Whitepaper

Preparing for NIS2:

How to Drive Awareness and Action at the Board Level

Phil MUNCASTER

Digital Security
Progress. Protected.

EVERSHEDS SUTHERLAND

February 2024

Table of Contents

Spot the difference:

	NIS	NIS2
 **SCOPE**	Limited list of operators of essential services (OES) and relevant digital service providers (RDSPs). OES includes: transport, banking, financial markets, drinking water, digital infrastructure, energy, health.	Broader range of sectors, now also including: Postal/courier, manufacturing, waste water/ management, public administration, space, research, digital services, food production/distribution, electronic comms providers, chemicals, broader scope in regulated subject' size.
 **SECURITY / REPORTING**	Vague requirements for OES and RDSPs to apply "appropriate" security measures and report incidents that "significantly impact" business continuity. Requirement to notify regulator within 72 hours.	10 mandatory baseline security measures (see below). And requirement to notify regulator "without undue delay" or 24 hours of an incident, and file an official report within 72 hours. Organizations also have auditing obligations.
 **ENFORCEMENT**	Member states allowed to set their own threshold for financial penalties.	Harmonized enforcement rules. Fines for essential entities of up to €10m or 2% of global annual turnover (whichever is higher). Fines for important entities of up to €7m or 1.4% of global annual turnover (whichever is higher).
 **MANAGEMENT ACCOUNTABILITY**	Senior managers not held directly accountable for incidents.	Senior management can be held personally liable for non-compliance in cases of serious negligence.

Introduction

According to the European Commission, the annual cost of cybercrime to the global economy is estimated to have reached 5.5 trillion Euros by the end of 2020, being forecasted to double this amount by 2025.

If it were a country, that would make it richer than any other except for the US and China. The target for many of these attacks is critical national infrastructure (CNI) providers, and related partners and suppliers. In response to these and surging nation state threats, the European Commission has introduced a new version of its **EU Network and Information Security (NIS)** directive.

The deadline for member states to implement NIS2 requirements into local law is 17 October 2024. Because it is an EU directive (rather than a regulation), individual countries will interpret the rules slightly differently from each other. That means complying organizations will need to wait until these locally transposed versions of NIS2 are published before they have complete clarity on their compliance requirements and timelines. However, there's still plenty that can be done today to prepare for the incoming rules.

NIS2 aims to improve cyber-resilience across a wider group of organizations deemed to provide essential or important functions across the region. It also aims to reduce inconsistencies in expected baseline cyber-risk management measures across EU member states. Furthermore, it seeks to enhance information sharing between relevant authorities, and establish clear rules for incident response in the event of a large-scale crisis, and reporting in general.

A single data breach is estimated to cost on average $4.5m (€4.1m) today, an all-time high. However, it can reach many times that figure in the event of serious ransomware attack which also takes critical services offline. European consulting firm Sopra Steria admitted a 2020 ransomware attack was likely to cost the firm up to €50m.

However, NIS2 compliance is not just about reducing the significant financial and reputational risks associated with serious cybersecurity breaches. For board members, there's also a more pressing reason. They can now be held personally liable for non-compliance if serious negligence is found to have caused an incident.

These are all compelling reasons why CISOs should be advocating NIS2 compliance to their boards. But rather than frame the process as one of risk mitigation, they can also make a compelling case for compliance as a business enabler. By embracing the challenges it represents as an opportunity, organizations can put the right pieces in place to drive successful digital transformation and sustainable growth.

This white paper will describe what CISOs and boards need to do in order to get there.

When complying with NIS2, board members can not only prevent themselves from being held personally liable if serious negligence is found to have caused an incident, but the compliance can be a business enabler as well. By embracing the challenges it represents as an opportunity, organizations can put the right pieces in place to drive successful digital transformation and sustainable growth.

What's new in NIS2?

NIS2 includes several key changes to the original directive. The main ones are:

A BROADER SCOPE

NIS2 will apply to organizations in the sectors deemed providers of "essential" or "important" services. The former includes large operators from sectors of high criticality like energy banking and healthcare, as well as some special cases. The latter includes large operators from other critical sectors, like digital service providers and manufacturers, as well as medium-sized operators.

STEEPER FINES

NIS2 regulators will be able to fine some organizations up to 2% of annual turnover, or €10m for serious non-compliance. And some penalties can be levied continuously.

