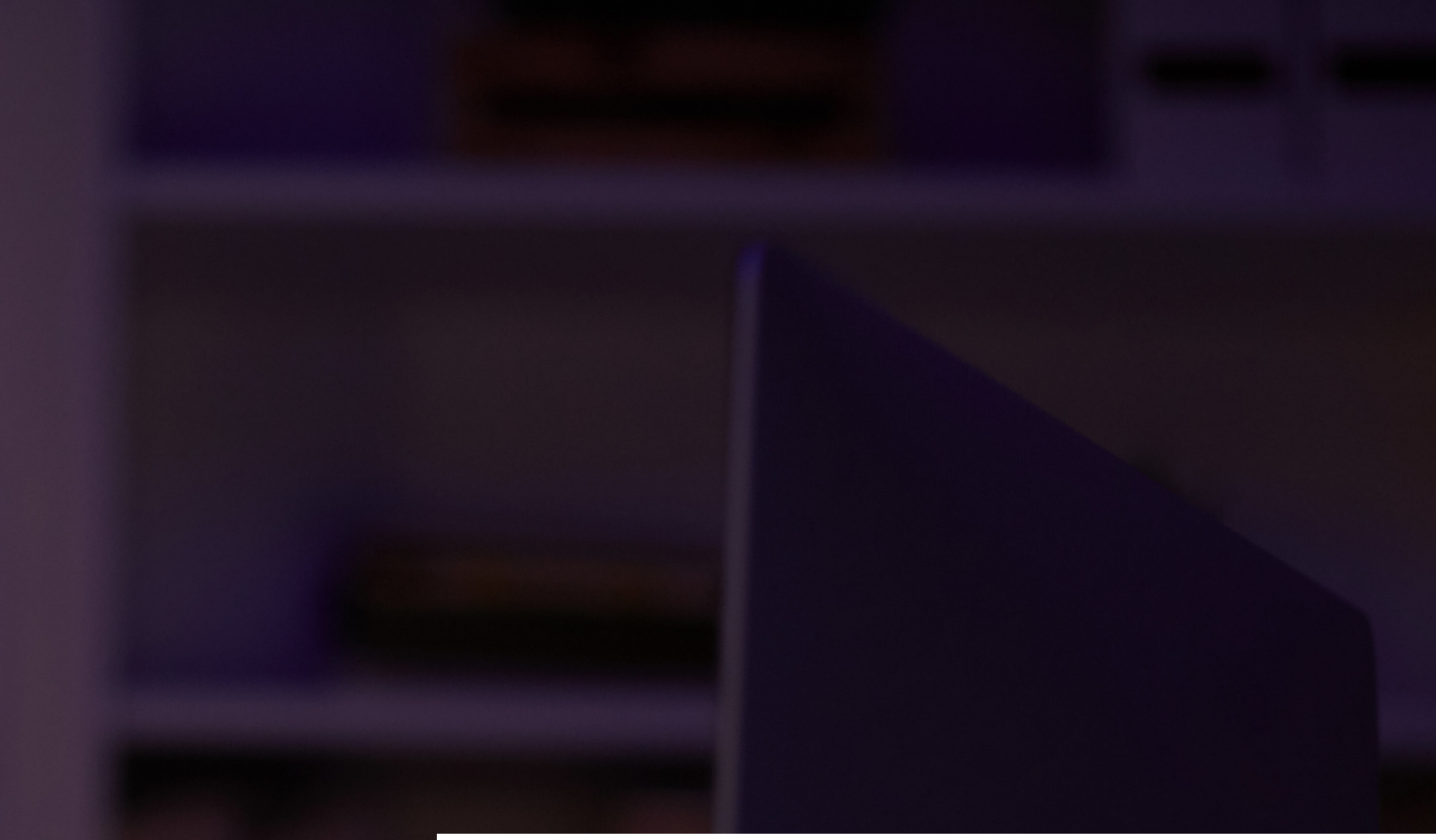
Capgemini invent

FROM STRATEGY TO SHIELD: NIS2 DIRECTIVE'S ROLE IN SAFEGUARDING THE (NATIONAL) CYBER LANDSCAPE


RANSOMWARE
DETECTED



In July 2021, the world was jolted by the far-reaching repercussions of a large-scale cyber-attack that targeted our global supply chain . The incident centered around the deployment of the REvil ransomware, which exploited software vulnerabilities to infiltrate company networks. However, the impact of this attack extended beyond the virtual realm. Factories ground to a halt, supermarkets grappled with shortages, and the episode served as a strong reminder that cyber threats have transcended mere digital nuisances.

