University of Piraeus

School of Information and Communication Technologies

Department of Digital Systems

Postgraduate Program of Studies

MSc Digital Systems Security

NIS 2 Directive: Implications for System and Infrastructure Security

Supervisor Professor: Stefanos Gritzalis

Alkiviadis Giannakoulias alkis.gian@gmail.com Student ID.: MTE2105

Piraeus

2023

Executive Summary

Responding to the evolving and expanding threat landscape, the evolution of digitalization, as well as the increase in cyber-attacks, the Commission proposed to expand the scope of the Network and Information Security (NIS) Directive, aiming to increase the level of cybersecurity in Europe in the longer term. Regulatory changes are geared by the effectiveness of the existing legislation, the development of technologies, our ever increasing dependence on information technology, with more sectors and services being increasingly interconnected, and the new ways attackers exploit vulnerabilities and launch their cyber-attacks. After a two-year legislative process, political agreement on NIS 2 took place in May 2022 followed by its publication in the Official Journal of the European Union (OJ L 333/80) entering into force on the 16th of January 2023.

Following the recent reform of the NIS Directive this study identified the **contributions** to the EU cybersecurity regulatory landscape as well as the **implications for system and infrastructure security**, including an **action plan for entities**, to help them comply with NIS 2, **and for Computer Security Incident Response Teams** (CSIRTs) in the performance of their tasks. The key findings of the study, include:

a) **Expanded scope**, as the "*directive applies to public or private entities which are medium-sized enterprises and which provide their services or carry out their activities within the Union*". The expansion of the scope covered by the new rules, will help **increase the level of cybersecurity in Europe in the medium and longer term**[1].

b) **Increased risk management** requiring from "*essential and important entities to take appropriate and proportionate technical, operational and organisational measures to manage the risks posed to the security of network and information systems*";

c) **Accountability of top management** for non-compliance with the NIS 2 requirements, resulting in serious consequences;

d) **Alignment with sector-specific legislation**, in particular, the regulation on digital operational resilience for the financial sector (DORA) and the directive on the resilience of critical entities (CER);

e) **Streamlined reporting obligations,** requiring from public or private entities that are victims of cyberattacks to declare within 24 hours an early warning to the CSIRT or, where relevant, their competent authority, followed by a submission of an incident notification "*without undue delay and in any event within 72 hours after having become aware of the incident, with the aim, of updating information submitted in the early warning notification*". This will make it possible to assess the importance and seriousness of the cyberattack, while avoid over-reporting and creating an excessive burden on the entities covered;

f) **Imposition of fines**, as in the event of non-compliance with the rules established by the NIS 2 Directive, entities can be subject to fines up to €10 million or 2% of their total turnover worldwide, whichever is higher (the same as a GDPR fine for a less serious violation);

g) **Formal establishment of the European Cyber Crises Liaison Organisation Network** (EU - CyCLONe), which will support the coordinated management of large-scale cybersecurity incidents and crises;

[1] https://ec.europa.eu/commission/presscorner/detail/en/IP_22_2985

h) **Voluntary peer-review mechanism** aiming to strengthen mutual trust and learning from shared experiences in the Union, achieving a high common level of cybersecurity;
i) **Security of supply chains and supplier relationships**, by ensuring that risk is managed within these processes;
j) **Upgraded tasks and powers of CSIRTs**, as they undertake new roles while expanding existing ones under the NIS Directive. CSIRTs tasks and powers are expanded from monitoring and analysing incidents to providing, upon request, assistance to entities, collecting and analysing forensic data and providing dynamic risk and incident analyses. In addition, proactive scanning of public networks and Coordinated Vulnerability Disclosure (CVD) tasks have been added to the tasks of CSIRTs.

The NIS 2 Directive **aims to set the baseline for cybersecurity risk management measures**, **harmonizes the cybersecurity requirements** and **implementation of cybersecurity measures** in all EU Member States, **addresses security of supply chains and supplier relationships**, includes **incident reporting obligations** for essential and important entities in all EU Member States and introduces **accountability of top management** for non-compliance with the NIS 2 requirements. It is an ambitious piece of legislation that requires a lot from companies and Member States in achieving a high common level of cybersecurity across the EU. Like its predecessor it is a challenging and costly task, but considering the "*annual cost of cybercrime to the global economy is estimated to have reached €5.5 trillion by the end of 2020*"[2], it is a small price to pay.

The NIS 2 Directive will care the resilience and incident response capacities of public and private entities, competent authorities and the EU as a whole and will ensure stronger risk and incident management and cooperation.

The enforcement of NIS 2 is not scheduled for tomorrow. Nevertheless, entities falling under the scope of the NIS 2 Directive should start working on compliance now, as some of the work might take more time than planned. The majority of the work to be done should be organized along the following three pillars: a) Governance, b) Incident Detection and Response, and c) Security Testing. Entities should investigate whether the fall under the scope of the NIS 2 Directive. If they fall under scope of the Directive, they should explore the organisational, financial and technical phases/steps that will be obliged to implement for complying with the Directive. Their actions should revolve around the cybersecurity measures (requirements) outlined in Article 21.

Member States, including their CSIRTs and national cybersecurity offices, will have to adapt to the increased tasks and number of entities. This will require additional capacity, in terms of human and financial resources to fulfil the increased tasks, as well as attracting expertise that may not be possible due to the lack of resources or a lack of candidates with the right skills and qualifications. Use of automated tools for scanning or information sharing must comply with the human rights principles, established in the EU Charter of Fundamental Rights, and in national constitutions of Member States, including the right to privacy and data protection.

[2] https://www.europarl.europa.eu/news/en/headlines/security/20221103STO48002/fighting-cybercrime-new-eu-cybersecurity-laws-explained

Contents

Figures

Acronyms & Abbreviations

Term	Description
AI	Artificial Intelligence
CER	Critical Entities Resilience Directive
CERT	Computer Emergency Response Team
CII	Critical Information Infrastructures
CIS	Critical Infrastructure Systems
CSIRTs	Computer Security Incident Response Teams
CVD	Coordinated Vulnerability Disclosure
DNS	Domain Name System
DORA	Digital Operational Resilience Act
DSPs	Digital Service Providers
DSPs	Digital Service Providers
EASA	European Union Aviation Safety Agency
ECA	European Court of Auditors
ENISA	EU Agency for Cybersecurity
EPRS	European Parliamentary Research Service
EU - CyCLONe	European Cyber Crises Liaison Organisation Network
GDPR	General Data Protection Regulation
IA	Impact Assessment
ICT	information and communication technology
IoT	Internet of Things
ISAC	Information Sharing and Analysis Centre
MISP	Malware Information Sharing Platform
MS	Member States
MSSPs	Managed Security Service Providers
NCA	National Competent Authority
NIS	Network and Information Security
OES	Operators of Essential Services
OPC	Open Public Consultation
RDP	Remote Desktop Protocol
RSB	Regulatory Scrutiny Board

SOCs	Security Operation Centres
VDP	Vulnerability Disclosure Policy
VPN	Virtual Private Network

1 Introduction

Europe is in the midst of a huge digital transformation, drastically affecting the economy and society by improving living standards and economic output. "*Digital transformation touches on all aspects of our lives, from public health, societal and democracy issues, and the environment, to the economy*"[3] and has the potential to radically change the economy and society. The information and communication technology (ICT) sector is the key enabler of digital transition and examples of digital technologies driving this revolution are the internet of things (IoT), cloud computing, artificial intelligence (AI) and blockchain technologies that have changed the way businesses operate today, how people connect and exchange information, and how they interact with the public and private sectors[4]. According to the OECD[5] their increased affordability and computing power is accelerating this transformation.

Cybersecurity is a challenge for the EU as a whole, underlined by the low ranking of virtually all EU Member States (MS) on the Global Cybersecurity Index.[3] Cyberspace has no boundaries and it relies on interconnected digital technology and interdependencies on backbone networks. Cyber warfare poses a threat to the global system, as threats are usually not restricted to one particular sector and in most cases affect more than one. In fact, several major cyber-attacks, deliberately, or unintentionally, spread far beyond their intended targets causing widespread harm to a nation's security and capacity to defend itself and its society.

The rapid increase in digitization and online transactions, puts sensitive data of individuals and organisations under constant threat from malicious actors (insiders and outsiders). Meanwhile the complex interdependencies and interconnections of Europe's critical information infrastructures (CII) are ever increasing, making them more exposed to cybersecurity threats and more vulnerable to cyberattacks. The evolving ICT infrastructures combined with the diversity of emerging technologies (e.g. IoT, cloud computing and AI) and continuous industry digitisation results in any large-scale incident in one industrial sector having a cascading effect elsewhere.

To this end the Network and Information Security (NIS) Directive, which was adopted on 6 July 2016, was the first horizontal EU cybersecurity legal act and established the EU's rules on the security of network and information systems thus achieving a high common level of cybersecurity across the MS. It forms part of the EU cybersecurity policy and in particular the EU's cybersecurity strategies.

While it has contributed to the overall increase of all EU MS cybersecurity capabilities, its implementation proved difficult, resulting in fragmentation across the Union internal market.

Responding to the evolving and expanding threat landscape, the evolution of digitalization, as well as the increase in cyber-attacks, the Commission proposed to expand the scope of the NIS Directive by effectively forcing more entities and sectors to take measures, aiming to increase the level of cybersecurity in Europe in the longer term.

[3] https://www.europarl.europa.eu/RegData/etudes/STUD/2022/699475/EPRS_STU(2022)699475_EN.pdf
[4] EU policies – Delivering for citizens: Digital transformation
[5] OECD Digital Economy Outlook 2017

1.1 Cyber security challenges

As identified by numerous reports and studies, including EU Agency for Cybersecurity (ENISA) Threat Landscape (ETL-2021) report[6], cybersecurity attacks are growing in scale, cost and sophistication, "*cybersecurity threats are on the rise*", while the cybersecurity landscape has greatly evolved "*in terms of sophistication of attacks, their complexity and their impact*". This is due to:

- **Exploitation of Work-From-Home technologies**, especially Virtual Private Network (VPN), Citrix and Remote Desktop Protocol (RDP) services, due to the COVID-19 pandemic, significantly increasing the attack surface and the number of cyber-attacks targeting organisations through home offices.
- **Ever-growing online presence and attack surface**, due to the transitioning of traditional infrastructures to online and cloud-based solutions, advanced interconnectivity, the exploitation of new features of emerging technologies such as AI, together with the constantly growing number of devices connected to the network, provide **new opportunities to threat actors** and use cases for cyberwarfare. According to publicly available reports[7], **threats are growing at three times faster** than they are going dormant with new threat groups discovered during the last period.
- **Cybercriminals fine-tuning their capabilities** to breach even the tightest security operations, improving their resources and (technical) capabilities to conduct advanced cyber-attacks by **taking advantage of existing and new vulnerabilities** and **automated attack tools**. At the same time response handling in Security Operation Centres (SOCs) and by Computer Security Incident Response Teams (CSIRTs) is still mostly human-centred, leading to an uneven battle: machine speed versus slow human inspection.

During the last few years, we witnessed an evolution in how threat actors are conducting their operation, as they conduct more **targeted operations** compared to the "noisy" approaches in the past. Observing the ongoing conflict between Russia and Ukraine, Russian state-sponsored threat actors use a variety of malware tools targeting governmental infrastructures, while their objectives vary from espionage attacks, designed to exfiltrate data from targeted systems, to destructive attacks meant to destroy data and render targeted systems inoperable. The **transportation industry** faces cybercrime threats targeted to initial access offerings, gift card fraud, and ransomware.[8] All four of the world's largest **shipping companies** were victims of cyber-attacks during recent years[9], while the trucking and logistics sector has experienced high-profile ransomware attacks.[10] Considering that during the pandemic the **Courier, Express, and Parcel** business bloomed, it attracted the attention of cybercriminals who targeted the sector[11]. Interestingly, the **finance, energy** and **education**

[6] https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021

[7] https://hub.dragos.com/hubfs/312-Year-in-Review/2020/Dragos_2020_ICS_Cybersecurity_Year_In_Review.pdf

[8] https://intel471.com/blog/how-cybercriminals-create-turbulence-for-the-transportation-industry

[9] https://www.zdnet.com/article/all-four-of-the-worlds-largest-shipping-companies-have-now-been-hit-by-cyber-attacks/

[10] https://www.freightwaves.com/news/5-defining-cyberattacks-on-trucking-and-logistics-in-2020

[11] https://www.srm-solutions.com/blog/the-courier-express-and-parcel-industry-is-booming-but-cyber-security-must-grow-alongside-revenues-heres-why/

sectors reported large increase in targeted and sophisticated **DDoS campaigns**[12] that are much more persistent and increasingly multivector. Moreover, many academic institutions experienced extensive data breaches, aiming to exfiltrate sensitive data on innovations for COVID-19 vaccine-related research. **Business E-mail Compromise** has also increased and grown in sophistication and has become more targeted. At the same time, as previously discussed in IOCTA 2020, **cybercriminals increasingly target smaller organisations** with lower security standards, ensuring successful attacks with smaller volumes of data and maximum revenue. Furthermore, as the cost of attacking well-protected organisations increases, attackers prefer to attack their **supply chain which may be less protected**, providing additional implications due to a potentially large-scale and cross-border impact, with systemic risk characteristics. Identification and mitigation of **targeted threats and sophisticated attack techniques** that can mimic valid user activity, do not have a signature, and do not occur in patterns, still **remains a challenge**. At the same time response and recovery times should be reduced, highlighting the **need for increased incident response automation**.