MINIMUM SECURITY REQUIREMENTS

NIS2 introduces a baseline set of measures which all organisations must adhere to. These include:

- Risk analysis and information security policies
- Incident management for prevention, detection and response to incidents
- Business continuity and crisis management, including disaster recovery
- Supply chain security
- Securing the acquisition, development and maintenance of network and information systems, including vulnerability management
- Testing and auditing of cyber-risk management measures
- Basic cyber hygiene including cybersecurity training
- Policies and procedures related to use of cryptography and encryption
- HR security, including access control policies and asset management
- Multi-factor authentication or continuous authentication; secure voice, video and text communication; and secure emergency communication systems

SUPPLY CHAIN SECURITY

Organisations must assess and manage third-party risk using "appropriate and proportionate technical, operational and organizational measures." This must begin with a coordinated risk assessment.

MANAGER LIABILITY

Senior managers will be made directly accountable for security in their organization. CEOs or senior legal representatives may even receive a temporary ban in the event of negligence leading to a serious breach. They must receive cybersecurity training and conduct regular risk assessments.

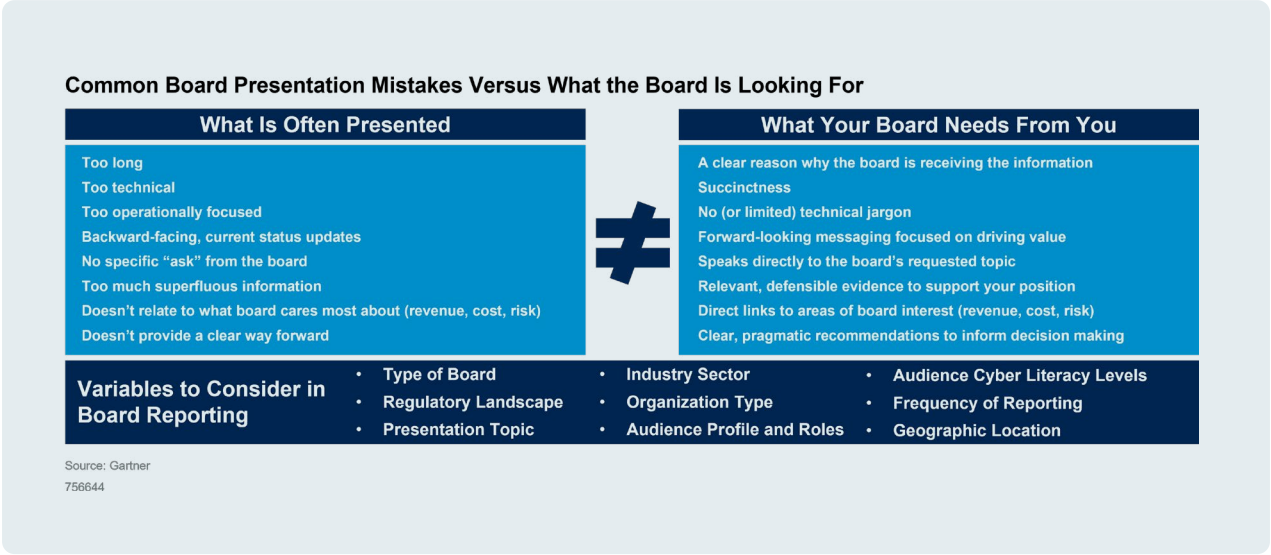
How to talk to the board about NIS2

Board members are becoming more attuned to the importance of cybersecurity to business success. A 2023 World Economic Forum (WEF) study claims "global geopolitical instability has helped to close the perception gap between business and cyber leaders' views on the importance of cyber-risk management."

However, despite this progress, legacy attitudes persist—that cyber is purely an operational IT matter rather than a strategic business function. A 2022 PwC survey reveals that only two-fifths (41%) of directors believe their boards understand security risk "very well." Separate data reveals that just 5% of European board members has cybersecurity experience.

That will make CISOs' challenges more pronounced as they try to communicate the importance of NIS2 compliance to business leaders. Gartner® recognises 8 "Common Board Presentation Mistakes":

Figure 1: Common Board Presentation Mistakes Versus What the Board Is Looking For



Source: *Gartner®*, *CISO Foundations: Comprehensive Resource List for Presenting Cybersecurity to the Board of Directors*, Originally Published 8 August 2022. Updated 26 September 2023. GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally and is used herein with permission. All rights reserved.

To ensure boards get the right message, CISOs should ensure that they:

SPEAK THE RIGHT LANGUAGE AND KEEP IT BRIEF

The first step towards closer cyber-business alignment on NIS2 compliance is to be understood. That means speaking a language of business risk rather than bits, bytes and complex "in the weeds" technology details. CISOs should ditch the technical jargon and make their language simple, clear and accessible. Anecdotal stories from the company or competitor organizations can also help to bring a point home. Explaining with concrete examples what happened to a business when it failed to follow cybersecurity rules could be a powerful way to influence boardroom opinions.

