KEY TAKEAWAYS ›

Risk Management

Boards already know that effective risk management helps Executives make informed decisions which support the successful delivery of the business strategy. This learning outlines five key insights to help Boards ensure cyber risk is managed effectively.

1. Integrating cyber security risk into organisational risk

Cyber security risk management should be integrated within the overall approach to risk management. This integration ensures that cyber threats are addressed in the context of wider organisational risks, helping to protect both immediate and long-term business objectives.

2. Define and communicate risk appetite

The Board is accountable for determining the organisation's cyber security risk appetite and overall risk tolerance. They should encourage effective communication of the risk appetite across the organisation through strategic questioning, ensuring alignment and enabling effective risk management.

3. Align cyber security with business objectives

The Board must seek assurance that business objectives and the potential impact of a cyber attack on the organisation have been considered in strategy discussions. This ensures that the protection of critical assets aligns with business priorities, strengthening the organisation's overall resilience against cyber threats.

4. Strengthen supply chain cyber resilience

The Board should ensure that risk assessments of the supply chain are guided by the organisation's cyber security strategy. While industry-standard practices, such as NCSC's supply chain guidance, offer a useful framework, each organisation should tailor its approach to its specific risks. This ensures a proactive approach to securing the supply chain that supports the organisations overall resilience.

5. Conduct regular risk reviews

Cyber security risk reviews should be conducted regularly, ideally at the same frequency as other organisational risk reviews. However, given how quickly cyber threats and technologies are advancing, reviews should also occur whenever internal or external changes warrant, such as new projects, regulatory shifts, or emerging threats. The trigger for these reviews should be outlined in the organisation's cyber security strategy, ensuring timely and relevant assessments.

Remember

By embracing these five practices, Boards can take an active, informed role in cyber governance, ensuring that organisational efforts to manage cyber risks are robust, aligned, and effective.

Question for the Board

Do we have a process that ensures cyber risk is integrated with business risk?
When assessing key risks, Boards should ask, "Have we considered cyber security risks in our decisions?" For instance, a company bidding for a contract faces pricing, quality, and competitor risks but also cyber risks, such as the theft or exposure of sensitive bid information.

National Cyber Security Centre