According to the 15th annual Verizon Data Breach Investigations Report (DBIR)[13] the number of ransomware attacks increased by 13% between 2020 and 2021 – a rise as big as the last five years combined (for a total of 25% for 2022).

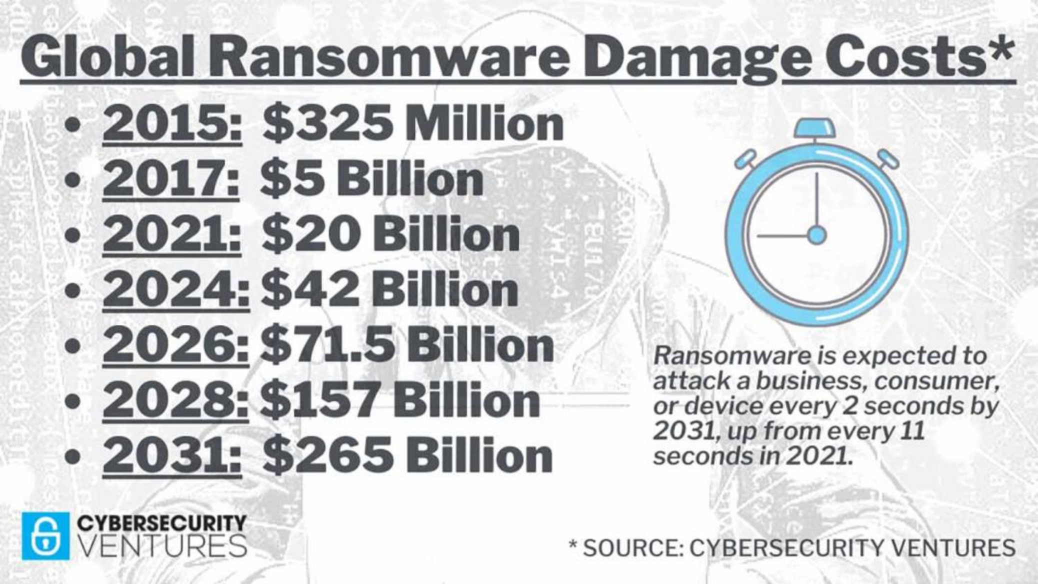

Figure 1. Ransomware-Data-Graphic

Consequently, **companies have to heavily invest to provide a safer cyberspace** not only for themselves but also their customers. We have to note however that attacks affect not only companies but also citizens and entire countries.

The first known cyber-attack on a country was a politically motivated cyber-attack campaign mounted on Estonia in April 2007, lasting twenty-two days, "*resulting in temporary degradation or loss of service on many commercial and government servers*"[14]. It affected the online banking services and Domain Name System (DNS) service providers. Since then, a

[12] https://www.f5.com/labs/articles/threat-intelligence/ddos-attack-trends-for-2020

[13] https://www.verizon.com/business/resources/reports/2022/dbir/2022-data-breach-investigations-report-dbir.pdf

[14] https://ccdcoe.org/uploads/2018/10/Ottis2008_AnalysisOf2007FromTheInformationWarfarePerspective.pdf

growing number of countries have been targeted by cyber-attacks on their critical infrastructures, such as on Electrical Power and Energy System (EPES), hospitals and water supply and distribution plants.

The latest known ransomware attack happened over the past year, was the Colonial Pipeline ransomware attack[15,16]. On the 7th of May 2021 this massive attack shut down gas supplies across the United States Eastern Seaboard, requesting the payment of a multi-million-dollar ransom. To keep supplies flowing multiple US agencies were involved such as the USDOT Federal Motor Carrier Safety Administration (FMCSA), the US Federal Bureau of Investigation (FBI) and the Cybersecurity and Infrastructure Security Agency (CISA). The attack highlighted the vulnerability of critical infrastructure systems (CIS) to ransomware attacks and motivated the multiple countries to introduce new legislation imposing stricter sentences for individuals targeting critical infrastructures with a ransomware attack. And as indicated by an ENISA report on Threat Landscape for Ransomware Attacks[17] it is not an idle threat.

Ransomware has significantly evolved, both technically and organisationally, since the first incident was observed in 1989[17]. As Sophos researchers anticipate the market has matured to such a degree that ransomware has become a commodity[18]. The new ransomware-as-a-service business model allows almost anyone to lunch ransomware attacks at discount prices.

According to Eurobarometer survey 2280 / FL496[19], 28% of European SMEs have experienced at least one type of cybercrime in 2021. SMEs are the most likely to be concerned about hacking (or attempts to hack) online bank accounts (32% are 'very concerned') and phishing, account takeover or impersonation attacks (31%), and viruses and spyware or malware (excluding ransomware) (29%).

According to Eurobarometer survey 2249 / 499[20], the majority of Europeans express concerns about becoming the victim of cybercrime, but only a minority have actually been a victim and are aware of this. Nearly eight in ten respondents believe that there is an increasing risk of being a victim of cybercrime (79%), while just over six in ten (61%) think that they are able to protect themselves against it.

Meanwhile in 2021, "*83% of organizations reported experiencing phishing attacks*"[21], with "*roughly 65% of cyber attackers leveraging spear phishing emails as a primary attack vector*".

According to the 15th annual Verizon DBIR, financially motivated attacks are still the top motive since 2015, ranging between 86% and 100% in 2022. Espionage-related attacks are 2nd place for years, and hacktivism is, for the most part, simply an afterthought. It is worth noting that espionage has almost certainly increased over the last few years. According to the same report credential theft in the EU remains a problem and regardless of how threat actors obtain those credentials (the rise of Social Engineering provides a likely answer), once they are acquired they are used to leverage access to obtain more Credentials via Phishing, or

[15] https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password

[16] https://www.zdnet.com/article/colonial-pipeline-ransomware-attack-everything-you-need-to-know/

[17] https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-ransomware-attacks

[18] https://www.computerweekly.com/news/252492290/2021-the-year-of-commodity-ransomware-says-Sophos

[19] https://europa.eu/eurobarometer/surveys/detail/2280

[20] https://europa.eu/eurobarometer/surveys/detail/2249

[21] https://www.cybertalk.org/2022/03/30/top-15-phishing-attack-statistics-and-they-might-scare-you/

utilize details gained from company emails to craft realistic pretexts as part of Business email compromise (BEC) attacks.

The human element continues to drive breaches. In 2022 82% of breaches involved the human element, either through the Use of stolen credentials, Phishing, Misuse, or simply an Error. About 46% of breaches featured hacking (The Denial of Service – DoS), followed by Backdoor or C2 malware types at 17%.

Fuelled by the technological developments such as the proliferation of devices linked to the Internet of Things (IoT), this trend is expected to increase further. Considering the rollout of over 41 billion IoT devices by 2025[22], and the growing challenges in the cybersecurity landscape have led the EU to reflect on the cyber security strategies and tools against cyber-threats and attacks.

1.2 Cost of Cybercrimes and Cybersecurity

Cyber-attacks are one of the fastest growing crimes worldwide. The global cyber security market was valued at USD 139.77 billion in 2021. The market is projected to grow from USD 155.83 billion in 2022 to USD 376.32 billion by 2029, exhibiting a CAGR of 13.4% during the forecast period.[23]

According to a report from Cybersecurity Ventures[24], "*the global ransomware damages is predicted to exceed $265 billion (USD) annually by 2031, 13 times more than the amount forecasted for 2021, with a new attack (on a consumer or business) every 2 seconds*", up from every 40 seconds in 2016 and 11 seconds in 2021.

According to the Ninth Annual Cost of Cybercrime Study[25], from Accenture Security, the average cost of the cybercrime increased from US$11.7 million in 2017 to US$13 million in 2018. According to the above-mentioned report, the United States average annual cost of cybercrime increased by 29% in 2018 to reach US$27.4 million, with the highest increase of 31% experienced by organizations in the United Kingdom which grew to US$11.5 million, closely followed by Japan which increased by 30% in 2018 to reach US$13.6 million.

[22] https://digital-strategy.ec.europa.eu/en/policies/next-generation-internet-things

[23] https://www.fortunebusinessinsights.com/industry-reports/cyber-security-market-101165

[24] https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-250-billion-usd-by-2031/

[25] https://www.accenture.com/_acnmedia/accenture/redesign-assets/dotcom/documents/local/1/accenture-ninth-annual-cost-cybercrime.pdf

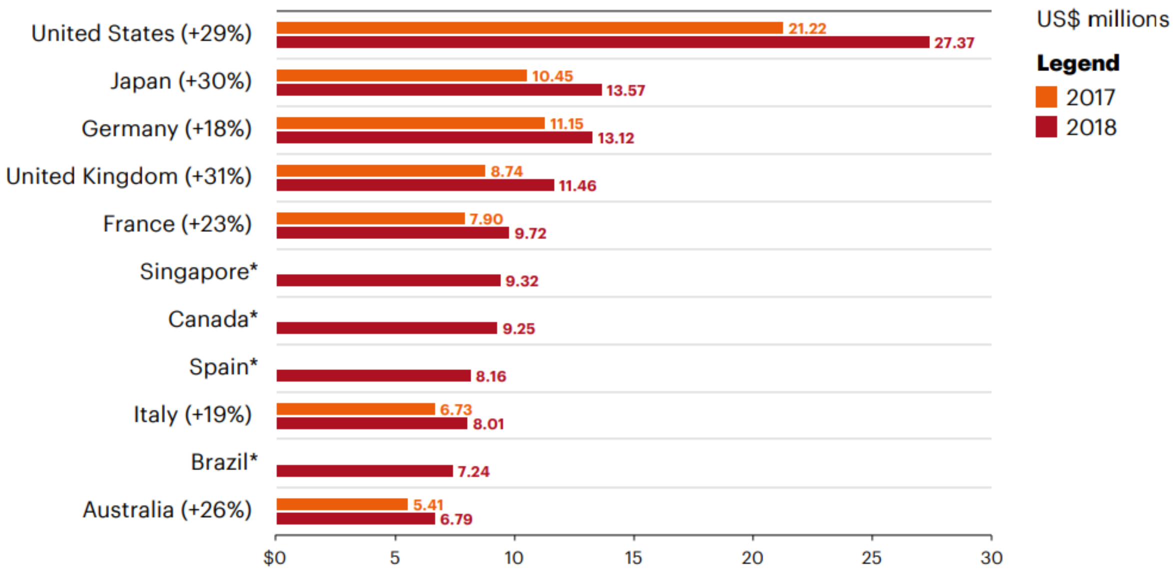

Figure 2. The average annual cost of cybercrime by country (25)

The global COVID-19 pandemic has been unprecedented and staggering, with security solution experiencing higher-than-anticipated demand across all regions compared to pre-pandemic levels. Based on our analysis, the global market had exhibited a rise of 7.7% in 2020 as compared to 2019.

1.3 EU Cybersecurity Policy

In March 2009, the Commission published a communication on Critical Information Infrastructure Protection “Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience”[26] [COM(2009) 149] that focused on prevention, preparedness and awareness, and defined a plan of immediate actions to strengthen the security and resilience of critical information infrastructures and strengthen the security of and the trust in the information society.

