How cyber-security champions drive business agility

January 2025

Theresa Esch, Stefanie Graf

As cyber-security threats become more sophisticated and pervasive, organisations face increasing pressure to secure their digital assets, data and operations. However, many departments within different organisations view cyber security as a bottleneck that delays projects and disrupts business goals. Cyber-security measures are often seen as obstacles, and communication gaps between security experts and operational teams further prevent integration with daily operations.

Cyber security is crucial due to risks such as data breaches, financial losses, reputational damage and regulatory penalties. These threats can severely impact an organisation's ability to operate effectively and maintain customer trust.

Currently, chief information security officers (CISOs) are responsible for any cyber-security incidents, even those originating outside of departments traditionally associated with cyber security. However, to effectively mitigate these risks, a broader, organisation-wide approach to cyber security is essential.

Integrating cyber security into the business

The most effective way to promote cyber-security adoption throughout all departments of an organisation is by empowering cyber-security champions – individuals within each team who act as advocates for cyber security and help drive awareness. Embedding cyber security into the core of an organisation fosters a culture of cyber-security awareness at all levels. Cyber-security champions serve as key players in fostering a secure-by-design (SBD) culture where cyber security is embedded into every process, and where every department actively contributes to a more robust cyber-security ecosystem, enhancing both resilience and efficiency.

For CISOs, this approach is transformative, ensuring that cyber security becomes a fundamental organisational priority. By distributing security responsibilities across all departments, organisations can better mitigate risks and strengthen governance, creating a resilient and sustainable cyber-security framework.

The role of cyber-security champions

Cyber-security champions help bridge the gap between technical and business teams, ensuring that cyber-security goes beyond technical solutions and becomes a shared responsibility, not just an IT concern. Cyber-security champions are integral to embedding cyber security into the daily operations of their teams, ensuring that policies, frameworks and best practices are not only understood but adopted across the organisation.

Cyber-security champions are the primary point of contact for cyber security within their departments. While they may not be cyber-security experts, they understand basic cyber-security principles and can communicate these effectively to their colleagues. Typically placed in departments with higher security risks – such as IT, HR, sales, procurement and facilities management – cyber-security champions help embed a security-first mindset across the organisation, ensuring that cyber security is treated as a shared responsibility rather than solely an IT issue.

How to introduce cyber-security champions across departments

The cyber-security champion model can be adapted to the unique needs of different organisations, recognising that there is no one-size-fits-all solution. This flexibility allows cyber-security champions to operate at various levels within the organisation and focus on different aspects of cyber security, ensuring that the model aligns with the specific risks and operational demands of each department. For example:

- **Departmental embedding**. Cyber-security champions can be placed in any department, depending on specific security risks. For example, an IT champion might focus on network and data security, while a procurement champion might address supplier risks, and a facilities management champion may focus on physical security.

- **Dual-role flexibility.** Many cyber-security champions can retain their primary roles while dedicating time to cyber-security-related tasks. This dual role ensures that cyber-security is integrated into daily operations without requiring a full-time commitment.

This flexibility ensures that cyber-security champions can contribute to the broader cyber-security strategy while still being closely aligned with the needs of their respective departments, which decentralises security responsibility and ensures that each department's specific cyber-security risks are addressed by someone who understands both the technical and operational aspects.

Practical steps to build a network of cyber-security champions

The success of any cyber-security initiative relies on fostering a culture of shared responsibility, where cyber security is integrated into the fabric of the organisation. By cultivating a community of cyber-security champions, CISOs can ensure that cyber-security practices are consistently communicated, reinforced and embraced at every level.

- **Community-driven engagement.** Effective cyber-security champion programmes thrive when they grow organically, driven by the enthusiasm of participants. While leadership support is crucial, the best programmes empower champions to take ownership of their roles. This approach ensures broader buy-in and sustained momentum across the organisation.

- **Facilitating knowledge sharing to address risks**. By promoting peer learning and collaborative problem-solving, cyber-security champions can identify and address cyber-security challenges more effectively, contributing to a more resilient organisation. In addition, data-driven insights and structured reporting ensure that

champions have access to the information they need to make informed decisions and address risks effectively. For the CISO, these interactions create a cross-functional network of champions who help enforce policies and address risks across departments.

- **Collaboration to build resilience**. Cyber-security risks are rarely confined to a single department. Bringing together champions from various teams and business units to collaborate, ensures that cyber security is addressed comprehensively. Champions bring diverse perspectives, enabling the organisation to identify and mitigate risks across all processes, roles and responsibilities. This cross-functional approach strengthens the organisation's overall cyber-security posture to build resilience.

- **Ongoing support and development**. A successful cyber-security champion programme requires continuous learning and support to keep champions engaged and ensure they remain well-prepared to drive cyber-security initiatives across the organisation. For CISOs, providing cyber-security champions with the right tools and knowledge helps build operational resilience and ensures that cyber security is actively managed throughout the organisation.

A model that embeds cyber security throughout the organisation

Cyber-security champions offer many benefits, including improved cyber-security awareness, increased efficiency, reduced risk and the creation of a sustainable security culture. Decentralising cyber-security responsibilities means that companies ensure cyber security is woven into everyday operations. This proactive approach prevents project delays and reduces the likelihood of missed vulnerabilities.

Ultimately, cyber-security champions foster a shared sense of responsibility, creating a cyber-security culture that extends across the entire organisation. This decentralised responsibility model is particularly critical for CISOs, as it ensures that cyber security is not only an IT concern but a broader organisational imperative. This approach helps to mitigate risk and improve governance by distributing responsibility for cyber security across all departments.