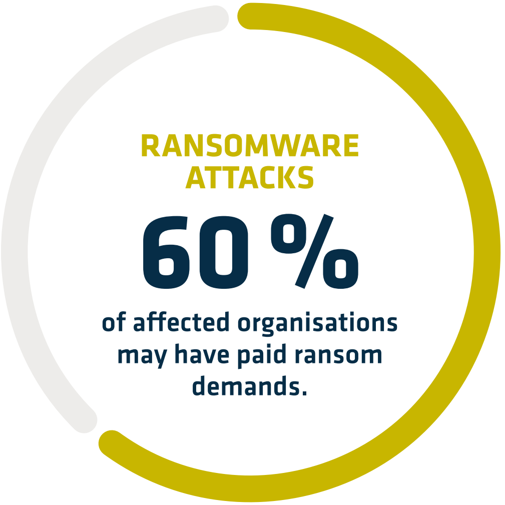
adesso

Insight into NIS2 Directive

INTRODUCTION

In recent years, there has been a significant increase in cyber threats worldwide in recent years. Considering this development, the European Union has been working on the Network and Information Security (NIS2) directive since 2020. This directive aims to enhance the digital resilience of European member states.



RANSOMWARE ATTACKS

60 %

of affected organisations may have paid ransom demands.

www.consilium.europa.eu/en/infographics/cyber-threats-eu/

The NIS2 directive seeks to contribute to greater European harmonization and a higher level of cybersecurity for companies and organizations. NIS2 is the successor to the first NIS directive, also known as the NIB, which was incorporated into the Dutch Network and Information Systems Security Act (Wbni) in 2016.

The global ransomware pandemic painfully highlights the urgency of NIS2. It's no longer a question of if companies will be attacked but when they will be attacked. The consequences of a cyberattack can be disastrous for businesses, including data breaches, financial losses, damage to reputation, and a loss of trust among customers.

How will the NIS2 directive enhance cybersecurity resilience across all European member states? Is it mandatory for your organization to comply with this directive? And what measures will be taken for the enforcement and penalties related to NIS2 violations? After reading this whitepaper, you will have answers to these questions.

"NIS2 will result in better cooperation among the various European member states in the field of cybersecurity, as it will facilitate and streamline information sharing more easily and efficiently."

JAN HEUKER
CEO | adesso Netherlands

2. NIS2 IN A NUTSHELL

The Network and Information Systems (NIS) Directive, initially established in July 2016, aimed to enhance cybersecurity and cyber resilience capabilities across the European Union. Its purpose was to set security measure baselines for digital service providers and operators to mitigate cyberattack risks. However, as cyberattacks evolved in sophistication and frequency over the years and with the widespread adoption of cloud computing, the NIS Directive struggled to adequately cover the intricate landscape of enterprise systems.

MALWARE

In June 2022 alone, adware trojans were downloaded 10 MILLION times.

www.consilium.europa.eu/en/infographics/cyber-threats-eu/

Recognizing the need for a more robust response, the European Union introduced the NIS2 Directive. In contrast to the original NIS Directive, NIS2 imposes stricter requirements and encompasses a broader range of sectors, with a primary focus on ensuring the business continuity of affected entities. Until mid-2024, European member states have to implement the NIS2 directive into their national legislation. According to the directive, a duty of care and reporting obligation must be included, which both public and private organizations within specific sectors are required to adhere to. The overarching goal of the NIS2 Directive is to bolster the cybersecurity strategies of entities and better prepare them against potential cybersecurity incidents, ultimately creating a safer digital environment for all in response to the ever-evolving nature of cyber threats.

THE KEYPOINTS OF NIS2

> Strengthening imposed security requirements.
> Addressing the security of supply chains.
> Enhancing and streamlining reporting obligations.
> Tighter supervision.
> Introducing enforcement requirements with harmonized sanctions across all European member states.

3. WHICH SECTORS AND ORGANIZATIONS FALL UNDER THE NIS2 DIRECTIVE?

The NIS2 directive focuses on sectors already covered by the first NIS directive and several new industries. This means the number of public and private organizations the directive covers is increasing. NIS2 distinguishes between essential sectors, with the main difference being monitoring and compliance with the rules. The organizations covered by the second NIS directive include:

VITAL SECTORS (ESSENTIAL)

- Energy
- Transport
- Banking
- Healthcare
- Drinking Water
- Digital Infrastructure
- Government Services
- Wastewater
- Aerospace
- Financial Market Infrastructure
- ICT Service Providers

IMPORTANT SECTORS

- Digital Providers
- Post/Courier Services
- Waste Management
- Food Industry
- Chemicals
- Research
- Manufacturing

3. WHICH SECTORS AND ORGANIZATIONS FALL UNDER THE NIS2 DIRECTIVE?

ESSENTIAL ENTITIES

An organization is large based on the following criteria:

at least 250 employees

an annual turnover of more than € 50 million and

a balance sheet total of more than € 43 million.