In February 2013, the European Commission and the High Representative of the Union for Foreign Affairs and Security Policy issued a Joint Communication, proposing the “Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace”[27] (JOIN(2013) 1) “*outlining the EU's vision in this domain, clarifying roles and responsibilities and setting out the actions required based on strong and effective protection and promotion of citizens' rights to make the EU's online environment the safest in the world*”. The adoption of the strategy was the first step towards the creation and development of an EU cybersecurity ecosystem and was structured along the following objectives:

- Achievement of cyber resilience;
- Reduction of cybercrime;
- Development of cyberdefence policy and capabilities related to the Common Security and Defence Policy (CSDP);
- Development of industrial and technological resources for cybersecurity;

[26] https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A52009DC0149
[27] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52013JC0001

- Establishment of a coherent international cyberspace policy for the European Union and promotion of core EU values;

Following the publication of the strategy the Commission published a proposal for a "Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security (NIS) across the Union"[28] [COM(2013) 48 final] – the NIS Directive – the first EU-level legislation on cybersecurity. The draft Directive[29] passed the European Parliament by a large majority on March 13th 2014[30] and entered into force in August 8th 2016, while the national transposition by the EU MS happened on May 9th 2018.

Then on the 19th September 2017[31] the European Commission and the High Representative of the Union for Foreign Affairs and Security Policy issued a Joint Communication to the European Parliament and the Council on "Resilience, Deterrence and Defence: Building strong cybersecurity for the EU" [32] [JOIN(2017) 450 final] that was part of a larger '*EU cybersecurity package'*, consisting of:

- an ambitious reform proposal for a regulation on ENISA and the EU cybersecurity certification framework[33] (the '*Cybersecurity Act'*) [COM(2017) 477 final];
- a communication[34] aimed at supporting MS in their efforts to effectively, swiftly and coherently implement the NIS Directive (the '*implementation toolkit*'), "*by providing best practice from the Member States relevant to the implementation of the Directive and guidance on how the Directive should be operating in practice*" as well as clarifications on some of its provisions;
- a recommendation on "Coordinated response to large-scale cybersecurity incidents and crises"[35] [C(2017) 6100 final] and its annex (the *'Blueprint'*). The presented Blueprint explained *"how cybersecurity is mainstreamed to existing Crisis Management mechanisms at EU level and sets out the objectives and modes of cooperation between the MS as well as between MS and relevant EU Institutions, services, agencies and bodies[36] when responding to large scale cybersecurity incidents and crises"*;

The Joint Communication provided both strategic views and practical measures to be taken to improve cybersecurity in the EU. Measures and key actions included:

- The full implementation of the NIS Directive and the blueprint;
- A permanent mandate of the EU Agency for Cybersecurity (ENISA) and a European cybersecurity certification framework, as a voluntary framework ensuring security in critical or high-risk applications, widely deployed digital products and IoT devices;
- Guidelines, guidance and best practice to support a harmonised implementation and transposition of the NIS Directive (the *'implementation toolkit'*);

[28] https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52013PC0048
[29] https://www.europarl.europa.eu/doceo/document/TA-7-2014-0244_EN.html?redirect
[30] https://ec.europa.eu/commission/presscorner/detail/en/STATEMENT_14_68
[31] https://ec.europa.eu/commission/presscorner/detail/en/IP_17_3193
[32] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52017JC0450
[33] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2017:0477:FIN
[34] https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=COM:2017:476:FIN
[35] https://ec.europa.eu/transparency/documents-register/detail?ref=C(2017)6100&lang=en
[36] hereafter referred to as 'EU institutions'

- Reinforcing EU cybersecurity capability through a *network of cybersecurity competence centres* with a *European Cybersecurity Research and Competence Centre*[37] *at its heart*, focusing on "*making strategic investment decisions and pooling resources from the EU, its Member States and industry, supporting research and innovation, including large-scale research and demonstration projects in next-generation cybersecurity capabilities*";
- Facilitating cross-border access to electronic evidence, further developing Europol's forensic capacity, and boosting deterrence through a Directive on the "combatting of fraud and counterfeiting of non-cash means of payment"[38] [COM(2017) 489];
- Stepping up the political response by adopting the framework for a joint EU diplomatic response to malicious cyber activities[39] (the *'cyber diplomacy toolbox'*);
- Strengthening international cooperation on cybersecurity, through a *"a new Capacity Building Network and EU Cybersecurity Capacity Building Guidelines"* as well as fostering *"cooperation between EU and NATO"* through cyber defence exercises involving the EEAS and other EU and NATO bodies, including the Cooperative Cyber Defence Centre of Excellence[40] (CCDCOE) in Tallinn, Estonia;

The European Parliament resolution[41] of 12 March 2019 called *"on the Commission to assess the need to further enlarge the scope of the NIS Directive to other critical sectors and services that are not covered by sector-specific legislation"*.

On June 7th 2019, "Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (the '*Cybersecurity Act'*)"[42] was published in the Official Journal of the European Union (OJ L 151)[43] and entered into force on the 27th of June 2019. In summary the Cybersecurity Act[44]:

- strengthens ENISA by granting the agency a permanent mandate, reinforcing its financial and human resources and generally enhancing its role in helping the EU to achieve joint, high-level cybersecurity;
- establishes the first EU-wide cybersecurity certification framework, to ensure a common approach to cybersecurity certification in the EU's internal market and ultimately improve cybersecurity in a broad range of digital products (e.g. internet of things) and services;

As part of Europe's Recovery, to protect lives and livelihoods, the European Commission on January 29th 2020, has adopted its Work Programme[45] for 2020, setting out the actions the Commission will take in 2020 to turn the Political Guidelines of President **von der Leyen** "*into concrete initiatives that will then be negotiated and implemented in cooperation with the European Parliament, Member States and other partners"*[46]. These major initiatives were

[37] https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-competence-centre
[38] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52017PC0489
[39] https://data.consilium.europa.eu/doc/document/ST-10474-2017-INIT/en/pdf
[40] https://ccdcoe.org/
[41] https://www.europarl.europa.eu/doceo/document/TA-8-2019-0156_EN.html
[42] https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32019R0881
[43] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L:2019:151:TOC
[44] https://digital-strategy.ec.europa.eu/en/news/cybersecurity-act-strengthens-europes-cybersecurity
[45] https://ec.europa.eu/info/publications/2020-commission-work-programme-key-documents_en
[46] https://ec.europa.eu/commission/presscorner/detail/en/ip_20_124

grouped under six headline ambitions: *1) A European Green Deal, 2) A Europe fit for the digital age, 3) An economy that works for people, 4) A stronger Europe in the world, 5) Promoting our European way of life and 6) A new push for European democracy*.

According to the Work Programme, technologies used in critical sectors such as healthcare, energy, banking, and legal systems are meant to be reinforced by the development of robust cybersecurity measures. On this front, the Commission launched initiatives such as Digital Operational Resilience Framework for financial services[47] [COM(2020) 595 final] which was adopted in September 2020 and is preparing a Network code for the cybersecurity of cross border electricity flows due for adoption by the end of 2022[48].

In the adopted communication[49] [COM(2020) 37 final] the Commission also announced, that the strategy would be accompanied by *"the review of the Directive on Security of Network and Information Systems and a proposal for additional measures on Critical Infrastructure Protection"* aimed to be completed by the end of 2020.

Following that in May 2020, the Commission adopted a communication "Europe's moment: Repair and prepare for the next generation"[50] [COM(2020) 456 final], announcing a "*new Cybersecurity Strategy, which will look at how to boost EU-level cooperation, knowledge and capacity. It will also help Europe strengthen its industrial capabilities and partnerships, and encourage the emergence of SMEs in the field*". The communication also proposed "*a new €806.9 billion[51] recovery instrument, called Next Generation EU, embedded within a powerful and modern long-term EU budget*". In total, this European Recovery Plan will put € 1.85 trillion[52] to help kick-start our economy and ensure Europe bounces forward.

In its conclusions[53] of 9th of June 2020, the Council welcomed *"the Commission's plans to ensure consistent rules for market operators and facilitate secure, robust and appropriate information sharing on threats as well as incidents, including through a review of the Directive on security of network and information systems (NIS Directive), to pursue options for improved cyber-resilience and more effective responses to cyber-attacks, particularly on essential economic and societal activities, whilst respecting Member States' competences, including the responsibility for their national security"*.

Succeeding the European Agenda on Security (2015-2020), the Commission on July 24th 2020 issued a communication on the EU Security Union Strategy 2020-2025[54] [COM(2020) 605], underlying that "*Cyber-attacks and cybercrime continue to rise. Security threats are also becoming more complex: they feed on the ability to work cross-border and on inter-connectivity; they exploit the blurring of the boundaries between the physical and digital world; they exploit vulnerable groups, social and economic divergences. Attacks can come at a moment's notice…and what happens outside the EU can have a critical impact on security inside the EU*".

[47] https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=COM:2020:595:FIN

[48] As empowered by Regulation (EU) 2019/943 on the internal market for electricity. Preparatory work was finalised in September 2019, an informal drafting process is ongoing

[49] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0037

[50] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2020:456:FIN

[51] https://ec.europa.eu/info/strategy/recovery-plan-europe_en

[52] Unless indicated otherwise, amounts are expressed in constant 2018 prices

[53] https://www.consilium.europa.eu/media/44389/st08711-en20.pdf

[54] https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1596452256370&uri=CELEX:52020DC0605

Then on December 16th 2020, the European Commission and the High Representative of the Union for Foreign Affairs and Security Policy issued a Joint Communication to the European Parliament and the Council[55] [JOIN(2020) 18 final] presenting the updated EU Cybersecurity Strategy, stating that "*Improving cybersecurity is essential for people to trust, use, and benefit from innovation, connectivity and automation, and for safeguarding fundamental rights and freedoms, including the rights to privacy and to the protection of personal data, and the freedom of expression and information"*. The Commission proposed, among many things, review/reform the NIS Directive (or "NIS 2"), to review the legislation on the resilience of critical infrastructure[56], to come up with a new Directive on the resilience of critical entities, to build a network of Security Operations Centres across the EU (that will "*serve as a real cybersecurity shield for the EU*"), and to support the improvement of existing centres and the establishment of new ones, as well as to deliver the Joint Cyber Unit (to further coordinate cybersecurity operational capabilities across the EU) and additional measures to strengthen the EU cyber diplomacy toolbox. The updated strategy was in line with the Commission's priorities to make *"Europe fit for the digital age"* and to build a future-ready economy that works for the people.

[55] https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=JOIN:2020:18:FIN

[56] directive on resilience of critical entities

2 NIS Directive

The NIS Directive[57] ((EU) 2016/1148), represents the first piece of EU-wide legislation on cybersecurity and provides legal measures (norms) to boost the overall level of cybersecurity in the EU, with a focus on protecting critical infrastructure by covering several key sectors and digital service providers (DSPs) and how these shall be supervised.

The directive's objective is to "*achieve a high common level of security of network and information systems within the EU so as to improve the functioning of the internal market*" (Article 1) and was designed to[58]: a) improve the EU MS national cybersecurity capabilities, b) improve the cooperation between MS, and c) supervise the cybersecurity of critical sectors.

On October 4th 2017 the Commission published a communication on "Making the most of NIS"[59] [COM(2017) 476 final/2] specifying that the third objective of the directive is to promote "*a culture of risk management and incident reporting among key economic actors, notably operators providing essential services (OES) for the maintenance of economic and societal activities and Digital Service Providers (DSPs)*". To achieve these objectives, the directive establishes the NIS Cooperation Group[60], and the network of Computer Security Incident Response Teams (CSIRTs)[61], ensuring the exchange of information on cybersecurity as well as the cooperation on specific cybersecurity incidents. Additionally a National Cybersecurity Strategy, a Computer Security Incident Response Team (CSIRT), and a National Competent Authority (NCA) were set by every MS, supporting risk information exchange and cooperation on security incidents.

To achieve its objectives, the directive provides for a number of measures[62] (see Table 1 and ENISA visual tool[63]).

Table 1. Objectives of the NIS Directive and MS obligations

Objective	Measures
Improved cybersecurity capabilities at national level	✓ Each MS will adopt a **national strategy on the security of network and information systems** defining the strategic objectives and appropriate policy and regulatory measures. ✓ MS will designate one or more **national competent authorities** (NCA) for the NIS Directive, to monitor the application of the Directive at national level. ✓ MS will designate a single point of contact, which will exercise a liaison function to ensure cross–border cooperation with the relevant authorities in other MS and with the cooperation mechanisms created by the Directive itself.

