NOZOMI NETWORKS

EXECUTIVE SUMMARY

Driving cyber resilience: the impact of the NIS2 Directive

An introduction to NIS2

Updates to the latest iteration of the NIS2 Directive to coordinate cybersecurity across the European Union specify new terms and mandates to be developed by Member States but implemented and validated by companies and organisations. The guidance tasks leaders with developing cybersecurity considerations and requirements for entities that serve a large part of the population and are considered vital to the economy, based on the scope and scale of services provided and the size of their operations.

While the original Directive came into effect in May 2018, EU Member States are further required to adopt provisions included in the latest update to the Directive by October 2024. To do so they must provide associated plans for how they intend to comply. Updates to the Directive expand its scope to include new critical sectors, and additional considerations for determining "essential" vs. "important" entities.

Fines for non-compliance could amount to **€10 million or 2% of global turnover** for essential entities and **€7 million or 1.4% of global turnover** for important entities.

All entities are subject to seven broad security requirements:

- Risk analysis and information systems security policies
- Incident handling (prevention, detection, and response)
- Business continuity and crisis management
- Supply chain security
- Security in network and information systems
- Policies and procedures for cybersecurity risk management measures
- The use of cryptography and encryption

New legislation and the wider picture

Organisations undoubtedly find it extremely challenging to adapt to new legislation, which can be complex and costly to interpret and maintain. It is equally challenging for legislators to keep up with an increasingly multifaceted cybersecurity landscape to protect the economy and national security. Compliance, however, is a standard way to encourage security enhancements across the board. Mandates will become crucial to enforce new legislation as the EU has the power to define reporting parameters and impose large fines on those who do not conform to the directive.

Organisations have never been more technology dependent, with large digital footprints adding to their potential attack surface. Threat actors strategies are evolving, and seem to vary between 'living off the land' tactics and tailored attacks on specific targets. Criminal groups are increasingly targeting organisational systems and networks (e.g., operational technology (OT), and Internet of things (IoT) that IT security professionals find themselves responsible for. NIS2 is in direct response to the growing threat landscape; at the heart of the new legislation is that organisations within critical infrastructure sectors must improve their resilience, detection, and incident response capabilities.

Through interviews with 300 IT security decision makers (DMs) in large organisations (with 500+ employees) across Europe, security leaders were asked questions about the responsibility and strategy for securing systems and assets beyond their IT and enterprise networks. This executive summary analyses the current state of organisations within 'critical infrastructure' industries and the road ahead for implementing the NIS2 directive.

OT / IoT cybersecurity responsibility does not completely fall on the CISO

According to IT leaders surveyed, responsibility for securing operational technology (OT) and IoT devices and networks is shared between both internal stakeholders and external third parties.

While just over a third of organisations give ultimate responsibility to the CISO (35%), many others rely on the IT department as a whole (24%) and/or operational technology (18%), amongst others.

The CISO has greater importance in Sweden (44%), France (43%) and the Netherlands (40%) than in Germany (21%). Likewise for those organisations in energy (52%) and financial services (43%) than transport (18%).

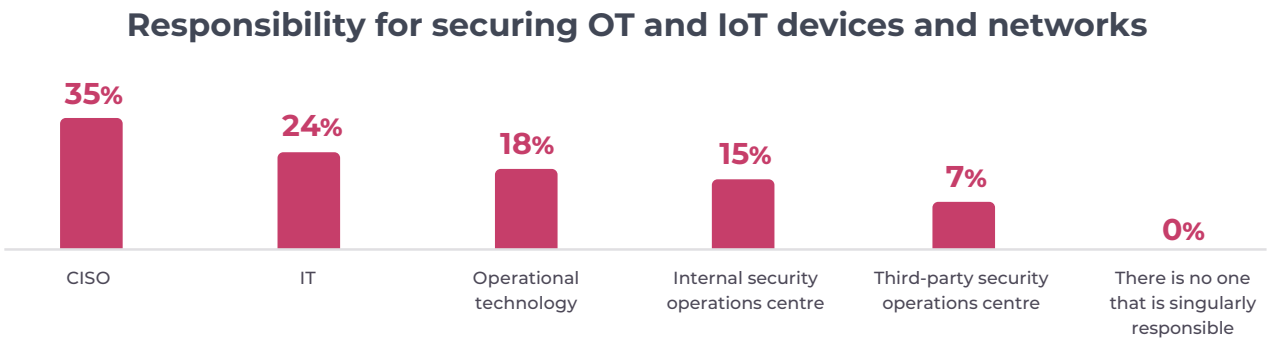

Figure 1. Who is responsible for securing operational technology and IoT devices and networks in your organisation? [300], not showing all answer options