IMPORTANT ENTITIES

An organization is medium-sized based on the following criteria:

at least 50 employees

an annual turnover and balance sheet total of more than € 10 million.

THE DIFFERENCE BETWEEN ESSENTIAL AND IMPORTANT:

Organizations can be classified as 'essential' or 'important,' the most significant difference lies in supervision and regulation compliance. Therefore, the enforcement approach differs between these two categories. For essential organizations operating in vital sectors, supervision will be proactive.

This means that active government monitoring will take place to ensure these organizations comply with legal requirements. However, for essential providers, supervision occurs retrospectively, for example, when an incident occurs. These organizations can also face consequences if it is found that they have not acted correctly and taken the necessary steps.

> *"Essential entities have a greater impact on society in case of failure than important entities. Essential entities are subject to more intensive compliance oversight both proactively and retrospectively. Important entities, on the other hand, only undergo retrospective oversight, typically in cases of non-compliance indications or after an incident."*

JAN HEUKER
CEO | adesso Netherlands

4. WHAT ORGANIZATIONS NEED TO COMPLY WITH

All organizations falling under the NIS2 directive are required to adhere to their duty of care, which includes a list of minimum required measures. Some examples of these measures are:

> Risk assessment: Ensuring that an organization pays sufficient attention to the security of information systems.

> Crisis management and operational continuity in a significant cyber incident.

> Ensuring the security of the supply chain and network and information systems.

> The use of cryptography and encryption.

> Having policies and procedures in place to assess the effectiveness of risk management measures.

Furthermore, NIS2 legislation mandates reporting requirements for all organizations covered by this regulation. This means that organizations are obligated to report incidents within 24 hours of becoming aware of them. Within one month of the report, a more comprehensive report must be submitted. An important change is that the entire management of both vital and essential organizations is jointly liable if the organization is affected by ransomware and it is found that insufficient preventive measures were taken.

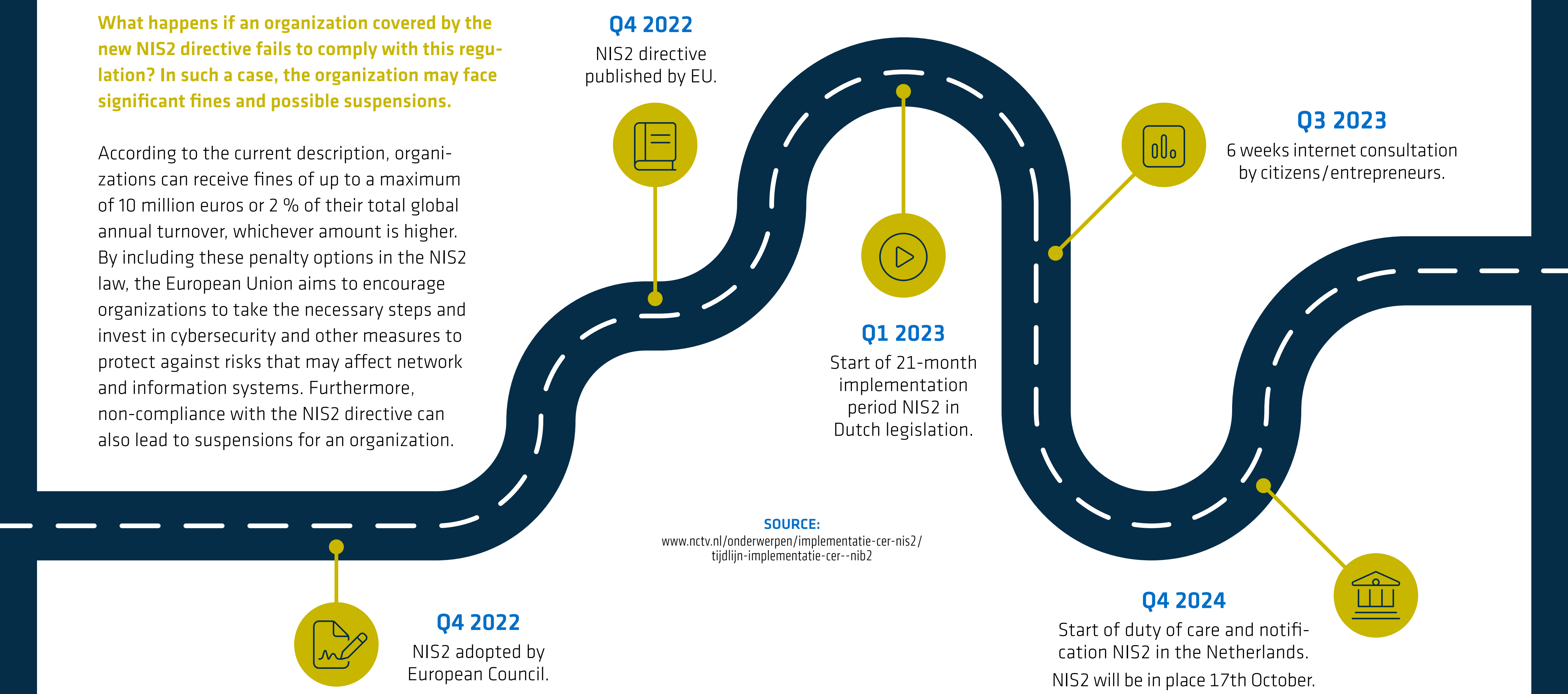
"The fact that the entire management is jointly liable underscores the importance and urgency of complying with the requirements of NIS2."