[57] https://eur-lex.europa.eu/eli/dir/2016/1148/oj

[58] https://www.enisa.europa.eu/topics/nis-directive

[59] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52017DC0476

[60] https://digital-strategy.ec.europa.eu/en/policies/nis-cooperation-group

[61] https://www.enisa.europa.eu/topics/csirts-in-europe/csirts-network

[62] https://ec.europa.eu/commission/presscorner/detail/en/MEMO_16_2422

[63] https://www.enisa.europa.eu/topics/nis-directive/nis-visualtool

	✓ MS will designate one or more **Computer Security Incident Response Teams** (CSIRTs)[64].
Increased EU-level cooperation	✓ Establish the NIS Cooperation Group[65], to support and facilitate strategic cooperation and the exchange of information among MS and to develop trust and confidence. The functioning of the group is based on Commission Implementing Decision (EU) 2017/17966 published February 2nd 2017, that lays down the procedural arrangements. According to Article 11 (2) of the Directive "The group is composed of representatives of the MS, the Commission and ENISA". ✓ Establish a network of the national CSIRTs[67], in order to contribute to the development of confidence and trust between the MS and to promote swift and effective operational cooperation. According to Article 12 (1) of the Directive "*The CSIRTs network shall be composed of representatives of the Member States' CSIRTs and CERT-EU*[68]*. The Commission shall participate in the CSIRTs network as an observer. ENISA shall provide the secretariat and shall actively support the cooperation among the CSIRTs*"
Risk management and incident reporting obligations for operators of essential services and digital service providers	Member States should **identify operators of essential services** (OES) by applying these criteria: 1. The entity provides a service which is essential for the maintenance of critical societal/economic activities; 2. The provision of that service depends on network and information systems; and 3. A security incident would have significant disruptive effects on the provision of the essential service. Identified OES will have to take appropriate security measures and to notify serious incidents to the relevant national authority. Important digital services[69], referred to in the Directive as "digital service providers" (DSPs), are also required to take appropriate security measures (technical and organisational) and to notify substantial incidents to the competent authority. The Directive identifies OES in the following seven sectors: 1. Energy: electricity, oil and gas

[64] Their role is described in Article 12 of the NIS Directive

[65] Established under Article 11 of the NIS Directive

[66] https://eur-lex.europa.eu/legal-content/GA/TXT/?uri=CELEX:32017D0179

[67] Established under Article 12 of the NIS Directive

[68] https://cert.europa.eu/

[69] 'digital service' means a service within the meaning of point (b) of Article 1(1) of Directive (EU) 2015/1535 of the European Parliament and of the Council which is of a type listed in Annex III of the NIS Directive

	2. Transport: air, rail, water and road 3. Banking: credit institutions 4. Financial market infrastructures: trading venues, central counterparties 5. Health: healthcare settings 6. Water: drinking water supply and distribution 7. Digital infrastructure: internet exchange points, domain name system service providers, top level domain name registries The Directives covers the following three digital services: 1. Online marketplaces (which allow businesses to set up shops on the marketplace in order to make their products and services available online) 2. Cloud computing services 3. Search engines Figure 3 illustrates the OES and DSPs that are within the scope of the NIS Directive

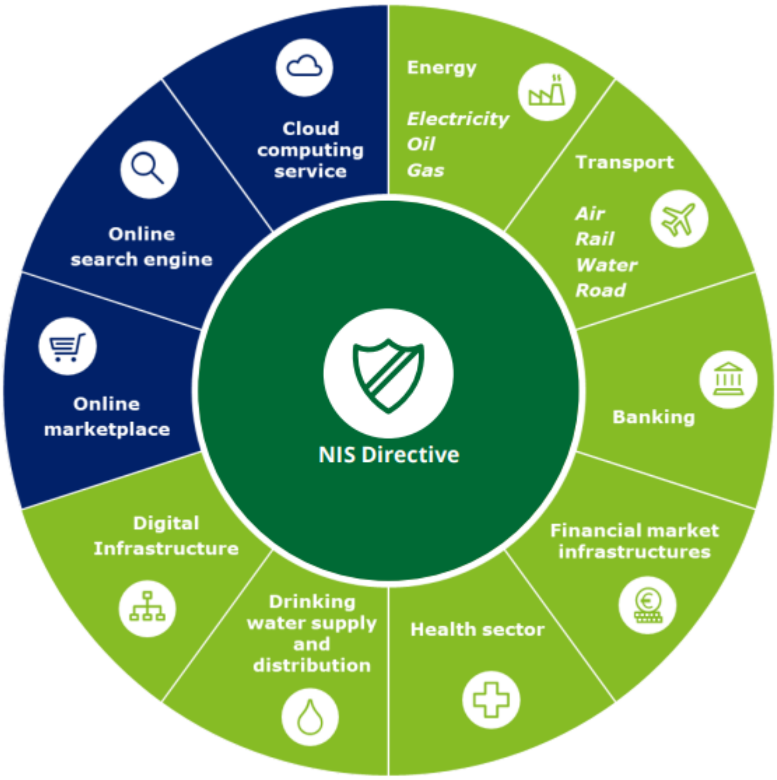

Figure 3. Sectors of OES and types of digital services in the scope of the NIS Directive[70]

The NIS Directive consists of 27 articles. Articles 1-6, sets out its subject matter and scope, and the main definitions (Article 4), identifies operators of essential services (Article 5) and

[70] https://www2.deloitte.com/content/dam/Deloitte/be/Documents/risk/Deloitte%20Belgium_Developing%20cybersecurity%20capabilities.pdf

defines the meaning of a “significant disruptive effect'”(Article 6). Articles 7-10, describe the national frameworks on the security of network and information systems that need to be adopted by each MS. Articles 11-13, set out the cooperation mechanisms, including the establishment of the Cooperation Group (Article 11) and the network of the national CSIRTs (Article 12). Articles 14–18 defines security requirements and incident notification for operators of essential services and digital service providers, respectively. Articles 19-20, encourage the use of European or internationally accepted standards (Article 19) and the process of voluntary notification (Article 20) on incidents having a significant impact on the continuity of the services provided by entities which have not been identified as operators of essential services and are not digital service providers. Finally articles 21–27 list the Directive's final provisions.

The NIS Directive also includes 3 Annexes. Annex I lists the “*Requirements and tasks of Computer Security Incident Response Teams (CSIRTs)*'. Annex II lists the *“Types of entities for the purposes of point (4) of Article 4”*, and identifies OES in the aforementioned seven sectors. Annex III lists the *“Types of digital services for the purposes of point (5) of Article 4*”, refers to digital services and covers the aforementioned three digital services.

2.1 Implementation Timeline

As already mentioned the NIS Directive entered into force in August 8th 2016, while the national transposition by the EU MS into national laws happened on May 9th 2018.

By 2020, all Member States had fulfilled their obligation[71], by fully transposing the directive into their national legislation, as well as preparing their national cybersecurity strategies and identifying their OES. As shown in Figure 4 the NIS Cooperation Group has also established its work programme and is operational.

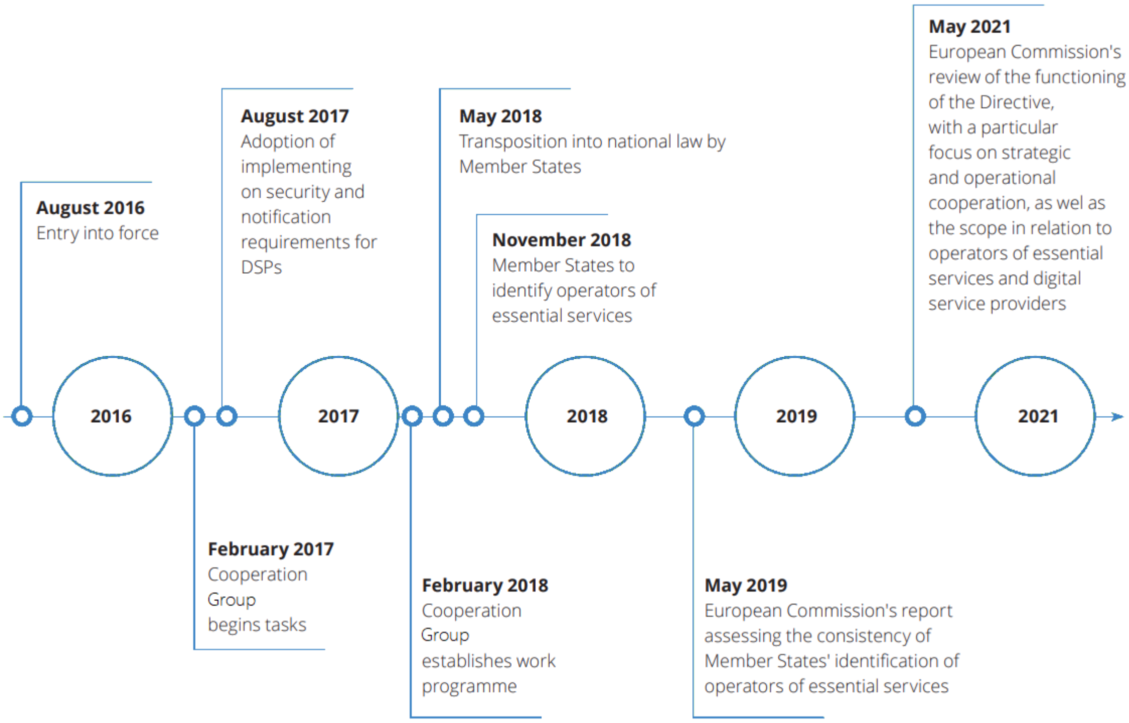
August 2016
Entry into force
August 2017
Adoption of implementing on security and notification requirements for DSPs
May 2018
Transposition into national law by Member States
November 2018
Member States to identify operators of essential services
May 2021
European Commission's review of the functioning of the Directive, with a particular focus on strategic and operational cooperation, as wel as the scope in relation to operators of essential services and digital service providers
2016
2017
2018
2019
2021
February 2017
Cooperation Group begins tasks
February 2018
Cooperation Group establishes work programme
May 2019
European Commission's report assessing the consistency of Member States' identification of operators of essential services

Figure 4. Planned NIS Directive timeline (Based on the Commission's table[62] and information)

[71] https://digital-strategy.ec.europa.eu/en/policies/nis-transposition

The NIS Cooperation Group has met 24 times[72]. Since the 15th meeting the agenda includes a sessions on reviewing NIS and the state of play on NIS 2. During the last meeting MS discussed "*where they expect the biggest challenges for the future work of NIS Cooperation Group (after publication of NIS 2 Directive)*". Among the key outputs of the NIS Cooperation Group, there are non-binding guidelines to the EU Members States to allow effective and coherent implementation of the NIS Directive across the EU and to address wider EU cybersecurity policy issues. Since its establishment, the Group has published several documents[73].

Regarding the CSIRTs network was established on the basis of Article 12 of the NIS Directive, and is composed of representatives of the MS CSIRTs and CERT-EU. According to the ENISA's CSIRTs Interactive Map[74] the number of members by MS ranges from 78 in Spain to 1 in Bulgaria. The 1st CSIRT Network Meeting was held in Malta between 22nd and 23rd of February 2017. Overall the CSIRTs network has met 18 times, in different MS, with the objective *"to continue developing operational cooperation capabilities in the EU as defined by the Network and Information Security Directive"*[75]*.*

2.2 Implementation Challenges and Issues

According to Article 23 (2) of the NIS Directive *"The Commission shall periodically review the functioning of this Directive and report to the European Parliament and to the Council. For this purpose … the Commission shall take into account the reports of the Cooperation Group and the CSIRTs network on the experience gained at a strategic and operational level… In its review, the Commission shall also assess the lists contained in Annexes II and III, and the consistency in the identification of operators of essential services and services in the sectors referred to in Annex II. The first report shall be submitted by 9 May 2021."*

Following this obligation on October 28th 2019 the Commission published a report to the European parliament and the council *"assessing the consistency of the approaches taken by Member States in the identification of operators of essential services"*[76] [COM(2019) 546 final]. Due to their important role for the economy and society as a whole, operators of essential services must demonstrate a particularly high level of resilience against cyber-incidents.[76] The report assessed information provided by MS between November 2018 and September 2019. According to the report: "*At the date of publication of this report 23 Member States had submitted all the data required under Article 5(7)"* while the "*other 5 Member States (Austria, Belgium, Hungary, Romania and Slovenia) have only partially provided data*".

