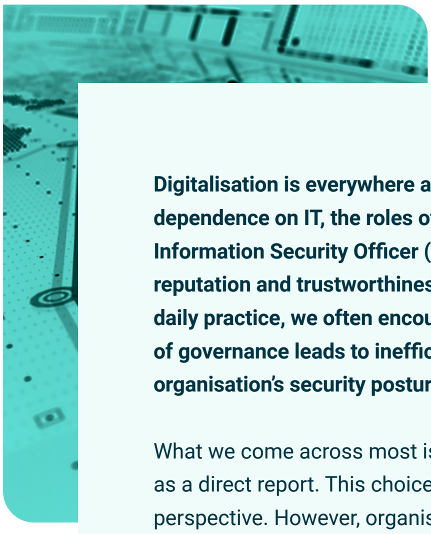
Empowering Good Governance of Cyber Security



Digitalisation is everywhere and so are cyber security incidents. With the increasing dependence on IT, the roles of the Chief Information Officer (CIO) and the Chief Information Security Officer (CISO) are crucial in safeguarding an organisation's reputation and trustworthiness, while ensuring the integrity of its IT infrastructure. In our daily practice, we often encounter the conflation of these two crucial roles. This choice of governance leads to inefficiencies, conflicts of interest and vulnerabilities in the organisation's security posture.

What we come across most is the CIO also taking the role of the CISO or having the CISO as a direct report. This choice might make sense for smaller businesses from a cost perspective. However, organisations that are midsize or larger organisations that often need to adhere to regulations like NIS2, DORA, GDPR and CSA, should seriously consider to structurally ensure the independence of these two roles.

The upcoming NIS2 and other European regulations explicitly define the cyber security responsibilities of the board, increasing the personal accountability of both executive and non-executive board members. This warrants their more precise attention on how to organise continuous control over this topic.

This piece outlines the seven most important arguments for why the roles of CIO and CISO should be separated to empower good cyber security.

1. Conflict of Interest

The primary responsibility of a CIO is to oversee the IT department, ensuring that the organisation's technology infrastructure supports business objectives efficiently and cost-effectively. This often involves implementing innovative technologies, optimising operations, and managing budgets. On the other hand, the CISO's focus is on protecting the organisation's information assets in line with business objectives, which sometimes necessitates stringent security measures that may conflict with the CIO's goals of efficiency, availability and cost-effectiveness.

By separating these roles, organisations can ensure that security and resilience are business decisions, not compromised for the sake of operational efficiency or budget constraints.

2. Specialised Expertise

Cyber security is a highly specialised field that requires deep knowledge of threat intelligence, regulatory requirements, human behaviour and advanced security technologies. While CIOs possess broad expertise in IT management, they may not have the in-depth security knowledge needed to effectively mitigate complex cyber threats.

A dedicated CISO, with specialised training and experience in cyber security, is better equipped to understand and address the nuances of emerging threats, ensuring robust protection of the organisation's information assets.

3. Focus and Accountability

Combining the CIO and CISO roles can dilute focus and accountability, as one individual is tasked with overseeing both IT operations and security. This dual responsibility can lead to divided attention, where neither function receives the full dedication it requires.

Separating these roles allows each leader to concentrate on their specific mandate. The CIO can focus on optimising IT performance and aligning technology with business strategy, while the CISO can concentrate solely on managing the security posture, developing and implementing comprehensive security measures.

4. Enhanced Risk Management

IT risks are of a limited scope compared to the business risks regarding cyber security. We often see that risks and corresponding measures are defined within IT, but the IT team does not have the capabilities to act upon it since ownership should be in the business.

Effective risk management is crucial for maintaining a strong security posture. A dedicated CISO can independently assess security risks without the pressure to align with the CIO's operational objectives. This independence allows for a more objective evaluation of risks and the implementation of appropriate mitigation strategies. Having a separate CISO ensures that security risks are managed proactively and rigorously, without being overshadowed by other IT priorities.

5. Clearer Communication and Reporting Structures

Incorporating distinct roles for the CIO and CISO establishes clearer communication and reporting structures within the organisation. The CISO can report directly to the CEO, the board of directors, or a risk management committee, ensuring that cyber security receives the attention and oversight it deserves at the highest levels of the organisation. This direct line of communication facilitates better-informed decision-making and reinforces the importance of security as a strategic priority.