These modern-day perils have evolved into entities capable of unraveling the very fabric of our societies by targeting the technologies that we have harnessed to our advantage. Disturbingly, this trajectory of cyber incidents shows no signs of slowing down any time soon. Consumer data, critical assets, and intellectual property are all poised to become potential targets within an increasingly interconnected and digitally reliant world.

Highlighting the urgency of the situation, the European Commissioner for Digital Market sounded the alarm, revealing a staggering 140% surge in cyber-attacks over the past year alone. This escalating trend of digital hazards and interests is documented annually by the EU Agency for Cybersecurity (ENISA) in its Threat Landscape assessment.

The report underscores three key observations: firstly, the proliferation of social engineering attacks, empowered by advancements in Artificial Intelligence, particularly through Large Language Models; secondly, the expanding impact of supply chain attacks due to heightened interconnectivity between organizations; and finally, a new fear that companies harbor, which rivals even ransomware attacks: the prospect of data leaks involving sensitive information which lead to a loss of competitive advantage or theft of trade secrets such as product designs.

The confluence of these threats serves as a poignant reminder of the growing dependency of our society on digital systems and infrastructure.

THE NIS2 DIRECTIVE: A HIGH COMMON LEVEL OF CYBERSECURITY IN THE EU

With the implementation of the NIS (Network and Information System) Directive in 2016 the European Commission introduced the responsibility of ensuring cyber-resilience for organizations belonging to the critical infrastructure.

Its revision in 2022 into the so-called NIS2 Directive triggers a new vision for cybersecurity aligned with the rise of digital threats and reinforced accountability for organizations. Critical market players in scope are divided into essential and important entities; the main difference being proactive monitoring from the – yet to be designated – competent authority versus reactive monitoring in case of a suspected incident.

Essential entities pertain to vital sectors such as energy, transport, banking, wastewater, healthcare, and public administration. NIS2 extends its scope of applicability to, among others, Managed Security Service Providers (MSSPs), data centers, and cloud computing service providers. The shift for digital service providers from a light supervisory regime under NIS1 into a stricter regime underlines the endeavor of the European Union to strengthen the security of the entire (digital) supply chain. The other entities qualified as important belong to sectors such as waste management, research, and food production to name a few. In total, seventeen market sectors are in scope representing substantial portions of the national economy.

The directive came into force in January 2023 and will be applicable from October 2024, which is also when Member States need to transpose the legislation into national law. Until then, the European Commission has yet to define its implementing guidelines, supported by further guidance from the EU Agency for Cybersecurity (ENISA) and the NIS Cooperation Group. During the national translation of the NSI2 Directive, each country may add requirements on specific sectors.

1. https://securityintelligence.com/posts/revil-ransomware-kaseya-supply-chain-attack/
2. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022

BRINGING CYBERSECURITY TO THE BOARD OF DIRECTORS

This European legislation is a unique opportunity for every CISO (Chief Information Security Officer), cybersecurity professional, and cybersecurity strategist to draw attention to cybersecurity at the board level and enforce a top-down mandate.

From an organizational point of view, the road to implementation of NIS2 starts with the understanding and acknowledgement of cybersecurity risks at the board level. For instance, cybersecurity should be considered for the feasibility of a new innovative project, when defining a multi-year business strategy, or when setting new business relations with IT suppliers.

In this regard, the perspective of digital security becomes an addition towards establishing the organizational strategy. Risk management, whether operational or financial, is already performed, and in most cases the security of assets is already in place. The major difference is that digital security is no longer the sole endeavor and task of IT or the responsibility of the Chief Information Officer (CIO) or CISO. Cyber is now the new normal and has become a “board issue”, which must be reflected in the overall governance.