JAN HEUKER
CEO | adesso Netherlands

5. PENALTIES AND SUSPENSIONS

What happens if an organization covered by the new NIS2 directive fails to comply with this regulation? In such a case, the organization may face significant fines and possible suspensions.

According to the current description, organizations can receive fines of up to a maximum of 10 million euros or 2 % of their total global annual turnover, whichever amount is higher. By including these penalty options in the NIS2 law, the European Union aims to encourage organizations to take the necessary steps and invest in cybersecurity and other measures to protect against risks that may affect network and information systems. Furthermore, non-compliance with the NIS2 directive can also lead to suspensions for an organization.



Q4 2022
NIS2 adopted by European Council.

Q4 2022
NIS2 directive published by EU.

Q1 2023
Start of 21-month implementation period NIS2 in Dutch legislation.

Q3 2023
6 weeks internet consultation by citizens/entrepreneurs.

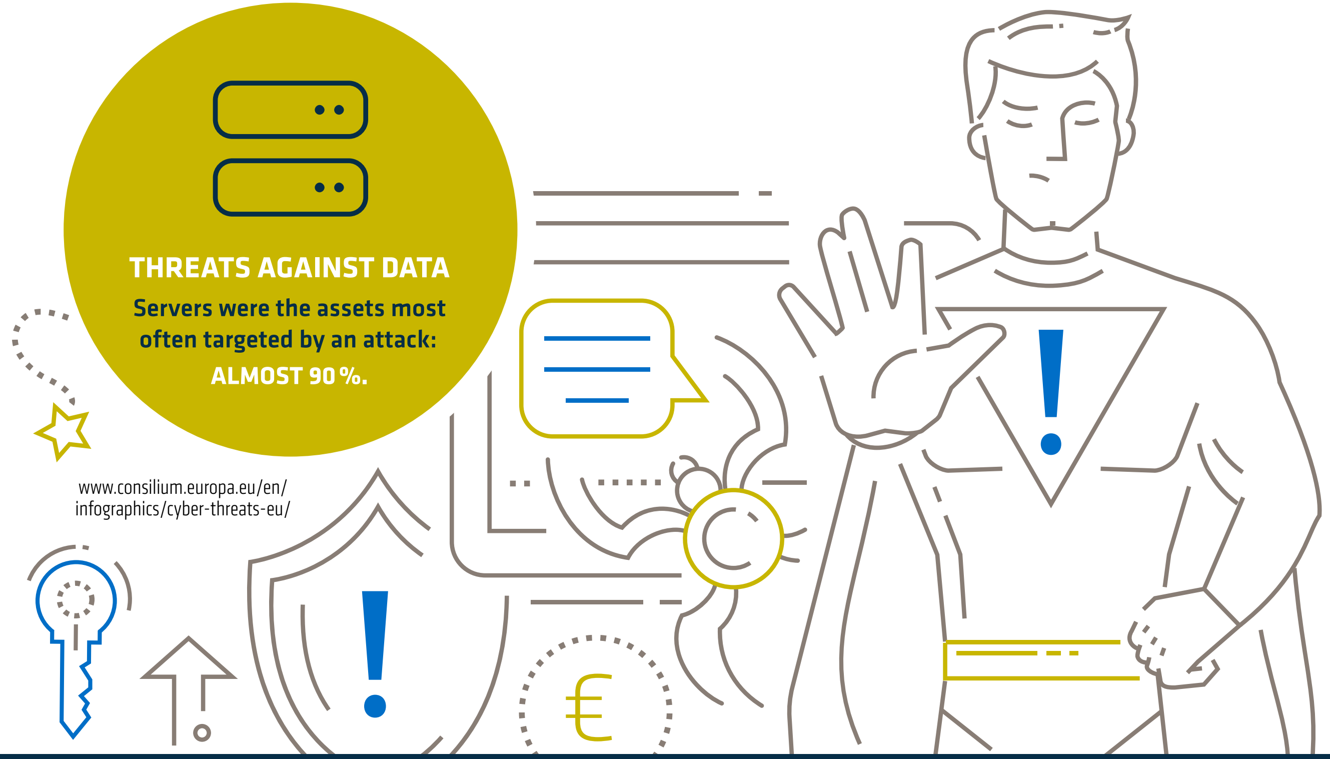
Q4 2024
Start of duty of care and notification NIS2 in the Netherlands.