The OES identification in Member States in numbers was as follows:

- The numbers of services identified by MS as covered by Annex II of the NIS Directive vary greatly between MS. With an average of 35 services per MS, the number of identified services ranges from 12 (in Hungary) to 87 (in Poland);
- The total numbers of OES reported by MS range from 20 to 10 897 with an average of 633 OES per MS, while Austria, Belgium and Slovenia counting 0, Portugal 1250 and Finland 10987[77];

[72] https://digital-strategy.ec.europa.eu/en/library/nis-cooperation-group-meetings-agendas

[73] https://digital-strategy.ec.europa.eu/en/policies/nis-cooperation-group

[74] https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-inventory/certs-by-country-interactive-map

[75] https://www.enisa.europa.eu/events/18th-csirts-network-meeting

[76] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52019DC0546

[77] Due to Finland's identification methodology, a very large number of OES were identified in the health sector

- 11 out of 28 MS have identified essential services in sectors not falling under the scope of Annex II of the Directive. Out of these 11 MS, 7 have identified a total of 157 OES providing services not covered by the types of entities in Annex II.

Although the NIS Directive had considerably contributed to the improvement of the MS cybersecurity capabilities and the level of protection of network and information systems throughout the EU, a number of issues relating to its implementation were identified, resulting in improvement recommendations. As identified by the report[76]:

- MS have developed different methodologies regarding the overall approach to the identification of OES, including the definition of essential services and the setting of thresholds, which "*can have a negative impact on the consistent application of the NIS provisions across the Union with possible consequences for the well-functioning of the internal market and the effective handling of cyber-dependencies*". The Commission suggested that *"A further alignment of thresholds on EU level could help alleviate this problem";*
- MS have "*diverging interpretations"* as to what constitutes an essential service under the NIS Directive, with MS *"applying different levels of granularity"*, making it *"difficult to compare the lists of essential services in the whole EU"*;
- *"The scope of the Directive risks being fragmented, with some operators being exposed to additional regulation (as they have been identified by their respective MS) while others providing similar services remaining excluded (as they have not been identified)"*. The Commission suggested that *"to address these inconsistencies, further work based on the experience of Member States could lead to a more aligned list of essential services"*;

The Commission has identified several national actions that could help alleviate the highlighted problems. In addition to national actions, additional measures that could potentially result in increased consistency, include[76]:

- Strengthening the role of the NIS Cooperation Group in order to promote a common understanding on how to implement the directive in a more consistent manner;
- The Cooperation Group should review its reference document on the modalities of the consultation process in cases with cross-border impact and agree on a consistent interpretation of the scope, objectives and procedures of such exercise. This is necessary to address the cross-border consultation procedure when it comes to identifying operators that are providing essential services in more than one MS;

The Commission preliminary conclusion was that "*while the NIS Directive has contributed to increased and improved risk management practices of operators in critical sectors, its implementation proved difficult, resulting in a considerable degree of fragmentation across the Union internal market, when it comes to the identification of OES, partly due to the design of the Directive and partly due to the different implementation methodologies used by the MS*"[76].

On a similar note, a briefing paper[78] by the European Court of Auditors (ECA), published March 19th 2019, identified multiple challenges to strengthen EU's cybersecurity and its digital autonomy. The briefing paper provided an overview of the EU's complex and uneven

[78] https://www.eca.europa.eu/en/Pages/DocItem.aspx?did=49416

cybersecurity policy landscape and identified major challenges to effective policy delivery. The majority of research was carried out between April and September 2018. Based on the analysis, the ECA grouped the identified challenges into four broad clusters: (i) the policy and legislative framework; (ii) funding and spending; (iii) building cyber-resilience; and (iv) responding effectively to cyber incidents.

In relation to the NIS Directive, the ECA briefing paper pointed out that:

- Despite a drive for greater coherence, **the legislative framework for cybersecurity remains incomplete**. Fragmentation and gaps hamper achievement of the overall policy objectives and lead to inefficiencies;
- The **balance of responsibilities** between users and providers of digital products, and certain aspects left **unaddressed** by the NIS Directive;
- It is **difficult to form a comprehensive picture of funding and spending**, in both the public and private sectors, in the absence of clear data owing to cybersecurity's cross-cutting nature. Investments must be aligned with strategic goals, which calls for the scaling up of investment levels and its impact;
- The EU's relevant cybersecurity agencies ENISA, Europol's EC3, and CERT-EU – are facing **resourcing challenges** which entails difficulties in attracting and retaining talents;
- While the NIS Directive's objective is to achieve a high level of security across the EU, it explicitly focuses on achieving minimum, not maximum, harmonisation[79]. Gaps will continue to emerge as the cyber-landscape evolves, while existing legislation is not consistently transposed by Member States;
- The **lack of** a coherent, international cybersecurity **governance framework** impairs the international community's ability to respond to and limit cyberattacks;
- There are still too **few legal and economic incentives for** organisations to notify and **share** information about incidents. Fearing reputational damage, many organisations still prefer to handle cyberattacks discretely or to pay off the perpetrators;
- Despite a foundation for strategic and operational cooperation at the EU level, **coordination in general is "insufficient"**[80];
- The NIS Directive's **cooperative structures**, were **not designed** to support the development of "cutting edge" solutions;
- National and sectorial **Information Sharing and Analysis Centres** (ISACs) already exist in many MS, but **at the European level**, they are still **relatively limited**[81]. They come with a number of challenges that will need to be overcome if they are to contribute to helping implement the NIS Directive and building security capabilities at a European-wide level[82];
- Although the NIS Directive in Articles 14–18 defined the security and incident notification requirements for OES and DSPs, respectively, following the 2017

[79] According to Article 3

[80] https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=JOIN%3A2018%3A16%3AFIN

[81] For example, the European Financial Institutes ISAC includes financial sector representatives, national CERT's, law enforcement agencies, ENISA, Europol, European Central Bank, the European Payments Council and the European Commission

[82] https://www.enisa.europa.eu/publications/information-sharing-and-analysis-center-isacs-cooperative-models

Wannacry attacks, the Commission concluded that the **CSIRT network** system was **"not yet fully operational"**[83];

- OES in certain sectors (for example the financial and banking sectors) have **multiple notification obligations** (including to consumers) under existing EU regulations, which may impair the efficiency of the process. It is therefore important to streamline these obligations since, aside from constituting an unnecessary administrative burden, such heterogeneity might lead to fragmented reporting;
- The NIS Directive **failed to address** the "limited" EU's capacity to respond to cyberattacks at the operational and political level in the event of a large-scale, cross-border incident;
- The NIS Directive aims to enhance readiness in key sectors responsible for critical infrastructure. However, **not all sectors are covered**[84], which "reduces the effectiveness of the strategy"[85]: of particular concern in this regard is protecting the democratic integrity of elections from interference in electoral infrastructure and disinformation campaigns, especially in view of European Parliament elections. Despite this, the Cooperation Group has developed practical guidance on election technology security to support public authorities
- Improving skills and awareness across all sectors and levels of society is recommended in order to overcome the growing global skills shortfall. This must be flanked by better information exchange and coordination between the public and private sectors;
- Rapid detection and response as well as protection of critical infrastructure and societal functions, remain key challenges for an effective EU-side response to cyber-attacks;

[83] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52017DC0354

[84] For example, public administration, the chemical and nuclear industries, manufacturing, food processing, tourism, logistics and civil protection

[85] Finding 3 of the SWD(2017)295

3 NIS 2 Directive – A high common level of cybersecurity in the EU

During the last few years, more sophisticated, powerful and devastating cyber-attacks put again EU's cyber health at risk. The catastrophic results that we have witnessed, confirmed the hard way that EU's cyber defence needs at least a lifting.

Since the adoption of the NIS Directive, back in 2016, "*which paved the way for a significant change in relation to the institutional and regulatory approach to cybersecurity in many Member States*"[86], the threat landscape has changed considerably. In addition, as already presented in section 2 its implementation and transposition by the EU MS into national laws revealed inherent flaws. Furthermore, during the COVID-19 crisis we have witnessed a sudden increase of the EU economy dependence on information technology with more sectors and services being increasingly interconnected. As a result disruptions, to one entity or sector, can have cascading effects, potentially resulting in far-reaching and long-lasting negative impacts in the delivery of services across the whole internal market.[87]

The global COVID-19 pandemic has confirmed the need to continually improve EU cyber-resilience and response to cyber incidents, particularly for those who operate on critical sectors such as healthcare, energy, banking, and legal systems.

To address these challenges, the NIS Directive scope should be updated and expanded to meet current risks and future challenges.

Cybersecurity is a priority as reflected in the EU's next long-term budget (2021-2027), notably the Digital Europe Programme and Horizon Europe, as well as the Recovery Plan for Europe. MS are encouraged to make full use of the EU Recovery and Resilience Facility to boost cybersecurity and match EU-level investment. The objective is to reach up to €4.5 billion of combined investment from the EU, the Member States and the industry, notably under the Cybersecurity Competence Centre and Network of Coordination Centres, and to ensure that a major portion gets to SMEs.[88]

3.1 Proposal Preparation

As already discussed, the Commission in the 2020 Work Programme[45] announced that the NIS Directive review will be completed by the end of 2020 something that was confirmed in the adjusted 2020 Work Programme[89] Annex I. The revision falls under the Commission's initiative to make *"A Europe fit for the digital age"*, and according to the programme aimed to "*further strengthen overall cybersecurity in the Union*". Despite the obligations of Article 23 (2) of the NIS Directive, to review the functioning of the Directive and submit a report to the European Parliament and the Council by May 9th 2021 the revision was *"further justified by the sudden increase in the dependence on information technology during the COVID-19 crisis"*.

To support the proposal and collect evidence, the Commission ran an Open Public Consultation (OPC), launched stakeholder interviews, country visits, workshops and surveys, carried out a study on NIS investment and an impact assessment, and drew up a roadmap.

[86] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2020:823:FIN

[87] https://digital-strategy.ec.europa.eu/en/library/proposal-directive-measures-high-common-level-cybersecurity-across-union

[88] https://ec.europa.eu/commission/presscorner/detail/en/IP_20_2391

[89] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0440&from=EN

3.1.1 Combined Evaluation Roadmap and Impact Assessment

In order to inform citizens and stakeholders and allow them to provide feedback on the intended Commission's initiative to review the NIS Directive, on June 25th 2020, the Commission published a "Combined Evaluation Roadmap/Inception Impact Assessment"[90]. The evaluation will *"assess the effectiveness, efficiency, coherence, relevance and EU added value of the NIS Directive taking into account the constantly evolving technological and threat landscape"*, focusing on the "*impact of the NIS Directive on increasing the level of national cybersecurity capabilities and the capacity to mitigate growing security threats to network and information systems used to provide essential services in key sectors*".

The Commission also stated that: *"Depending on the results from the evaluation of the functioning of the NIS Directive, an open public consultation and an impact assessment, the Commission might propose measures aimed at enhancing the level of cybersecurity within the Union".*

In order to ensure consistency and coherence with related Union legislation, the NIS Directive review will take into account the following Commission initiatives in particular: a) the review of the European programme for critical infrastructure protection; b) the initiative on a Digital Operational Resilience Act (DORA) in the financial sector, and c) the initiative on a network code on cybersecurity with sector specific rules for cross-border electricity flows.

3.1.2 Open Public Consultation

The Open Public Consultation (OPC)[91] was used for the evaluation and impact assessment of the NIS Directive. It was launched on July 7th 2020 aiming to "*collect views on its implementation and on the impact of potential future changes*" from different stakeholder groups such as MS competent authorities, OES, DSPs, researchers and academia, cybersecurity industry professionals and citizens. The consultation closed on October 2nd 2020. According to the "Summary Report"[92] 206 replies were collected. The findings of the OPC revealed that:

a) **all specific objectives of the Directive are still relevant**, and even very relevant, while the most relevant objective of the three is to promote a culture of security across all sectors vital for the EU economy and society (77.2%);
b) the **cyber threat level has increased since 2016** (88.4%), with SMEs being rated on average as rather poorly prepared in dealing with the evolving cybersecurity threats;
c) **common EU rules are needed to address cyber threats**, given that cyber risks can propagate across borders at high speed. Additionally, mandatory **sharing** of cyber-risk related **information** between national competent authorities across the EU, would contribute to a high level of joint situational awareness on cyber risks;
d) the **NIS Directive sectorial scope** should **extend** to include further sectors and types of digital services at risk of cyber threats, including **public administrations and data centres**.