Senior leadership must oversee cybersecurity compliance because of their accountability in mitigating cybersecurity risk measures and providing training across the organization.

Indeed, C-level management is personally liable in case of proven negligence of a cyber incident or for not adequately investing in the required organizational and cybersecurity measures. Business line management, or head of departments, should incorporate and adopt cyber threats in their current risk management processes, support a thorough identification of their critical digital assets, and keep cyber hygiene part of the way of working for their teams. Beyond its own perimeter the organization must be aware of how its ecosystem manages cybersecurity in the provision of its services.

A tangible manifestation of this expanded scope is evident in the inclusion of MSSPs and digital infrastructures among the entities subject to national compliance monitoring. Similarly, public administrations, such as local governments and executive organizations like employment agencies or tax authorities, are now included by NIS2. For these entities, safeguarding the network and information systems that underpin citizen data emerges as an imperative. In the long term, the NIS2 directive could become a new concept or label that citizens may use as an assurance for trust.

The supply chain will see its due diligence increase, as clients should consider the cyber practices or the quality and resilience of third-party products and services. Furthermore, organizations’ compliance with NIS2 will spill over into domains other than cybersecurity, to name one, it will force organizations to improve and review the coordination and communication lines within the organization due to the crisis management requirements laid out by NIS2, which go beyond cybersecurity. Clients who are NIS2 compliant will over time become more thorough in their cybersecurity management and agreements.

At the European level, Information Sharing and Analysis Centers (ISACs) started to develop in 2016, fostered and embraced by the 2016 NIS Directive. In an ISAC CISOs engage in conversations with each other in a trusted environment. This improves the situational awareness of every individual organization and fosters a culture where in similar companies can exchange knowledge on vulnerabilities and warn and be warned of upfront cascading threats that have been identified.

Another initiative propelled by the NIS2 Directive is the EU-CyCLONe. This new cooperation network will gather all Member States to support the coordination of large-scale incidents, promote situational awareness, and increase preparedness for cross-border or cross-sector cooperation. This is an incentive for Member States to be trained and ready forlarge-scale scenarios.

For organizations, this aligns with the requirement to regularly test not only their environment but also their communication procedures on the top threat scenarios. This will include regular training of the board decision-making under the pressure of a cybersecurity attack and knowing how to communicate internally, to the authorities, or to the public.

STRICTER REPORTING TO THE AUTHORITIES

National authorities, yet to be determined per sector in all countries, will proactively monitor the compliance of the essential entities in scope.

"Significant cyber incidents" will be reported by any organization under the NIS2 Directive to the National Computer Security Incident Response Team (CSIRT). Therefore, entities will have to prepare their internal reporting procedures for the authorities within set timelines: 72 hours in case of a cyber incident and 24 hours in case of suspected malicious cyber activity.

This will require having a robust cybersecurity organization with roles and responsibilities, clear internal communication, mitigation of cascading effects within the organization or on other sectors, and a good outlook on threats. Besides, this means that the regulator will have to provide guidance, information, and training to help prepare the market.

Crucially, NIS2 introduces a powerful enforcement mechanism in the form of fines—a turning point for European legislation on cybersecurity.

Entities that fail to meet NIS2's stipulated requirements will be subjected to financial penalties, marking a significant difference from the previous legislation. If negligence in taking the proper cybersecurity or organizational measures is proven in the aftermath of a cybersecurity breach, the organization risks an administrative fine. This fine is capped at either EUR 10 million or 2% of the total global turnover (whichever is higher) Such breaches could potentially culminate in temporary bans for managerial personnel and the designation of monitoring officers tasked with overseeing and enforcing mitigating actions.

Since NIS1 in 2016, public awareness of cybersecurity has grown significantly because of the large-scale attacks and data breaches that did not go unnoticed by the media. The news awoke sensitivity to the issues in individuals, businesses and organizations, which lead to increased awareness of the growing risks and the ever-developing techniques cyber criminals and state-sponsored attackers use.

