White Paper

Whitebridge

Cybergovernance Task Force

June 2024

Risks and impact of the new European Union cybersecurity rules

Understanding the NIS2 Directive:
Enhancing Cybersecurity in the Digital Age.

Introduction

The NIS2 Directive is a significant step in enhancing cybersecurity across the European Union (EU). As society becomes more digitised and cyber threats continue to rise, this directive aims to establish a comprehensive framework to ensure the resilience of critical infrastructure and essential services. This white paper provides an overview of the NIS2 Directive, including its key components, stakeholder implications, and potential challenges and opportunities. It is also a call to action for organisation, their customers and suppliers.

10 Take-away Points for Board Members

01 Unlike the GDPR, the NIS2 is a directive that each European Union member state must implement into their national law. This means **compliance** is necessary **under the national law** of the country where the contract is based.

02 The **NIS2 will go into effect on 1 January 2025**, and the deadline is approaching. All existing contracts should be updated to incorporate the directive, which will apply during the contract duration.

03 Establish a cyber security policy, ensure that your contracts are in place, and verify that your suppliers are also cyber security compliant. **Address these issues in your sourcing contracts** to ensure compliance with the new directive, as both companies and IT suppliers fall under its scope.

04 Under NIS2, **Board Members can be personally liable** if the company's cyber security policy turns out to be inadequate. The organisation may face **a penalty of up to 2% of its global turnover**, which poses a significant risk for any Board

05 **Companies may be held responsible for their own cyber security policy and that of their suppliers.** Therefore, it's important to ensure that contracts with suppliers incorporate sufficient safeguards.

06 NIS2 also imposes obligations on certain IT companies such as data center companies and manufacturers and providers of ICT products and services. This means that **IT companies and sourcing companies may also fall under the scope of NIS2.**

07 Small companies with less than 50 employees are exempt from NIS2. However, **as a company, you can still be held responsible for these small companies** if they are your suppliers.

08 There is a **comprehensive list of companies that fall under NIS2** on the customer side.

09 The **application of NIS2 to companies on the customer side is not clear**, so you will need to determine this yourself. You are required to register, and you will be supervised by a cyber security authority.

10 **Don't delay!** Take action now.

Cybergoverance Task Force White Paper Whitebridge

In-depth analysis of the NIS2 Directive

The ongoing digital transformation of our economy and society has created an exciting new era filled with unprecedented opportunities for innovation and growth. As we embrace these advancements, we must also confront the ever-evolving landscape of cyber threats requiring constant vigilance. These threats can disrupt vital services, compromise sensitive data, and undermine trust in digital technologies. In response to these challenges, the EU has taken decisive steps to address cybersecurity concerns by introducing the NIS2 Directive.

The NIS2 Directive, officially known as the Network and Information Security Directive 2, marks a significant advancement in strengthening cybersecurity measures within the EU. Expanding on the groundwork laid by its predecessor, NIS1, NIS2 aims to enhance the resilience of critical infrastructure and essential services by promoting collaboration among member states, imposing cybersecurity requirements for operators of essential services (OES), and fostering a culture of proactive risk management and incident response. The comprehensive scope of the NIS2 Directive acknowledges the diverse sectors affected by cyber threats. It emphasises the evolving nature of cybersecurity requirements by mandating that companies in scope maintain a consistently high level of security, regardless of their client base.

> **“NIS2 is a serious game changer. As of 1 January 2025, board members can be held personally liable concerning cybersecurity.”**

This broadens the directive's scope to encompass a wider range of sectors, including digital infrastructure, online marketplaces, and cloud computing services.

NIS2 introduces a robust **duty of care**, highlighting the significance of comprehensive risk assessments and security measures in line with identified risks. This approach allows companies to tailor their security measures to specific risks, presenting an opportunity for focused risk management—however, the absence of a uniform standard challenges meeting this legal obligation.

Companies under the NIS2 Directive must promptly **report significant incidents** to the Computer Security Incident Response Team (CSIRT) or the competent authority, including real-time status updates. Moreover, NIS2 empowers national authorities to define the parameters of a "significant incident."

Member states are strongly encouraged to effectively promote **collaboration and information** sharing to address cross-border cybersecurity threats.

The directive requires each member state to assign an authority to oversee compliance and enforce cybersecurity requirements. This ensures **a cohesive and forward-thinking approach to cybersecurity across the EU.**

Implications for Stakeholders

Companies under NIS2:

Companies that operate critical infrastructure must comply with new cybersecurity requirements, invest in strong security measures, and establish effective incident response mechanisms.

Board Members:

NIS2 requires management bodies to approve their company's security measures. This makes officers of Board Members personally accountable for their company's security policy decisions.

Member States:

National authorities are responsible for implementing the directive, coordinating with other member states, and ensuring compliance with cybersecurity standards.

Consumers and Citizens:

Improved cybersecurity measures help safeguard the digital economy and protect individuals' personal data and privacy.

Challenges and Opportunities

- **Challenge:** Implementing the NIS2 Directive may pose challenges for companies due to its complex requirements and varying interpretations across member states. Also, since EU member states may impose higher requirements than those contained in NIS2, companies need to check their approach against all the national requirements that may apply to them.
- **Challenge:** Effective cooperation among member states is crucial for addressing cyber threats that transcend national borders, but it may require overcoming legal, cultural, and operational barriers.
- **Opportunity:** While compliance with the directive may require upfront investments, it also presents an opportunity for companies to strengthen their cybersecurity posture, foster innovation, and build trust with customers and partners.
- **Challenge:** NIS2 provides minimum requirements; this presents companies with a potential risk because national governments are free to impose requirements higher than those of NIS2.