NIS2 will be in place 17th October.

SOURCE:
www.nctv.nl/onderwerpen/implementatie-cer-nis2/tijdlijn-implementatie-cer--nib2

6. WHAT CAN ORGANIZATIONS DO IN ADVANCE TO PREPARE?

While awaiting national legislation, organizations can proactively prepare for their duty of care by taking steps to enhance the security and resilience of their processes and services. For instance, on the websites of the National Cyber Security Center (NCSC) and the Digital Trust Center, various measures are outlined that organizations can implement to better defend against the risks and damages caused by cyberattacks. Some examples include:



THREATS AGAINST DATA

Servers were the assets most often targeted by an attack: ALMOST 90 %.

www.consilium.europa.eu/en/infographics/cyber-threats-eu/

- Mapping the used network and information systems.
- Identifying and analyzing risks.
- Developing business continuity plans and crisis management protocols and organizing incident response.
- Identifying alternative supply chains.
- Raising staff awareness of risks and necessary measures.
- Mapping their own assets, including their network and information systems.

It's also advisable to allocate the budget and resources necessary to comply with the guidelines.

7. ADESSO AND NIS2: HOW WE SUPPORT BUSINESSES

Discover how adesso can assist your business in achieving and maintaining compliance with NIS2 regulations, both now and in the future. As a strategic partner, we specialize in helping organizations meet their NIS2 compliance requirements. Our comprehensive services range from consulting to an automated NIS2 readiness assessment, streamlining your journey toward NIS2 compliance.

Our team provides the expertise necessary to navigate the intricacies of NIS2, complemented by a state-of-the-art assessment tool that ensures your IT environment is fully prepared to meet all NIS2 requirements.

Partner with adesso for a seamless path to NIS2 compliance.

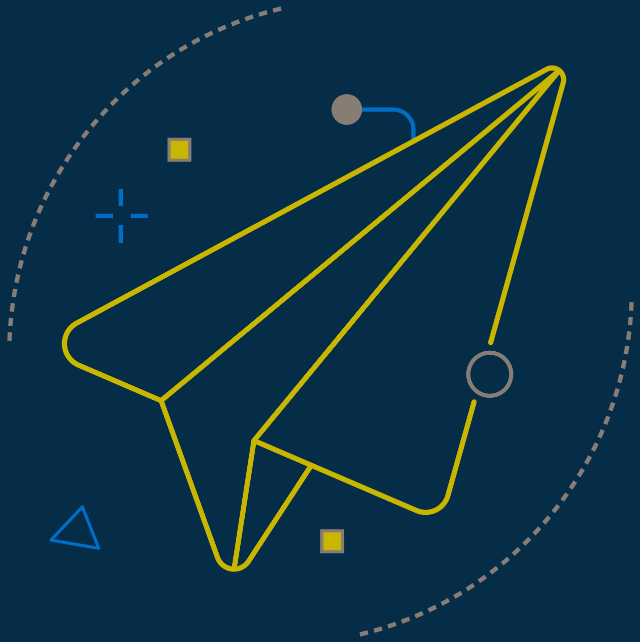
https://www.adesso.nl/NIS2readiness

To learn more, feel free to contact us without obligation:

PIETER KUIJER
Business Manager
adesso NL

✉ Pieter.Kuijer@adesso.nl
☎ +31 6 2741871
in linkedin.com/in/pieterkuijer
🌐 www.adesso.nl

adesso



Any questions?

info@adesso.nl | www.adesso.nl

adesso Netherlands

Zoomstede 21 A
3431 HK Nieuwegein

✉ info@adesso.nl
www.adesso.nl
www.linkedin.com/company/adesso-netherlands/
www.instagram.com/adesso_nl/
www.facebook.com/adessoNL/

DISCLAIMER

This white paper is for informational purposes only and does not constitute legal advice. Entities should consult legal and cybersecurity professionals for comprehensive guidance on NIS2 compliance.

SOURCES

www.nctv.nl/onderwerpen/implementatie-cer-nis2/critical-entities-resilience-directive-cer
www.nctv.nl/onderwerpen/implementatie-cer-nis2/network-and-information-security-directive-nis2
www.nctv.nl/onderwerpen/implementatie-cer-nis2/tijdlijn-implementatie-cer--nib2
www.kvk.nl/advies-en-informatie/veiligzakendoen/cybersecurity/europese-cyberwetten-dit-gaan-ze-voor-je-bedrijf-betekenen/