Whatever the content, CISOs should also be aware that their audience will have a limited attention span. That means they should focus on the key points, keep slides to a handful at most, and ensure the presentation is brief and engaging.

SHOW GOODWILL

CISOs should get ready for board requests to get compliant with NIS2 within their existing budget. Those who prepare an analysis on what can be cut now will help to get their CFO and board onside.

MAKE THE DISCUSSION RELEVANT TO THE AUDIENCE

Relevance is everything. That doesn't just mean using a language of metrics and business risk that board members will understand, it's about bringing home the potential impact of non-compliance on them personally. This should be relatively straightforward given NIS2's new personal liability obligations for senior management.

Fines for essential entities run to

€10m

or 2%

of the global annual turnover.

Important entities could face maximum fines of

€7m

or at least 1.4%

of the global annual turnover, whichever is higher.

CISOs should also articulate the potential impact of failing to adhere to NIS2 requirements, in terms of the financial and reputational damage that could stem from serious security breaches. This could include:

- Post-breach response, including regulatory fines and legal costs
- Auditing and proof-of-compliance requirements which could lead to fines from supervisory authorities if not met
- Lost business including immediate disruption, lost customers and an inability to recruit new customers

As part of this discussion, it may also be useful to articulate how regulators will enforce the new directive. For both types of entities, authorities will have the power to conduct on-site inspections and off-site "ex-post" supervision, as well as ad hoc security audits, security scans and data access requests. The latter could include requests for evidence of implementation of cybersecurity policies, such as the results of third-party security audits.

MAKE A POSITIVE BUSINESS CASE FOR COMPLIANCE

CISOs don't have to frame NIS2 compliance in terms of risk avoidance. There's also a strong case to be made for positive business enablement. Specifically, NIS2 compliance could help to:

- Reduce operating costs by eliminating or minimizing downtime, fines and other breach costs listed above.
- Boost revenue by helping the organization differentiate and appeal to customers that prioritize security and privacy. Some 87% of consumers say they'll take their business elsewhere if they don't trust a company is handling their data responsibly. An important competitive differentiator are voluntary certifications such as the EU's ENISA certification or certifications and audit reports relevant for specific industries.
- Differentiate and appeal to business partners that prioritize security. Most organizations where you supply to or do business with, will require a full NIS2 compliance, so you should have it covered. And you should also require it from your suppliers.
- Enhance internal efficiencies through improved processes and reduced error.
- Fuel innovation-powered growth by delivering a stable and secure foundation for digital transformation.

PROMOTE COMPLIANCE AS OPPORTUNITY FOR UP-LEVELLING SECURITY

NIS2 compliance is not a nice-to-have. It is the law. Board members should therefore be advised to look out for nationally transposed NIS2 legislation when it arrives in around October 2024. They will then know more clearly where compliance gaps still exist and what investment is still required.

CISOs should grasp the opportunity this presents to lock in greater investment in security initiatives from the board. This could be the time to promote the need for a multi-year, best practice zero trust program, for example.

62%

of services operators and digital service providers in the EU believe the NIS directive had a positive impact on threat detection.

Source: *ENISA, NIS Investments, November 2022*.

21%

or 1/5

say the same about their ability to swiftly recover from an incident.

Source: *ENISA, NIS Investments, November 2022*.

As always, metrics can help to build the case. According to EU security agency ENISA, 62% of essential services operators and digital service providers in the region believe implementing the first NIS directive had a direct and positive impact on threat detection. And a fifth (21%) say the same about their ability to swiftly recover from an incident.

Preparing a NIS2 compliance program

Once the board has agreed to fund a NIS2 compliance program, it's time to lay the groundwork for kickstarting the project. The first step is determining whether the organization is an essential or important entity. This will dictate what rules it must follow and the potential penalties for non-compliance.

Next, consider the following:

1. **Perform scoping:** What are the regulated services? How can the organization frame them in terms of assets, organizational units, sites and networks?
2. **Undertake a GAP analysis:** To assess existing security posture and highlight areas of NIS2 non-compliance and other vulnerabilities. This should deliver actionable recommendations for improving security controls, governance and other critical areas.
3. **Plan the compliance program:** It should include training and awareness raising for staff and management in line with the new requirements of NIS2.
4. **Consider eligibility for state aid:** To help fund NIS2 compliance efforts. The European Commission has set aside a large pot of funding to specifically help SMEs.
5. **Execute the plan**
6. **Perform reviews / preliminary audits:** To verify the status of compliance.
7. **Adjust the plan and proceed to #3 until compliant.**

Keep these concepts front of mind

Tens of thousands of organizations across the EU will fall under the scope of the new NIS2 directive. Some will be able to handle compliance in-house. But many smaller companies will need to seek external expertise, and potentially funding, to help them accelerate their journey ahead of the October 2024 deadline.