The national transposition of the NIS2 by the Member States is the opportunity for the European governments to manifest and disseminate their stance on cybersecurity. It can also be an invaluable vehicle to educate and engage citizens. Using legislation as such an instrument is not a new practice: consider the impact that the introduction of the General Data Protection Regulation (GDPR) had in informing citizens about the European values of privacy and personal data protection. Those values translated into renewed rights and created a shared vocabulary to work together on issues (e.g., the terms "data controller" and "data processor" defined in legislation, that today we all share).

THE FUTURE

The EU Digital Agenda for cybersecurity goes further than NIS2 alone. Sectoral legislations complement the NIS2 Directive, such as the Critical Entities Resilience Act (CER), which considers physical security for critical infrastructures, or the Digital Operational Resilience Act (DORA) which sets cybersecurity as part of the financial resilience for the financial sector. The Cyber Resilience Act (CRA) was presented in November 2022. It lays the foundation for more regulated cybersecurity of connected products and software and positions the liability on the manufacturer. At the heart of the discussion will be the question of the origin and the location of the data processing, as well as the disclosure requirements.

Zooming out, these legislations are all part of the larger EU-cybersecurity framework designed to instill the concept of ''cybersecurity by design'' into organizations and connected products and devices circulating on the EU market, as affirmed recently again by the European Commission with the release of the Cyber Shield to step up for a collective resilience. Cybersecurity by design is, in the long run, the sustainable approach to cybersecurity as it ensures minimal vulnerabilities and therefore minimal opportunities for attackers. Today, organizations must start by considering this long-term goal and adjust their business and operations according to the NIS2 Directive which sets the tone.

CONCLUSION

The organizations in the selected sectors have been given the responsibility to secure their core processes if they are important for national stability, resilience, and the economy. However, there is a risk that organizations in scope view the NIS2 as an exercise in compliance, rather than an action-oriented call to increase cybersecurity maturity. This would be a mistake. Becoming compliant with NIS2 requires strong coordinated efforts across an organization which go beyond the usual control assessment. The business lines, the legal department, procurement, human resources, learning and development, and security and IT offices will have to work side by side to achieve the prescribed level of cybersecurity maturity.

It is the momentum for any organization to raise awareness, and knowledge on what cybersecurity means for everyone's daily jobs and set up good habits to protect not only the organization but society as a whole. At first glance this might seem rigorous, yet, relating to the REvil ransomware attack the importance of NIS2 is emphasized when thinking about the potential adverse effects of a vulnerable food, energy, or transport sector. Upon its implementation in national laws – and even before that – NIS2 will become the driving force to accelerate the maturity of organizations' digital security.

ABOUT THE AUTHORS

Ana-Isabel Llacayo, CISM
NIS2 Lead Advisor and Data Security Manager, Capgemini Invent
Ana-Isabel is specialized in EU Cyber policies, and advises public and private organizations on EU regulations, seeking to raise awareness on cyber risks.
ana.isabel.llacayo@capgemini.com

Emir Hajduk
Management consultant data security, Capgemini Invent
Emir works on security governance, digital crime, and advises on behavioral change approaches to cybersecurity.
emir.hajduk@capgemini.com

With thanks to

Roeland de Koning for his insights and review.

About Capgemini Invent

As the strategy, innovation, design and transformation brand of the Capgemini Group, Capgemini Invent enables CxOs to envision and shape the future of their businesses. Located in more than 36 offices and 37 creative studios around the world, it comprises a 10,000+ strong team of strategists, data scientists, product and experience designers, brand experts and technologists who develop new digital services, products, experiences and business models for sustainable growth.Capgemini Invent is an integral part of Capgemini, a global leader in partnering with companies to transform and manage their business by harnessing the power of technology. The Group is guided everyday by its purpose of unleashing human energy through technology for an inclusive and sustainable future. It is a responsible and diverse organization of over 360,000 team members in more than 50 countries. With its strong 55-year heritage and deep industry expertise, Capgemini is trusted by its clients to address the entire breadth of their business needs, from strategy and design to operations, fueled by the fast evolving and innovative world of cloud, data, AI, connectivity, software, digital engineering and platforms. The Group reported in 2022 global revenues of €22 billion.

Capgemini Invent
Postbus 2575 - 3500 GN Utrecht
Tel. + 31 30 203 05 00
www.capgemini.nl/invent

06-049.23