KEY TAKEAWAYS

Strategy

A cyber strategy guides the choices an organisation makes about risk mitigation, the technology capabilities and people-focused initiatives they put in place, as well as allocation of resources and investment. It is a key enabler of achieving cyber resilience and supports long-term success.

1. Embed cyber strategy within the organisational strategy

Boards play a critical role in ensuring that a cyber strategy is developed and embedded within the organisational strategy. This alignment ensures cyber security efforts support the overall business goals and objectives.

2. Elements of a robust cyber strategy

A cyber strategy should reflect the distinct needs, risks, and structure of the organisation. Each organisation should have the flexibility to tailor its approach. Key strategic elements to guide Executive-level planning include:

- Setting the strategic approach for assessing and identifying potential threats and vulnerabilities
- Defining priorities and principles for mitigating risks
- Outlining objectives for incident response and recovery
- Establishing governance frameworks that provide oversight and accountability for cyber security efforts
- Embedding a commitment to security awareness as a strategic priority across the organisation

3. Investing in cyber strategy

Allocating appropriate resources and investment is essential to successfully managing cyber security threats and associated business risks. By investing in the right technologies, tools, and expertise, organisations can enhance their ability to enhance their cyber resilience.

4. Monitoring cyber strategy

A cyber strategy should be reviewed regularly and whenever significant changes occur in the internal or external environment, such as shifts in technology, organisational priorities, strategic goals, or regulations. This ensures the strategy stays relevant and aligned with the organisation’s objectives.

Remember

With the Board’s oversight and commitment, a cyber strategy drives resilience, adapts to threats, and ensures long-term success.

Question for the Board

Do all employees know where accountability and responsibility resides? *Accountability and responsibility for cyber security should be clearly defined. If leadership struggle to identify where responsibility and accountability sits, reporting structures and communication need improvement.*