[90] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=PI_COM:Ares(2020)3320999&from=EN

[91] https://digital-strategy.ec.europa.eu/en/news/eu-cybersecurity-commission-launches-public-consultation-nis-directive

[92] https://digital-strategy.ec.europa.eu/en/library/summary-report-open-public-consultation-directive-security-network-and-information-systems-nis

Overall, the most frequently mentioned sectors were (in order of importance):

- Public services – e-government, e-health, and emergency services (police, fire);
- Telecommunications;
- Energy and electricity;
- Cloud and DNS providers;
- Manufacturers of electronic hardware and software;
- Traditional media online;
- Social media platforms;
- Postal and courier services;
- Data centres;
- Banking, finance, and insurance;
- Food production and waste management

When asked about digital service providers, the most reported types of services were:

- Data centres;
- Social media platforms (social networks);
- Manufacturers and suppliers of important hardware and software;
- Providers of communication and navigation services;
- Service hosting providers;
- All digital or internet products and services;
- Application service providers (SAAS) and stores;
- Online collaboration environments/tools, including video conferencing;
- ICT security services

e) the **"light-touch" regulatory approach applied to DSPs is no longer justified and should not be maintained** (39.8%). Conversely, only 27.7% of the OPC respondents thought the regulatory "light-touch" for DSPs should be maintained, Furthermore, almost half (48.5%) of respondents agreed that **the cross-border nature of the NIS Directive's operations justified the harmonised treatment of DSPs by comparison to OES**;

f) the NIS Directive **impacted national competent authorities and CSIRTs**, with the strongest impact regarding cooperation with OES and DSPs;

g) the **current approach does not ensure that all relevant OES are identified across the Union** (37.4% disagrees and 6.3% strongly disagrees). In the same vein, above 40% of respondents disagree or **strongly disagree with the statement that the identification process has contributed to the creation of a level playing field for companies from the same sector across the MS**. Amongst the OPC participants the most often discussed topic was the **lack of harmonised approach resulting in significant inconsistencies in the way that Member States draw up lists of OES**, divergent applications of the thresholds and different applications of the *lex specialis* principle. Concerning the identification of OES, Member States' approaches often show strong heterogeneity. To that end, it was suggested to **establish** a common set of **criteria** to **ensure a harmonised process of identification of OES**. When it comes to the identification of operators of essential services, the setting of security requirements and the rules governing incident notification responses indicated that it **can have a strong negative impact on the level playing field for companies in the internal market** and potentially render entities more vulnerable to cross-border cyber-threats.

Responses related to the context of OES identification refer to the **need to cover the public sector** by the Directive considering the magnitude of data they treat and potential impacts of a cyberattack. In light of the COVID-19 pandemic, the **pharmaceutical sector** has been identified. Additionally, a small share of OPC answers covered the **transport sector**. According to these, the **automobile industry** should be covered by the NIS Directive. **Food supply** and **manufacturing** have also been mentioned by a few OPC participants;

h) **small companies appear to be most vulnerable** as they lack the financial and human capacity, staff and awareness to provide adequate cybersecurity to their operation. **A large share of small companies do not perceive cyber threats as a risk to them or find that they do not face the same level of risk presented by large or medium sized companies**. Furthermore, there appears to be an agreement that discrepancy exists related to level of resilience and the risk-management practices both by size of the enterprise and the (sub-) section/sector in which it operates. These point out that in some sectors (i.e. banking, energy) there is a strong legislative framework and high level of cybersecurity maturity. Finally, most of the OPC respondents (60.2%) either agreed or strongly agreed that European legislation should require MS to put in place frameworks to raise awareness of cyber threats among SMEs and to support them in facing cyber threats;

i) imposing **security requirements on OES** has a high impact in terms of cyber resilience, however the **lack of harmonisation limits its impact**. On the contrary given the "light-touch" regulatory approach applied to DSPs, imposing maximum security requirements it has a minimal impact on them that also depends on the country. In countries where the maturity was initially low, the NIS had more impact. Furthermore, **improved alignment** between the various approaches adopted in different MS **would be helpful** because the wide discretion that is given to MS in identifying OES and establishing security requirements leads to incongruity between the different MS. **Outcome-focused measures,** as opposed to more prescriptive requirements, are **required** in order to create sufficient common understanding of what is the regulatory obligation, as well as in order to provide the necessary incentives to organizations to pursue that compliance;

j) the differences in the definition of mandatory reporting of security incidents in the MS results in **different reporting obligations**. The lack of harmonisation of incident reporting requirements under various regulations and programs[93], has led to a **fragmented approach** and creates unnecessary regulatory and compliance burden for OES and companies. Identifying the right authority to inform and the right information is also a heavy burden;

k) the **level of information-sharing** between MS **requires substantial improvement**. At the same time the simplification of reporting processes guaranteeing anonymity, as well as free and transparent access to anonymised reporting information was suggested as a means to motivate information sharing with cybersecurity authorities. Organisations in the financial and banking sectors indicated the highest level of information exchange, while the health sector was the lowest;

[93] Including PSD2, GDPR, NIS

l) the **effects of the NIS Directive have been achieved at a reasonable cost**, while the **NIS Directive had medium to high impact on the overall level of resilience against cyber-threats across the EU**;

m) the **coherence of the NIS Directive** was rated as being medium and high;

n) the level of **effectiveness of national policies on vulnerability discovery** was medium (24.8% of OPC respondents), while 15.5% of the respondents rated the national disclosure policies as low or very low. Regarding **coordinated vulnerability disclosure** a significant proportion of the respondents (48%, 99 out of 206 respondents) did not respond or indicated this did not apply to them or their organisation;

Similar findings can be found on the "Study to support the review of Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union (NIS Directive) – N° 2020-665"[94]. Based on the combined evaluation roadmap and impact assessment, setting out the scope and terms of reference of the NIS Directive evaluation, and following the Better Regulation Guidelines[95] the study suggests that *"the current NIS Directive was relatively successful to address some of the main market failures. However, a number of regulatory shortcomings together with a rapid evolving ecosystem suggest that there are pending issues in the current NIS Directive."* The most noticeable shortcomings of the NIS Directive and its policy context are:

- **Member States' preparation remains uneven and not sufficiently comprehensive**;
- There should be a **better alignment of requirements** in terms of reporting authorities, thresholds, timeframe, and penalties, between the NIS Directive and other EU legislation;
- The **level of cooperation at the EU level is below its potential**;
- MS diverge considerably in terms of standards and practices required on reporting, incident notification and the minimum-security requirements for OES and DSPs;
- **Increased interconnectedness and interdependencies in sectors not covered**;
- Too **broad discretion in defining the de facto scope of the Directive** in each MS and the national competence over DSPs remains unclear;
- Too **broad discretion in setting requirements** and unclear requirements;
- Vague provisions on enforcement and **light-touch on DSPs**;
- **Insufficient resources** for competent authorities set aside by Member States;
- **Cooperation** mostly on voluntary basis (of public authorities and private entities);

In summary[94], *"enhanced cybersecurity resilience is inherently a cross-border phenomenon to which the NIS Directive has largely contributed. However, the divergence across Member States in the implementation of the Directive coped with the evolving digital transformation of our society results in a fragmented regulatory policy landscape"*.

3.1.3 ENISA Study on NIS Investments

Regarding the nature of NIS investments across different sectors and countries, on December 11th 2020 ENISA released a report[96] on information security spending for network and

[94] https://op.europa.eu/en/publication-detail/-/publication/3b6ad641-d23c-11eb-ac72-01aa75ed71a1/language-en

[95] https://ec.europa.eu/info/law/law-making-process/planning-and-proposing-law/better-regulation-why-and-how/better-regulation-guidelines-and-toolbox_en

[96] https://www.enisa.europa.eu/publications/nis-investments/

information services (NIS) under the NIS Directive. The report presents the findings of a **survey of 251 organisations** (OES and DSPs) **across five EU MS** (France, Germany, Italy, Spain and Poland), examining their approaches to cybersecurity spending. The survey showed that **82%** of OES and DSPs find that the **NIS Directive has had a positive effect**. However, **gaps in investment still exist**, with "*with certain sectors investing in information security a percentage of their IT budget up to 5-6 times higher than that invested by sectors with the lower information security spending profiles*". When comparing organisations from the EU to their US counterparts, data shows that **EU organisations allocate on average 41% less to cybersecurity than their US counterparts**.

3.1.4 Impact Assessment

The report of the impact assessment (IA) conducted by the Commission on the Review of the NIS Directive[97] explored four different policy options for the NIS review: Option 0) baseline scenario – maintaining the status quo; Option 1) non-legislative measures to align the transposition; Option 2) limited changes to the NIS Directive for further harmonisation; and Option 3) systemic and structural changes to the NIS Directive. The analysis led to the conclusion that option 3 is the preferred one, as it would envisage a more fundamental shift of approach towards covering a wider segment of the economies across the EU, yet with a more focused supervision targeting proportionally big and key companies, while clearly determining the scope of application. It would also streamline and further harmonise companies' security-related obligations, create a more effective setting for operational aspects, establish a clear basis for shared responsibilities and accountability of the entities concerned, and incentivise information sharing.

As part of the review process required by Article 23(2) of the NIS Directive, an evaluation on the functioning of the NIS Directive was conducted. The conclusions of the evaluation were summarised into six main categories of findings, as shown in Table 2.

Table 2. Impact Assessment Report - Results of the evaluation of the NIS Directive

Evaluation finding 1: Increased interconnectedness and interdependencies in sectors not covered
The scope of the NIS Directive is too limited in terms of the sectors covered, mainly due to: i) increased digitalisation in recent years and a higher degree of interconnectedness; and ii) the scope of the NIS Directive no longer reflecting all digitalised sectors providing key services to the economy and society as a whole.
Evaluation finding 2: Scope not clearly determined by the NIS Directive and unclear national competence over digital service providers
This has led to a situation in which certain types of entities have not been identified in some Member States and are therefore not required to put in place security measures and report incidents. For example, five Member States have not identified any or only one OES in the health sector. At least eight Member States have not identified any OESs in the road transport subsector. At least four Member States have not identified any OESs in the railway subsector. Furthermore, the evaluation also identified that Member States are not fully aware of their potential competence for specific DSPs.
Evaluation finding 3: Divergent security and reporting requirements
The NIS Directive allowed wide discretion to the Member States when laying down security and incident reporting requirements for OESs. The evaluation shows that in some instances Member

[97] https://ec.europa.eu/transparency/documents-register/detail?ref=SWD(2020)345&lang=en

States have implemented these requirements in significantly different ways, creating an additional burden for companies operating in more than one Member State.
Evaluation finding 4: Ineffective supervision and enforcement
Evaluation finding 5: Uneven resources for competent authorities
The financial and human resources set aside by Member States authorities for fulfilling their tasks (such as NIS implementation supervision, OES identification and CSIRTs for incident handling) and consequently the different levels of proficiency in dealing with cybersecurity risks, vary greatly. This makes it challenging for certain competent authorities to effectively meet their obligations stemming from the NIS Directive and further exacerbates the differences in cyber-resilience among Member States.
Evaluation finding 6: Limited information sharing between Member States
Member States do not share information systematically with one another, while exchange of information throughout the cybersecurity lifecycle remains limited and mostly unstructured, with negative consequences to the effectiveness of the cybersecurity measures and the level of joint situational awareness at EU level. This is also the case for information-sharing among private entities and for the engagement between the EU level cooperation structures and private entities.

On October 23rd 2020 the IA report was submitted to the Regulatory Scrutiny Board (RSB) and the Commission on November 20th 2020 received its feedback[98] in the form of an overall positive opinion with reservations, while expecting the DG to rectify the following aspects:

- the problem analysis did not discuss sufficiently how enforcement has integrated cross-border spill-overs in risk assessments of entities in key sectors;
- the report did not explain what success would look like for the initiative;
- the list of options and justifications provided was not exhaustive, especially regarding the sectoral coverage; and
- the impact analysis lacks in depth, in particular regarding the costs assessment;

Among other things the RSB required from the Commission that the report should:

- reinforce the problem analysis to better focus on the problems the Directive aims to solve;
- clarify the difference between the ‘essential’ and ‘important’ sectors, what criteria were used to establish those categories, and whether alternative approaches were possible, and expand on whether the definition of sectoral coverage risks shifting the danger of exposure to other sectors. It should analyse how the choice of sectors can be made future proof;
- include a more complete set of options on reporting, supervision and crisis response;
- include ways to interact with the linked European critical infrastructure Directive, which is also under revision;
- strengthen the analysis of compliance costs, especially for medium-sized enterprises.

On February 11th 2021, the European Parliamentary Research Service (EPRS) released an appraisal[99] on the impact assessment report, suggesting that the NIS 2 proposal “appears to

[98] https://ec.europa.eu/transparency/documents-register/api/files/SEC(2020)430?ersIds=de00000000002602
[99] https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/662606/EPRS_BRI(2021)662606_EN.pdf

follow the general considerations of the IA. The preferred option identified in the IA is at the basis of the proposal. The monitoring provisions however do not appear to be described in the proposal in the same detail as they are laid out in the IA".