6. Improved Incident Response

In the event of a cyber security incident, a dedicated CISO can lead the response efforts with a focused and coordinated approach. The separation of roles ensures that the CISO is not burdened with IT operational issues during a crisis, allowing for a swift and effective response to contain and mitigate the impact of the breach. This clear delineation of responsibilities enhances the organisation's ability to manage incidents and recover more efficiently.

7. Strengthened Security Culture

A dedicated CISO can play a pivotal role in cultivating a strong security culture within the organisation. By focusing exclusively on security awareness and training, the CISO can ensure that employees at all levels understand their roles and responsibilities in protecting the organisation's information assets. This emphasis on security culture can lead to better adherence to security policies and practices, reducing the likelihood of human error and enhancing overall security posture.

Enabling Digital Business

In an era where cyber threats are increasingly sophisticated and pervasive, the delineation of CIO and CISO responsibilities is not just a matter of organisational efficiency; it is a critical step towards ensuring the long-term security maturity and cyber resilience of the organisation.

Beyond just separating the roles lies the joint goal of both the CISO and the CIO to enable the business to be in be increasingly digital, innovative, resilient and compliant. Their communication and alignment with the strategy are essential.

This is why we recommend the CIO and CISO to form a joint steering committee to guide the safe digitalisation of the business and lead the company towards making justifiable decisions based on quantified risk in the context of a clear digital strategy.

The Challenge of Building the CISO Role

The separation of the CIO and CISO roles is clearly a strategic move that empowers midsize and larger organisations to establish robust governance frameworks for cyber security. By recognising and institutionalising the unique contributions of both roles, organisations will empower themselves to better safeguard the organisation's reputation and ability to compete and innovate.

Building the CISO capability, however, **can be challenging**. Many organisations already struggle to enable their IT operations due to constraints in the available specialists. Introducing the CISO capability will prove equally challenging. CISOs are highly sought after and having a CISO does not yet ensure the day-to-day operation of the security management role throughout the organisation. It requires a multitude of expertise and a smooth machinery based on frameworks and best practices. Building up this function can be costly as well as risky and time consuming. Safeguarding the continuity of this function can prove to be even more complicated.

Outsourcing

There are service offerings that can aid with this challenge. The three most relevant offerings in the market today are confusingly all often labelled as **"CISO as a Service"**. Let's take a closer look to understand the differences.

- **Subscription to Time.** This service is in fact a consultancy retainer, usually connected to an individual. This 'CISO' is made available to your organisation for a fixed amount of time per month. Service beyond this is not guaranteed, neither are any operational functions that a CISO team should perform. The value this brings is limited to having CISO as an available person, which can prove useful when the operational capacity is otherwise guaranteed.
- **Subscription to Time + Tooling.** There are many Software as a Service platforms promising to deliver administrative support for security management. Most are based on Information Security Management Systems such as ISO 27001. This service offering delivers a combination of such platforms as well as support for using the system properly. This can be valuable as an addition to an already standing CISO team, looking for backend automation.
- **Managed Security Office.** This offering delivers the complete and integrated functions that a mid-size or larger organisation should expect from their CISO team to be in control. It combines the security management platform with functions for incident management, employee awareness programs, activity management, compliance management, and supplier- and third-party due diligence. Offerings can include dedicated resources for key roles such as IT and Business Security Officers and of course the CISO. This can also be combined with resources from the organisation, creating a hybrid service model. This service model offers a quick and complete enablement of the CISO with a supporting team. Northwave is offering this model as a service option to clients.

We believe that the safety of your digital journey will rely on mobilising two independent pairs of eyes to help you navigate through an ever-evolving landscape of threats and regulations, while you execute your digital business strategy.

We are ready and able to assist you with that from a holistic perspective and the ability to guarantee an Intelligent Security Operations that will keep you in control around the clock and around the globe.

Get in contact with us

Currently facing a security incident?

Call day and night: 00800 1744 0000

Contact

E: info@northwave-cybersecurity.com
T: +31 (0) 30 303 1240
W: northwave-cybersecurity.com