience to boards and subcommittees. He has specific experience assessing cyber governance against better practices working with Directors and Management.

If you would like a discussion on how Peakstone Global can help your organisation please contact them directly:

DARREN TAYLOR

Specialist Advisor

E: dtaylor@peakstoneglobal.com

M: + 61 (0) 466 938 217

Areas of Expertise

- Board governance and compliance including the risk and audit agendas
- Internationally experienced within the corporate (ASX & NYSE) and public (Australian & UK) sectors
- Managing the interface between the Board and Management regarding cyber risk

JASON WILK

Practice Director – Governance of Information & Technology

E: jwilk@peasktoneglobal.com

M: +61 (0) 403 588 111

Areas of Expertise

- Technology strategy and risk for Directors and the interface with management
- Cyber for Directors and Officers, from culture to crisis management
- Managing the interface between the board and management regarding governance of information and technology