KEY TAKEAWAYS

People

People are an essential part of good cyber governance. Their positive attitude and behaviours are vital to shaping a positive cyber security culture.

1. Promote positive behaviours

Boards set the tone in promoting a positive cyber security culture through constructive questioning in meetings and adhering to policies. They must lead by example, avoiding special treatment, as their actions influence the organisational attitude toward security. Addressing cultural issues such as staff perception of the handling of blame is key to continuous improvement.

2. Practical policies

Fair policies that balance cyber security with workforce needs require collaboration between Executives and employees. Boards must ensure collaboration across the organisation occurs, making policies practical, supportive, and effective.

3. Ongoing learning

The Board should ensure a continuous training program is in place with feedback mechanisms to test understanding. Regular monitoring of progress, through both quantitative and qualitative feedback, will help identify areas for improvement. Developing the capability to tackle evolving cyber challenges is crucial for effective cyber governance.

4. Open communication

Boards should foster an environment where employees and stakeholders are encouraged to voice concerns and offer security insights freely, without fear of retribution. Organisational communication mechanisms should encourage this behaviour and be integrated into the cyber security strategy. This promotes knowledge sharing, identifies potential risks, and encourages a collective responsibility for cyber security. Regular cyber security discussions in the boardroom help maintain its priority within the organisation.

Remember

Culture is an outcome of the right behaviours and actions, not an input that can be quickly altered. You can encourage behaviours that create the right cyber security culture, but changing culture itself is a gradual process.

Question for the Board

Does your organisation have a 'no blame' culture? *While 'no blame' doesn't mean no accountability, a culture of learning from incidents and focusing on underlying causes and responses leads to continuous improvement. Blaming individuals or teams signals a less mature cyber security culture.*