3.2 Key Elements of the NIS 2 Directive

On December 16th 2020, the European Commission issued a proposal[86] [COM(2020) 823 final] for a directive on measures for a high common level of cybersecurity across the Union (NIS 2), repealing the existing NIS Directive (NIS) that aims to address the deficiencies and limitations of the current NIS Directive, to adapt it to the current needs and make it future-proof.

To this end, the Commission proposal:

- extends the scope of the current NIS Directive *"to provide a comprehensive coverage of the sectors and services of vital importance for key societal and economic activities within the internal market"*;
- introduces "*a uniform criterion to determine the entities falling within the scope of application of the Directive, that consists of the application of the size-cap rule, whereby all medium and large enterprises, as defined by Commission Recommendation 2003/361/EC 15 , that operate within the sectors or provide the type of services covered by this Directive, fall within its scope"*; These are entities having at least 50 employees and a minimum turnover of €10m per year;
- eliminates the differentiation between operators of essential services and digital service providers, "*since it does not reflect the actual importance of the sectors or services for the societal and economic activities in the internal market*" and distinguishes two types of entities: Essential Entities (EE), and Important Entities (IE), detailed in Annex I and II respectively of the NIS 2 text;
- strengthens security requirements for "*all entities that are active in sectors covered by the NIS legal framework, based on the concept of risk management"* providing a minimum list of basic security measures that have to be applied;
- "*lays down a two-stage approach to incident reporting*", including content of the reports and timelines; it requires from affected companies to submit an initial report within 24 hours from when they first become aware of an incident, followed by a final report within one month;
- addresses "*cybersecurity risks stemming from an entity's supply chain and its relationship with its suppliers*" by requiring entities to "*appropriately manage supply chain and supplier related cybersecurity risks*". To this end "*the Cooperation Group involving relevant national authorities, in cooperation with the Commission and ENISA, should carry out coordinated sectoral supply chain risk assessments, as was already done for 5G networks following Recommendation (EU) 2019/534 on Cybersecurity of 5G networks[100]"*
- introduces more stringent supervisory measures for national authorities, by providing "*a minimum list of supervisory actions and means through which competent authorities may supervise essential and important entities*" as well as "*establish a differentiation of supervisory regime between essential and important entities*";
- introduces stricter enforcement requirements;

[100] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32019H0534

- harmonises sanctions regimes across Member States, through a "*a minimum list of administrative sanctions for breach of the cybersecurity risk management and reporting obligations*"; entities can be subject to fines up to €10 million or 2% of their total turnover worldwide, whichever is higher (the same as a GDPR fine for a less serious violation);
- enhances the role of the Cooperation Group in order to *"support and to facilitate strategic cooperation and the exchange of information among Member States*" and to "*react to changing and new policy priorities and challenges*" as well as shaping strategic policy decisions on emerging technologies and new trends;
- lays down obligations on cybersecurity information sharing, increases and improves information sharing and cooperation between Member State authorities;
- enhances operational cooperation, by establishing a network of the national CSIRTs;
- establishes the European Cyber Crises Liaison Organisation Network (EU - CyCLONe) *"to support the coordinated management of large-scale cybersecurity incidents and crises and to ensure the regular exchange of information among Member States and EU institutions"*;
- establishes a "*framework for Coordinated Vulnerability Disclosure*", that "*specifies a structured process through which vulnerabilities are reported to organisations in a manner allowing the organisation to diagnose and remedy the vulnerability before detailed vulnerability information is disclosed to third parties or to the public*" while ENISA establishes and maintains a European vulnerability registry;

3.3 Implications and Challenges for System and Infrastructure Security

The NIS 2 Directive, has been recently adopted (November 10th 2022) by the European Parliament responding to the evolving threat landscape and takes into account the digital transformation, which has been accelerated by the COVID-19 crisis.

Shortly after on the 14th of December 2022 the Directive has been published in the Official Journal of the European Union (OJ L 333/80)[101] entering into force on the 16th of January 2023, improving cybersecurity risk management and introducing reporting obligations across sectors such as energy, transport, health and digital infrastructure. Member states must incorporate the provisions of the NIS 2 Directive into their national laws, by September 2024.

The NIS 2 **strengthens the cybersecurity requirements** imposed on public and private entities, **addresses security of supply chains and supplier relationships**, includes **incident reporting obligations** for essential and important entities in EU and introduces **accountability of top management** for non-compliance with the NIS 2 requirements.

Operators of essential entities, operating in key sectors such as healthcare, energy and transport, will be proactively supervised, while operators of important entities such as digital providers, manufacturers of certain critical products and postal and courier service providers will be subject to a reactive supervisory regime, whereby supervision is triggered by indications of an incident.

Regarding the healthcare sector the NIS 2 Directive includes new requirements, notably for actors in the medical devices and pharmaceutical field, given the increasing security threats that arose during the COVID-19 pandemic. New types of entities are added while, medical

[101] https://eur-lex.europa.eu/eli/dir/2022/2555

device and in vitro diagnostic medical devices manufacturers might be considered important entities. Essential entities now include EU reference laboratories, entities carrying out R&D activities of medicinal products, entities manufacturing basic pharmaceutical products and preparations manufacturers of medical devices considered as critical during a public health emergency[102].

In the financial sector additional requirements for risk management frameworks in the financial sector are covered by the European Commission's Digital Operational Resilience Act (DORA) that overlaps with the NIS 2 Directive and will have a similar implementation date in H2 2024.

3.3.1 Encryption

The NIS 2 Directive in recital 98 emphasises the need to "*use end-to-end encryption"* and *"where necessary, it should be mandatory for providers of public electronic communications networks or of publicly available electronic communications services, in accordance with the principles of security and privacy by default and by design for the purposes of this Directive*".

Although cryptographic methods strengthen our trust in digital communication tools, the importance for competent authorities to gain access to electronic evidence in order to conduct their investigations and bring criminals to justice, while protecting victims and ensuring security, could weaken cryptographic procedures. Weakening of encryption can negatively affect Europe's digital sovereignty and could set a precedence for authoritarian regimes. Therefore, national authorities should strictly oppose any technical solutions, such as backdoors or master key, as it would weaken encryption in the EU.

Europe needs not fewer, but more trustworthy IT solutions to reap the benefits of the digital transformation in administration, industry and society. To this end, European legislators should be proponents of strong encryption and should increasingly promote the development of post-quantum cryptography procedures to accommodate future requirements for secure communication.[103]

3.3.2 Scope (Article 2 in conjunction with Annex I+II)

The NIS 2 Directive concerns only medium and large companies. Indeed, Article 2 introduces a notion of "*the size-cap rule, whereby all entities which qualify as medium-sized enterprises under Article 2 of the Annex to Commission Recommendation 2003/361/EC (5), or exceed the ceilings for medium-sized enterprises provided for in paragraph 1 of that Article, and which operate within the sectors and provide the types of service or carry out the activities covered by this Directive fall within its scope*".

However, there are sectors subject to other cybersecurity legislation that may complement the NIS 2 Directive, or even supersede it. It is therefore important for entities to be aware if they are affected by any other legislation.

[102] https://www.law.kuleuven.be/citip/blog/the-nis2-proposal-which-regulatory-challenges-for-healthcare-cybersecurity/

[103] https://issuu.com/bdi-berlin/docs/20211129_position_bdi_nis_2_directive_itre-comprom

Entities can look for guidance in the impact assessment report[97] that accompanies the NIS 2 proposal (PART 3/3 page 46), outlining that:

- in the financial sector, the DORA (Digital Operational Resilience Act) regulation, adopted on 24 September 2020, is "*lex specialis in relation with the NIS Directive, setting out consolidated, simplified and upgraded ICT risk requirements throughout the financial sector*";
- in the energy sector, the Risk Preparedness Regulation complements the NIS Directive. The same applies to Regulation (EU) 2017/1938 concerning measures to safeguard the security of gas;
- in the transport sector, several European initiatives are mentioned; and
- as for the electronic communication networks and services, the European Electronic Communications Code (EECC) is widely discussed.

3.3.2.1 Aviation Sector

The inclusion of aviation as an essential service and the manufacturers of aviation parts as important entities, might introduce redundant regulations for the same subject area. The reason is that the aviation sector is highly regulated by the EU Member State Civil Aviation Authorities and the European Union Aviation Safety Agency (EASA) that has recently published Opinion 03/2021[104] to efficiently contribute to the protection of the aviation system from information security risks, and to make it more resilient to information security events and incidents. Consequently organisations would be required to duplicate efforts to demonstrate their security, increasing business operational frictions and reducing the competitiveness of European aviation industry. At the same time competent authorities for EASA Part-IS and competent authorities for NIS 2 may disagree on acceptable measures making it challenging for organisations to find cost effective and mutually acceptable solutions. Finally, the unique operational constraints of the aviation industry, resulting from the extensive safety regulations, may prohibit some standard responses expected by security agencies leading to infringements of NIS 2.

3.3.2.2 Cloud Computing Service Providers

Regarding the cloud computing service providers, the term (Annex I No. 8) is too wide and imprecise. As a result it includes not only providers of distributed storage and processing capacities, but also software providers who offer storage in a cloud in connection with their software products. Furthermore, the broad definition together with the further virtualisation of information technology, could lead to an increasing number of services falling into this category.

3.3.2.3 Online Marketplace Providers

Similarly, regarding the providers of online marketplaces, classified as "important entities", the definition is too broad. As a result it includes entities, whose service is primarily based on an online marketplace, and entities "offering" an online marketplace as a subordinate service to another business activity. This "second order" online marketplaces lead to an increasing number of entities falling into this category.

[104] https://www.easa.europa.eu/en/document-library/opinions/opinion-032021

3.3.2.4 Public Administration

During 2021-2022 we have witnessed an increasing amount of cyber-attacks/incidents targeting various cities and regions. As these entities handle very sensitive data and offer vital public services, such as construction permits/approvals and social benefits issuance, the exemption introduced by the European Council, could have severe consequences for the operational capacity of NUTS-2 and NUTS-3 regions.

Like privately managed entities, public administration entities lead by example in terms of ensuring a risk-based cybersecurity level and therefore, all requirements stemming from Articles 17, 18 and 20 must be also implemented by public administration.

3.3.2.5 Research Institutions

In terms of a holistic approach to protecting Europe's cyber-resilience, inclusion of research institutions into the Directive's scope is much appreciated, since entities/businesses often collaborate with these institutions for research projects. In terms of supply-chain security and to counter industrial espionage and to protect trade secrets, including entities that share, disseminate or exploit the results of their research, for commercial purposes into the Directive's scope seems to be reasonable.

3.3.3 Harmonisation (Article 4 and 5)

The European Parliament and the Council have aligned the text with sector-specific legislation, in particular the regulation on digital operational resilience for the financial sector (DORA) and the directive on the resilience of critical entities (CER), to provide legal clarity and ensure coherence between the NIS 2 Directive and these acts.[105]

As set out in the NIS 2 Directive Article 4, "*where sector-specific Union legal acts require essential or important entities to adopt cybersecurity risk-management measures or to notify significant incidents and where those requirements are at least equivalent in effect to the obligations laid down in this Directive, the relevant provisions of this Directive, including the provisions on supervision and enforcement laid down in Chapter VII, shall not apply to such entities.*" If, however, "*a sector-specific Union legal act does not cover all entities in a specific sector falling within the scope of the directive, the relevant provisions of the directive should continue to apply to the entities not covered by those sector-specific provisions*".

As a result, entities should verify whether national horizontal law regulations implementing the NIS 2 Directive will apply, in addition to sector specific legal acts.

Additionally, the NIS 2 Directive in recitals 23, 24, and 25 clarify that "*Where sector-specific Union acts entail cybersecurity requirements that are at least equivalent to those introduced by the NIS 2, these sector-specific Union acts should apply*".

Given the existing mixture of various legal acts addressing cybersecurity, achieving complete harmonisation across sectors and legal clarity across the Single Market could be challenging.

3.3.4 National cybersecurity strategy (Article 7)

Article 7 obliges each Member State to "*adopt a national cybersecurity strategy that provides for the strategic objectives, the resources required to achieve those objectives, and*

[105] https://www.consilium.europa.eu/en/press/press-releases/2022/11/28/eu-decides-to-strengthen-cybersecurity-and-resilience-across-the-union-council-adopts-new-legislation/

appropriate policy and regulatory measures, with a view to achieving and maintaining a high level of cybersecurity".