> **NIS2 is one of the many EU Directives and Regulations that will impact companies in the coming years: The Artificial Intelligence Act was adopted in April 2024. It contains penalties up to 75 million Euro or 7 per cent global turnover (whatever is the highest). Companies must seriously prepare themselves and understand the various roles and duties under the AI Act.**

- **Challenge:** NIS2 starts off with a straightforward jurisdictional rule: companies fall under the jurisdiction of the EU member state in which they are established. However, it also provides for a range of exceptions and specifications. These exceptions and specifications expose companies to potential uncertainty that they must address by cooperating with national bodies. Besides territorial jurisdiction, NIS2 allows EU member states to establish multiple bodies to deal with the issues raised under NIS2.

7 Take-away Points for COI's and CISO's

01 **Security by Design** should drive the implementation of practices, rather than just adhering to standards on paper. Adhering to NIS2 will enforce of this.

02 Cybersecurity practices like ISO 27001 are appropriate guidelines. **Still, the practices must be implemented, not just on paper.** While certification may not be required, audits, whether internal or external, should aim to ensure security measures and drive continuous improvement.

> **Cybersecurity has become Chefsache**

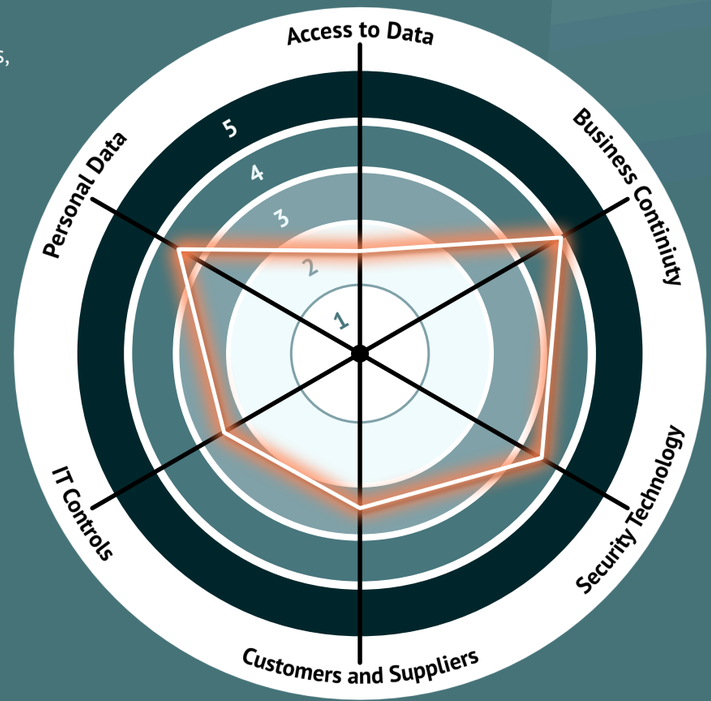
03 **All participants in the ecosystem determine the effectiveness of security measures.** The organization is responsible for its contractors and subcontractors. NIS2 measures must be included in all agreements, and companies must be able to demonstrate NIS2 Compliance.

04 Senior management awareness is important, **but senior management ownership** is even more crucial to establishing effective security measures across the entire company. The CISO is responsible for guiding and overseeing the security measures and their practical implementation.

05 Not only should NIS2 obligations be defined in contracts, but the **consequences of the measures taken or not taken that lead to penalties** should also be stipulated for the contract parties.

06 NIS2 most likely will apply to your IT Suppliers directly. However, as a company, you will need the contracts in place to **ensure enforcement for your company's NIS2 compliance.**

07 A quick assessment should provide insights into the risks and practical measures taken (a 'risk profile radar' as shown below).



References

[1] Directive (EU) 2020/0000 of the European Parliament and of the Council of [date] on measures for a high common level of cybersecurity across the Union, repeating Directive (EU) 2016/1148.

[2] European Commission, "NIS2 Directive - Questions and Answers,".

[3] European Union Agency for Cybersecurity (ENISA), "NIS2 Directive – Overview and Resources,".

Conclusion

The NIS2 Directive is designed to take a proactive approach to cybersecurity, recognising our digital society's changing threat landscape and interconnected nature. It aims to establish clear requirements, promote cooperation, and foster a culture of resilience. NIS2 seeks to strengthen the EU's cybersecurity stance and protect its digital future. However, by setting a standard for security requirements, NIS2 also introduces new challenges for companies and raises unanswered jurisdictional questions.

Contact us

Whitebridge Cybergovernance Task Force is there to assist you with any question regarding NIS2, access your risk profile, and review your contracts.

Whitebridge Advocatuur

mr. drs. Anja E. Dekhuijzen MCJ
Lawyer
+31 6 2951 3067
dekhuijzen@whitebridge.nl

mr. Pavle Bojkovski
Senior Advisor
+31 6 3206 9141
pbojkovski@whitebridge.nl

Whitebridge Consulting

Gerwin Pol
Managing partner
+31 6 5732 4652
gerwin.pol@whitebridge.eu

Paul van Wijngaarden
Partner
+31 6 1292 3750
paul.vanwijngaarden@whitebridge.eu