	CISO
Sweden [50]	44%
France [100]	43%
Netherlands [50]	40%
Germany [100]	21%
Energy, oil/gas, utilities and mining and metals [56]	52%
Financial services (excluding insurance) [56]	43%
Telecoms [60]	30%
Manufacturing [34]	29%
Transport [55]	18%

Figure 2. Who is responsible for securing operational technology and IoT devices and networks in your organisation? [Bases size in chart], only showing those who answered "CISO", split by country and key sector

The role of the CISO clearly differs country-to-country and sector-to-sector. There's no hard and fast rule to securing systems and networks. While responsibility is clearly shared among internal stakeholders / departments and external experts, organisations need to ensure they understand their OT and IoT assets. The greater the visibility and the understanding, the better protected they can be. It is essential to perform asset inventory and vulnerability management for OT and IoT assets to perform root cause analysis and review events and activities during incident response.

Organisations look elsewhere for support and guidance

Today, organisations often rely on external providers for both threat intelligence and consultancy during internal or external network breaches.

Malicious activity or external breaches can occur anywhere within an organisation's IT systems, potentially leading to compromise of organisational networks (e.g., OT or IoT).

To address breaches, IT security DMs are most likely to **contact an IT consultant (60%)** or a **cybersecurity solutions provider (56%)**, showing the key role external third parties play when it comes to cybersecurity.

OT systems may be more vulnerable than IT, as many known vulnerabilities persist with less threat intelligence widely available. As a result, incident response within IT is far more secure, and threat modelling is more advanced. OT risk analysis can be limited and outdated, with legacy systems remaining operationally critical to some organisations regardless of existing exploitable vulnerabilities. Mapping known vulnerabilities, securely designed architectures, and potential security controls to prepare for and respond to OT incidents still has some way to go to catch up to comparable remediation in other systems and networks.

Despite the limited availability of threat intelligence, it is still important for many organisations to understand more about the potential threat landscape and risks to OT and IoT. When it comes to cyber threat intelligence related to all assets or networks, IT security decision makers are most likely to use third party cyber threat intelligence providers or feeds (64%) and government disclosures / information sharing (49%).

Overall, it's clear third-party providers are crucial in helping organisations secure all their systems and networks. External expertise, while clearly valuable, can only go so far. It begs the question whether IT security DMs have the in-house tools and knowledge available to them in order to best protect their systems and networks. With NIS2 around the corner, the opportunity is there for organisations to use data available to them and manage their cybersecurity needs more proactively. An understanding of threat groups and their TTPs is crucial for organisations to stay ahead of the game.

Owning the risk management picture

Organisations have blind spots when it comes to cybersecurity, particularly surrounding their critical information systems (CIS).

Only half (50%) follow a schedule when it comes to conducting and updating a risk analysis related to their CIS.

Around a third (34%) do it on an ad hoc basis.

Concerningly, 15% don't currently conduct a risk analysis at all with this figure highest in France (29%) (Sweden 22%) (Germany 4%) (Netherlands 4%).