Throughout this process, CISOs should keep three key concepts top of mind: communication, awareness and collective resilience. Communication and awareness-building are critical at a leadership level to secure the necessary funding and ensure that senior managers have the right levels of knowledge and engagement to make key risk management decisions. Above all, this is about building a formidable, Europe-wide collective defense against cyber threats.

Conclusion: Time for action

According to WEF's survey, most business and cybersecurity leaders claim that geopolitical tensions are "moderately" (93%) or "very likely" (86%) to lead to a catastrophic cyber event in the next two years. The stakes couldn't be higher. And that is why NIS2 has been designed—not just to improve cyber-resilience across the bloc, but to make it a board-level issue for the most critical service providers. If, as former IBM boss Ginni Rometty claims, today's CEO also needs to be their organization's chief risk officer, then cyber must be at the heart of any calculation they make about the future direction of the business. Yet most (72%) are still uncomfortable making security-related decisions. This must change, and NIS2 will be the agent of that change.

However, a great responsibility rests on the shoulders of the CISO. It is they who must convince the board and CEO of the importance of NIS2 compliance—not just for avoiding business risk, but also empowering the organization to grow and digitally transform. And it is they who must chart a course towards compliance, including critical training and awareness building among senior leadership. This won't be easy, but the CISOs who excel will find their own role and career prospects enhanced.

The amount of work required will depend on the maturity of the organization's existing security posture and processes, and the level of engagement among senior management. But as with any compliance program, NIS2 is a continuous journey, not a destination. The only certainty is that the journey must start now.

MINIMIZE THE ATTACK SURFACE AND INCREASE NIS2 COMPLIANCE

Vulnerability & Patch Management

Your organization can benefit from additional layer of security thanks to active tracking of vulnerabilities in operating systems and common applications as well as automated patching across all of the endpoints managed through ESET PROTECT.

Managed Detection & Response

ESET MDR and ESET Detection & Response Ultimate are 24/7 threat management services, using AI and human expertise to deliver world-class ransomware protection without the need to maintain in-house security specialists.

Extended Detection & Response (XDR)

ESET Inspect, our XDR-enabling solution, provides risk managers and incident responders with outstanding visibility into threats. It allows them to perform fast and in-depth root cause analysis and immediately respond to incidents.

ESET Threat Intelligence (ETI)

Threat Intelligence from ESET's world-renowned experts delivers in-depth feeds and APT reports. Get a unique perspective on the threat landscape and improve your cybersecurity posture.

ESET Endpoint Encryption

It provides uniquely simple and powerful data encryption and helps greatly increase your organization's data security and compliance with data regulations.

ESET PROTECT PLATFORM

ESET PROTECT Platform

A unified cybersecurity platform, augmented by unique threat intelligence, that integrates balanced breach prevention, detection and response capabilities, complemented by ESET managed & professional services.

An all-in-one protection with 24/7 MDR service
Find out more about **ESET PROTECT MDR**

EXPLORE

This is ESET

Proactive defense. Our business is to minimize the attack surface.

Stay one step ahead of known and emerging cyber threats with our **prevention-first approach**, **powered by AI and human expertise**.

Experience best-in-class protection thanks to our in-house global **cyber threat intelligence**, compiled and examined for over 30 years, which drives our extensive R&D network led by **industry-acclaimed researchers**.

ESET protects your business so it can unlock the full potential of technology.

Progress. Protected.

30+
years of expertise

1bn+
internet users protected

400k+
business customers

195
countries & territories

13
global R&D centers

protected by ESET since 2016
more than 32,000 endpoints

ISP security partner since 2008
2 milion customer base

protected by ESET since 2016
more than 4,000 mailboxes

protected by ESET since 2017
more than 9,000 endpoints

30+ years of continuous innovation

Leading European Union vendor

Always focused on technology

Growing YoY since its inception

Digital Security
Progress. Protected.

Eversheds Sutherland is a global law and civil-law notary firm with 74 offices in 35 countries and employs more than 3,000 lawyers. Due to our international character, we are able to provide cross-border advice like no other. In Europe, Eversheds Sutherland has 44 branches offices.