KEY TAKEAWAYS

Assurance and Oversight

Embedding cyber security within the organisation's governance structure is essential to making it a core part of decision-making at all levels. Accountability for an organisation's cyber resilience begins with the Board, whose oversight and assurance ensure that governance and risk management processes are effective and aligned with organisational resilience and risk appetite.

1. Strategic alignment

It's essential to ensure the cyber security strategy is integrated and resourced within the wider organisational strategy. This alignment guides decision-making, ensuring cyber security supports the business objectives and allows the Board to take ownership of the overall risk management approach.

2. Monitoring and reporting

Establishing a robust governance framework ensures that monitoring and reporting of cyber risks strengthen the overall cyber security posture. This framework should include clear roles and responsibilities for Board members, regular updates on cyber risk management, and a commitment to continuous improvement. By integrating cyber governance into the Board's agenda, organisations can ensure that cyber security is prioritised at the highest level, fostering a culture of vigilance and resilience.

3. Collaboration in cyber security governance

Cyber security responsibilities involve the whole organisation and require active participation from the Board. Collaboration between the Board, Senior Executives, and the Chief Information Security Officer (CISO) is essential to ensure alignment, shared understanding, and proactive risk management. By ensuring that areas like Finance and Procurement incorporate cyber security when considering new suppliers; and major investments have cyber security designed into their plans from the outset, embeds cyber into everyday thinking. This approach makes it a fundamental part of the organisation rather than an afterthought.

4. External and internal assurance

External assurance provides organisations with an independent assessment of their cyber resilience, ensuring compliance with legal and regulatory standards while instilling stakeholder confidence. Internal audits, while conducted by the organisation, maintain objectivity and complement external reviews by addressing gaps, validating measures, and reinforcing governance actions. The Board must gain assurance that these audits are effective, appropriately focused, and in line with the organisation's risk appetite.

Remember

Board members don't need to be technical experts, but they must have a holistic understanding of cyber security risk within their organisation to discuss issues and challenge assumptions with stakeholders. They also need to ensure that the right mechanisms and processes are in place for effective oversight and assurance.

Question for the Board

Has an independent external cyber security risk assessment been considered? *An external cyber risk assessment can offer valuable insight into the organisation's security posture, helping the Board make informed decisions and guide the cyber security strategy. The scope of the assessment should be tailored to the organisation's needs and budget.*