GOVERNANCE STEP ONE:

BUILDING A CULTURE OF CYBER RESILIENCE

NATIONAL CYBER SECURITY CENTRE
A PART OF THE GCSB

New Zealand Government

Organisations must develop a culture of cyber resilience. Everyone in the organisation should feel supported to make decisions that protect the confidentiality, integrity and availability of information assets and systems. Awareness of and accountability for cyber resilience should be seen throughout the organisation as an important and complementary part of that organisation's mission.

Establishing an organisation's cyber security culture occurs from the top down. The board must demonstrate a commitment to cyber resilience. This can be communicated and reinforced through strategy, policy and standards.

Cyber Resilient Culture

The board has a duty to identify the organisation’s key assets and provide strategic direction to the leadership team. If information technology is a key asset or contributes to the organisation’s strategic direction, then cyber security should be on the board’s agenda.

Ensuring the board’s awareness of cyber security is a critical first step towards building a cyber resilient culture. Cyber security is a complex and often technical subject. However, for the board, expressing cyber security in a more familiar business language is advantageous.

Health and safety provides a useful comparison with cyber security for boards. The board does not need to grapple with medical diagnoses to understand the business impact of a health and safety incident. Boards are also interested in more than just incidents; evaluating near-misses, where an organisation gets close to experiencing a security breach, can provide useful insights into current levels of cyber resilience.

A supportive culture in which emerging risks, near-misses, and actual incidents are reported and addressed is fundamental to cyber resilience. Boards should demand strong situational awareness with which to support timely decision-making. It should not require a major incident to make the board aware of the cyber security resilience of the organisation.

> “Setting an organisation’s cyber security culture is something that happens from the top down and should recognise an organisation’s existing culture.”

Cyber Security Strategy

A strategy is a foundational document because it aligns cyber security with wider organisational objectives. Business and cyber security outcomes depend on the same people, processes and technology — a strategy addresses this relationship for the organisation's specific context.

Part of that context is the organisation's operating environment. External factors will differ in their influence on the organisation's approach to cyber security. Some organisations might have higher regulatory or compliance considerations, while others will have a more diverse threat landscape. Internal factors also differ, from insider threats to key business partners or third-party dependencies.

> "A strategy should allow for and recognise key business objectives and provide guidance on how they can be achieved securely."

Policies & Standards

Policies and standards provide further guidance to an organisation on establishing a culture of cyber resilience. Write these policies and standards in a tone that represents the current culture of the business; they should lead the organisation on a pathway to cyber resilience, rather than trying to transform it by writ.

Policies and standards need not be long or overly complicated; it is most important for them to be clear. This usually starts with creating a cyber security policy but can be extended to include policies addressing issues such as privacy, data governance, and acceptable usage. These policies will have a wide audience, so it should be easy to interpret and implement them.

Where policies do not provide specific detail, they can be further defined by standards. Standards are also mandatory, but may change more often than the policies they support to keep pace with technology.

There are many frameworks available to guide the creation of policies and standards, including the New Zealand Information Security Manual (NZISM), ISO27001, or Center for Internet Security (CIS) Critical Security Controls.

The New Zealand Information Security Manual (NZISM) and Protective Security Requirements (PSR) contain standards and guidance related to governance. While every effort has been made to align *Charting Your Course* with the PSR and NZISM, where difference is found, they remain the authoritative standard for mandated agencies.