Conduct and regularly update a risk analysis related to CIS

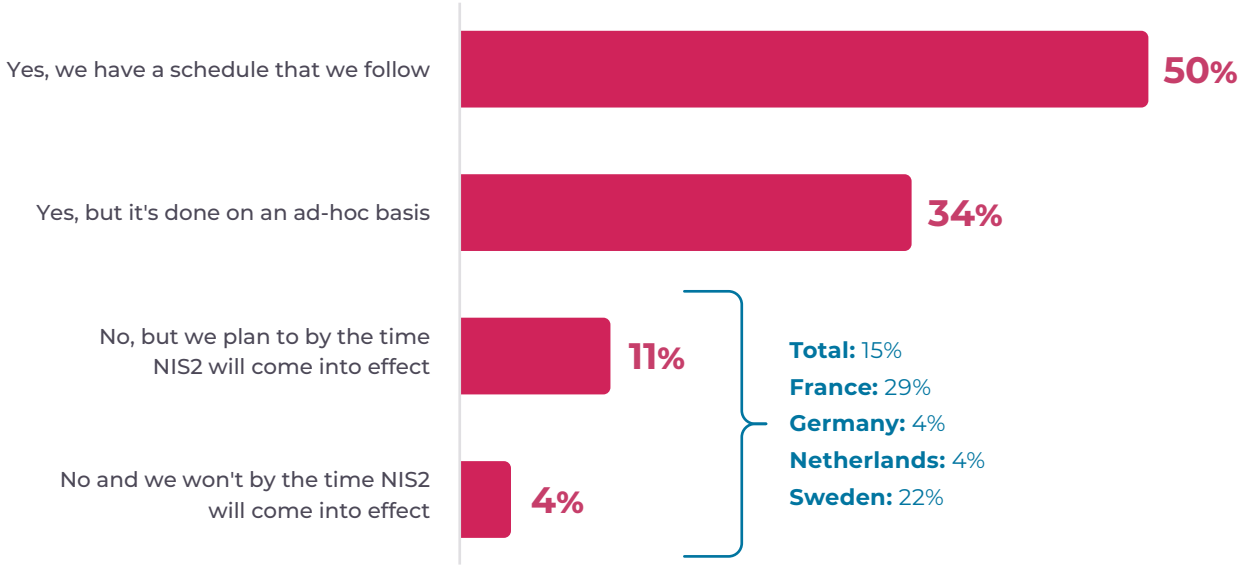

Figure 3. Does your organisation do the following in relation to its critical information systems (CIS)? - Conduct and regularly update a risk analysis related to CIS [300]. Not showing all answer options

Many organisations either only know what threats or risks they face when they're forced into action, or don't know at all. Considering the damage that can be caused through cybersecurity attacks or breaches, there are clear improvements that need to be made to risk management.

Shortcomings in risk analysis are only amalgamated by other weaknesses within cybersecurity management. IT security DMs say their organisation are most lacking in programs associated with asset identification and inventory management (81%), vulnerability mapping / threat hunting (80%) and situational awareness / data analytics (75%)

The results highlight the immediate need for organisations across Europe to revise security and risk management priorities, particularly for operational technology in critical infrastructure. Many report not knowing the risks they face, challenges for safeguarding key assets and lacking insight over who might be targeting them. Above all else, more frequent and in-depth risk analysis will allow organisations to improve their monitoring and detection capabilities.

NIS2 legislation will force change

NIS2 is just around the corner. Organisations will have to cover many bases when it comes to upcoming legislation, with compliance needed across a number of policy areas.

IT security DMs rank information, communication services and technology supply chain consideration as the NIS2 policy area their organisation is most mature in (28%). In contrast, training and education is the policy area (7%) that is least mature.

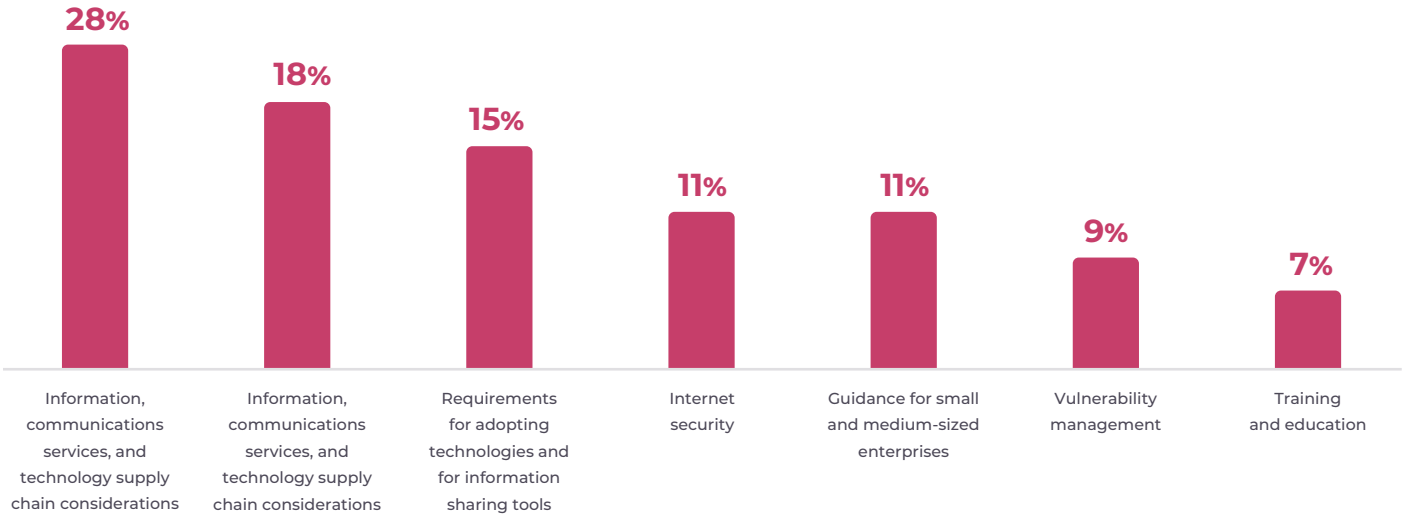

Figure 4. Of the following NIS2 policy strategies, please rank the level of program maturity in your organisation from most to least mature? Responses ranked first [300], not showing all answer options

