NORTHWAVE
CYBER SECURITY

Management Memo

Journey with the CISO

A Mountain Climb to Cyber Security Resilience

Inge van der Beijl, Northwave Director Innovation

14th November 2024

Today's cyber security is a complex journey, comparable to climbing Mount Everest. Organisations must navigate a threat landscape that is constantly changing, new security regulations, and their own stages of maturity to effectively protect business assets and develop a culture that prioritises security. The modern Chief Information Security Officer (CISO) plays a pivotal role, guiding the organisation's progress and adapting security strategies to meet evolving challenges. As a result, the scope of this role is quickly expanding, expectations are rising, and the outlook for this profession is uncertain.

At Northwave, we aim to support a future-proof CISO role and foster a transparent working environment where CISOs can thrive. Based on our quantitative and qualitative research on the changing role of the CISO, we have developed a detailed framework of the CISO journey. Our metaphorical approach, which we call Mount Securest, is segmented into three primary destinations: Base Camp, High Camp, and the Summit. Each of these destinations represents different cyber security focuses and organisational goals, which influence expectations for the CISO role and the type of CISO best suited for the organisation.

Base Camp: Foundational Security

- **Characteristics:** Organisations focused on the foundational layer of security that is necessary for incident prevention and compliance. Typically operating in industries such as manufacturing and logistics.
- **Role of CISO:** The "Foundational CISO" sets up initial security frameworks, policies, and governance. They usually have a technical background and work in close collaboration with both the CIO and CFO.
- **Challenges:** Ensuring business continuity and externally sourced threats such as ransomware and intellectual property theft.

High Camp: Security-Conscious Culture

- **Characteristics:** Organisations that value a security-first mindset throughout the organisation, often in healthcare, housing corporations, and governmental agencies.
- **Role of CISO:** The "Transformational CISO" seeks to embed security within the organisation's culture, driving awareness and upholding the concept of risk management. Beyond IT, they influence business processes, decision- making, and behavioural changes.
- **Challenges:** Supply chain attacks, building up a secure cultural attitude, and ongoing development of security maturity.

The Summit: Strategic Security Integration

- **Characteristics:** For the primarily digital organisations, critical sectors, and tech companies that must protect intellectual property, security is inherent in the corporate strategy and an enabler of business innovation with proactive risk management. Also, within corporate environments that use security as a differentiating factor to build trust in branding and service delivery, such as insurers and other organisations where reliability is a core value.
- **Role of CISO:** The "Strategic CISO" aligns security to long-term business strategy; optimises processes and team collaboration. They are the visionaries and strategic leaders, with exceptional business acumen and communication skills.
- **Challenges:** Effectively balancing business goals with technology and human risks while sustaining a high level of security maturity.

Key Enablers and Challenges

Our research highlights the critical need for CISOs to have direct access to the board, enabling them to escalate issues and provide strategic advice. Early involvement in decision-making is essential, yet many CISOs are often relegated to reactive roles. Significant differences in team structures and resources impact their effectiveness, with some CISOs leading large teams and others working alone. Key challenges include increasing digitalisation, knowledge gaps between CISOs and the rest of the organisation, and balancing security measures across technology, organisational structure, and people. These factors make the CISO role highly demanding and stressful, with many CISOs experiencing work overload, lack of control, inadequate support, and poor work-life balance.

To address these challenges, the executive board should facilitate solutions that will support the CISO–enabling them to be effective in their role, thereby enhancing the organisation's resilience in cyber security and keeping the mission of aligning security with long-term business goals.

- **Ensure Direct Board Access:** We recommend an independent reporting line to the board for the CISO, allowing the CISO to escalate issues in a timely manner and provide strategic advice directly to decision-makers.
- **Early Involvement:** Let the CISO be involved in early strategic planning. This proactive approach will help to move beyond merely reactive firefighting and give a voice to the CISO in shaping the organisation's strategic objectives.
- **Resource Allocation and Team Structure:** Grant the CISO responsibility and authority to form and structure their own team, with the necessary resources to attract and retain qualified talent in cyber security. This will set up the CISO for success and improve the organisation's security posture.
- **Foster a Security-Conscious Culture:** Promote a security-first mindset across all departments, using continuous education and awareness programmes to bridge the knowledge gap between the CISO and the rest of the organisation. A strong culture of information security will distribute the responsibility of cyber security across the organisation.
- **Balance security measures:** Strive for a balanced approach to security that integrates technology, organisational structure, and people. This holistic strategy will address the rapid developments in the threat landscape and the evolving needs of the organisation.

Each organisation's path to cyber security maturity is unique, and what that requires from an organisation is a different kind of CISO and support. That means every organisation needs to define what the final destination will be and whether the resources and leadership are in place to make that journey in cyber security.