The contrasting levels of program maturity show where focus needs to be placed. Cybersecurity relies on each employer knowing the risks they face. A lack of training and education could undermine progress made across all areas.

These results raise the question - Are organisations ready for NIS2?

When asked which legislation and/or cybersecurity regulation is most widely used within their organisation, IT security DMs across Europe cite the NIST Framework for Improving Critical Infrastructure Cybersecurity (CSF) (48%) as being top of the list. The original NIS directive is only used most widely by 16% of organisations.

Given the NIST framework was first introduced in 2014, it shows it takes many years for organisations to become compliant with new legislation. With revisions to the NIS CSF due to be released later in 2023, it's likely that the implementation of NIS2 will be a huge challenge, perhaps too much of a challenge, for many. Decision makers will need to carefully consider how their organisation and sector ties into the legislation. In any case, organisations will need all the help they can get.

Conclusion

With every passing year, new cybersecurity legislation comes into force. Each set of guidelines or laws can be a large hurdle for organisations to overcome. At the same time, organisations are constantly having to keep up to date with the latest threats and technology in order to make sure their defences against attacks and potential breaches are robust.

The research demonstrates that the upcoming NIS2 legislation will prove to be a substantial challenge for essential and important organisations representing critical infrastructure industries. Despite competing priorities, a particular focus needs to be put on risk management beyond IT to include operational technology. Indeed, greater visibility of all assets and networks is crucial – not only helping organisations to protect themselves better but ensuring compliance with key legislation.

Methodology

Nozomi Networks commissioned independent technology market research specialist Vanson Bourne to undertake the quantitative research upon which this report is based. A total of 300 IT security decision makers were interviewed in March and April 2023 in Germany, France, Sweden and the Netherlands. The respondents were from organisations within 'critical infrastructure' industries and had at least 500 employees. Interviews were conducted online using a rigorous multi-level screening process to ensure that only suitable candidates were given the opportunity to participate.

The Nozomi Networks Advantage

NIS2 calls out the broad spectrum of resources available to entities to carry out cybersecurity considerations and requirements, noting “the supervisory and enforcement regimes for those two categories of entities should be differentiated to ensure a fair balance between risk-based requirements and obligations on the one hand, and the administrative burden stemming from the supervision of compliance on the other.” Compliance is mandatory, and failure to do so could still result in significant fines.

The key to effective network monitoring and risk management lies in using information to inform an accurate risk view. If network activity is not monitored in real time, the status of assets is largely unknown, and whether or not they have vulnerabilities, these assets cannot be protected without the necessary visibility into their day-to-day functionality. Based on comprehensive AI behaviour-based analytics and signature-based detection engines, the Nozomi platform reliably detects security incidents, policy breaches and process anomalies that could affect the delivery of essential services. Covering the entire industrial control network environment, our technology learns and understands normal network and process behaviour. Changes from known state results in alerts, allowing users to detect known “indicators of compromise” (IoCs) and novel threat attempts.

The Nozomi Networks solution provides detailed asset identification and network discovery that helps an organisation achieve deep visibility into the status of its industrial control networks. Armed with information, an organisation can identify risks and threats active in its environments. Insight also allows it to implement an effective and targeted mitigation program that maximizes the use of limited human resources, while making informed risk decisions that are both efficient and effective.

VansonBourne

About Vanson Bourne

Vanson Bourne is an independent specialist in market research for the technology sector. Their reputation for robust and credible research-based analysis is founded upon rigorous research principles and their ability to seek the opinions of senior decision makers across technical and business functions, in all business sectors and all major markets. For more information, visit **www.vansonbourne.com**

Nozomi Networks protects the world’s critical infrastructure from cyber threats. Our platform uniquely combines network and endpoint visibility, threat detection, and AI-powered analysis for faster, more effective incident response. Customers rely on us to minimize risk and complexity while maximizing operational resilience.

NOZOMI NETWORKS

nozominetworks.com