However, these strategies must be highly compatible in order to ensure that the national measures in their entirety enhance Europe's cyber-resilience. In addition, increased cooperation among competent authorities both for cybersecurity-related threats as well as non-cybersecurity-related threats, is crucial. Therefore, Article 7(1)(g) that requires from Member States to include in their national cybersecurity strategy "*enhanced coordination between the competent authorities under NIS 2 and the Critical Entities Resilience (CER) Directive*", is much appreciated.

Furthermore, prolonging the assessment/review period of the strategy to "*at least every five years*", provides policymakers and other cybersecurity actors with a better possibility to implement the measures introduced by a national cybersecurity strategy, since most EU Member States do not have a weakness in terms of strategy but rather on implementation.

3.3.5 National Cyber Crisis Management Frameworks (Article 9)

As already demonstrated by the Solarwinds case and the attack on the Ukrainian power grid, cyber incidents can have far-reaching repercussions. Therefore, the "*designation of one or more competent authorities responsible for the management of large-scale cybersecurity incidents and crises*" is welcomed. However, when developing and drafting such plans, Member States should consult relevant public and private entities as they have far-reaching insights into current attack-vectors and are aware of the consequences an outage of their service would have.

3.3.6 Requirements, Technical Capabilities and Tasks of CSIRTs (Article 11)

The tasks and powers of CSIRTs have been considerably improved in the updated NIS 2 Directive, as they undertake new roles while expanding existing ones under the NIS Directive.

Considering that the operational powers of CSIRTs are too extensive, it must be ensured that they do not interfere too extensively in the sovereign realm of enterprises. Instead a trustworthy structure should be fostered, where governmental and enterprise CSIRTs can collaborate, also with the globally well organised CERT and CSIRT community. [103]

According to the impact assessment report[97] that accompanies the NIS 2 proposal (PART 1/3 page 84), the broadening of the scope of the Directive and the expansion of tasks of national authorities, would result in an "*increase of about 20-30% of resources (including staff) of the relevant authorities per Member State at central level needed mainly for performing supervisory actions on a larger number of entities (i.e. on-site and off-site checks, audits, requests for and assessment of compliance evidence, etc.) and interactions with industry (including sector-specific)*".

Specifically for incident reporting, the Commission estimated an "*approximate increase of 10-15% in the staff of the competent authorities tasked to handle incident reporting*".

Under the NIS2 Directive the requirements for an entity to be designated as a CSIRT are similar to those of Annex I of NIS, but they are more specific and more demanding. However newly added requirements and capabilities for CSIRTs include:[106]

[106] https://www.ncsc.nl/binaries/ncsc/documenten/publicaties/2022/oktober/13/index/NCSC_NIS2_D1_Final.pdf

- A transparency obligation to "*clearly specify the communication channels and make them known to constituency and cooperative partners*" (Article 11(1)(a));
- A "*confidentiality and trustworthiness of operations*" obligation (Article 11(1) (d))
- Appropriate training of the CSIRT staff (Article 11(1)(e));
- A business continuity obligation by being equipped with "*redundant systems and backup working space*" (Article 11(1)(f));

While the NIS Directive specified that CSIRTs could only monitor and analyse incidents, NIS 2 expanded the material scope of this task in Article 11(3)(a), since "*upon request*", CSIRTs should also "*provide assistance to essential and important entities concerned regarding real-time or near real-time monitoring of their network and information systems*". Furthermore, according to Article 11(3)(d), CSIRTs are tasked to "*collect and analyse forensic data and providing dynamic risk and incident analysis*", providing valuable help for victims that do not have the capacity to conduct such an analysis themselves.

Within the information sharing task described in Article 11(3)(b) the threshold for "*providing early warnings, alerts, announcements and dissemination of information… on cyber threats, vulnerabilities and incidents*" is quite high, as it is required that the information is shared "*if possible in near real-time*". While the NIS 2 Directive does not make it clear who those "*other relevant stakeholders*" might be, they should be differentiated by 'any third parties' and the general public.

NIS 2 introduces another task in Article 11(3)(e) that of "*proactive scanning of the network and information systems, upon the request of an essential or important entity*" aiming at detecting vulnerabilities with a potential significant impact. Specifically, according to recital 44 the competent CSIRT "*should have the ability… to monitor the entity's internet-facing assets, both on and off premises, in order to identify, understand and manage the entity's overall organisational risks as regards newly identified supply chain compromises or critical vulnerabilities*". On the other hand the "*proactive non-intrusive scanning of publicly accessible network and information systems of essential and important entities*" mentioned in Article 11(3) aims at "*detecting vulnerable or insecurely configured network and information systems and inform the entities concerned*" independently of their potential impact.

However, considering the intrusive nature of proactive scanning it might affect the privacy and confidentiality of communications as well as the protection of personal data, and have a chilling effect on freedom of expression and speech. This suggests that proactive scanning should comply with the human rights principles, established in the EU Charter of Fundamental Rights[107], and in national constitutions of Member States. This is why, the European Parliament, in its Compromise Amendment[108] proposed that the proactive scanning of CSIRTs should be limited to "*serious threat to national security*". Consequently, CSIRTs should conduct an impact analysis and plan their strategy accordingly, ensuring that their operational framework has clear boundaries on what is and what is not allowed by legislation, other than the NIS 2, such as a legal basis for processing and human rights impact assessments.

NIS 2 introduces a legal task in Article 11(5) requiring from CSIRTs to "*promote the adoption and use of common or standardised practices, classification schemes and taxonomies in*

[107] https://www.europarl.europa.eu/charter/pdf/text_en.pdf

[108] https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/ITRE/DV/2021/10-28/NIS2_COMPROMISE_amendment_EN.pdf

relation to: a) incident-handling procedures, b) crisis management and c) coordinated vulnerability disclosure under Article 12“. Recital 58 outlines two specific international standards on vulnerability handling and vulnerability disclosure, namely ISO/IEC 30111 and ISO/IEC 29147. Therefore, CSIRTs should use technical standards by recognised standardisation bodies such as ISO, as well as national non-mandatory security standards and specifications that might be useful.

3.3.7 Coordinated Vulnerability Disclosure and a European Vulnerability Database (Article 12)

Coordinated Vulnerability Disclosure (CVD) is a new task aiming to holistically address cyber-resilience of ICT products and services, since any security vulnerability, regardless of whether it is an unintentional or an intentional weakness, susceptibility or flaw that can be exploited by a cyber threat, should be included in the database. However, manufacturers of such products and providers/developers of such services should be obliged to swiftly address them, as soon as they are reported.

The European vulnerability database developed and maintained by ENISA should support a lean and efficient reporting process, in order to keep the effort for everyone involved as low as possible. The European Parliament’s approach, to leverage global Common Vulnerabilities and Exposures (CVE) is in the right direction as it supports the global nature of developing and selling ICT services and products.

When disclosing vulnerabilities, ENISA must cooperate with the respective manufacturer of a product or the provider/developer of a service and inform them prior to any public disclosure.

3.3.8 Report on the State of Cybersecurity in the Union (Article 18)

The foreseen “*biennial report on the state of cybersecurity in the Union*”, will not augment the EU’s cyber-resilience, considering that ENISA’s report includes merely general information, which will not be of any help especially for SMEs. Instead, ENISA should maintain an online, concrete and up-to-date ‘actionable’ information on cybersecurity incidents, taking into account the evolving cyber threat landscape.

3.3.9 Management Liability for Cybersecurity Risk Management (Article 20)

For the first time, NIS 2 specifically places an obligation on “management bodies” (including C-Suite members) for implementing and complying with heightened security measures (Article 20) and any failure to recognise that could result in serious consequences, including management liability and administrative fines (Article 34), as provided for in the implementing national legislation. It obliges Member States, when implementing NIS 2, to ensure that management bodies:

- approve the cybersecurity risk management measures taken by the entity;
- oversee the implementation of the risk management measures;
- follow specific, regular cybersecurity-related training to obtain the needed knowledge and skills (competence and capacity) to apprehend and assess the cybersecurity risks to their essential or important entity; and
- are held liable for infringements by the entities;

Regarding the “*specific, regular cybersecurity-related trainings*” it is not clear what the content should be, nor how entities will prove that such trainings have been performed. Nevertheless, there are existing ways to educate employees at all levels about cybersecurity risk management, as well as the most fundamental hygiene best practices. For example the ANSSI's MOOC[109] free program covers the basics of digital security in France and leads to a proof of completion (however, it does not lead to certification).

The practical implication of this requirement is that individuals in those management bodies of essential and important entities falling within scope of NIS 2 could be held personally liable and may be subject to enforcement action where those entities breach their obligations under NIS 2. For instance, in the context of essential entities, NIS 2 permits Member States to foresee in their national transposing legislation that relevant bodies or courts suspend certifications and authorizations for services or activities provided by the organization and temporarily ban individuals from discharging managerial functions, including at the senior management C-Suite level, until necessary action has been taken to remedy deficiencies and/or comply with requirements requested by the competent authorities.

In addition to temporary bans, NIS 2 permits Member States to request that breaching entities make a public statement outlining not only that they have breach their obligations under NIS 2, but also identifying the individual(s) responsible for the breach. Penalties need to be effective, proportionate and dissuasive, and the recitals to the current NIS 2 text make it clear that they may include criminal penalties for infringement of the legislation.[110]

By pushing responsibility for cybersecurity risk management to the management level of those entities demonstrates a tendency to ensure that cybersecurity risk management is a senior management responsibility.

Although the current text of NIS 2 does not define what constitutes a "management body", it suggests that "*any natural person discharging managerial responsibilities at chief executive officer or legal representative level*" could be considered a "management body". This aspect will eventually be determined by implementing national legislation in the Member States.

The non-compliance liability of management bodies and training obligations requires companies to appoint a 'cybersecurity officer' at board level, to ensure compliance oversight and to reassess company and management assurance conditions in terms of liability risk mitigation.[111]

3.3.10 Cybersecurity Risk Management Measures (Article 21)

Entities providing a service which is essential for the maintenance of critical societal and/or economic activities, should review and enhance their technical and organizational structure and capabilities. Considering that NIS 2 aims for a more aligned cybersecurity management approach it outlines, in Article 21(2), the following cybersecurity measures (requirements), which are perceived as highly prescriptive and should be taken by all essential and important entities, to manage the risks posed to the security of their network and information systems when providing their services:

1. Risk analysis and sufficient information system security policies;
2. Incident handling (Preventing, detecting, and responding to incidents appropriately);

[109] https://secnumacademie.gouv.fr/

[110] https://www.europarl.europa.eu/doceo/document/TA-9-2022-0383_EN.pdf

[111] https://www.twobirds.com/-/media/new-website-content/insights/pdfs/220607_nis2-directive_provisional-agreement_newsletter_final.pdf

3. Business continuity, such as backup management and disaster recovery, and crisis management, in the case of a major cyber incident;
4. Supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers;
5. Security in network and information systems, from the acquisition to the development and maintenance stages, including vulnerability handling and disclosure;
6. Policies and procedures for assessing the effectiveness of cybersecurity risk management measures.
7. Use of cryptography and where appropriate, encryption;

Hopefully, most of these measures are already implemented by entities and as it represents a good approach on data protection it also goes hand in hand with General Data Protection Regulation (GDPR) activities. The exact cybersecurity measures each entity must implement to comply with their legal obligations under NIS 2 depends on factors such as their size, exposure to risk, the likelihood of occurrence of incidents and their severity, and the availability and cost of implementing technology or international standards. Although "*basic cyber hygiene practices and cybersecurity training*", the "*use of cryptography*" and "*the use of multi-factor authentication or continuous authentication solutions, secured voice, video and text communications and secured emergency communication systems within the entity*" are important, entities should always decide which measures they deem necessary for the affected/involved part(s).

Regarding point 5 above, recital 58 outlines that "*Since the exploitation of vulnerabilities in network and information systems may cause significant disruption and harm, swiftly identifying and remedying such vulnerabilities is an important factor in reducing risk. Entities that develop or administer network and information systems should therefore establish appropriate procedures to handle vulnerabilities when they are discovered. Since vulnerabilities are often discovered and disclosed by third parties, the manufacturer or provider of ICT products or ICT services should also put in place the necessary procedures to receive vulnerability information from third parties. In that regard, international standards ISO/IEC 30111 and ISO/IEC 29147 provide guidance on vulnerability handling and vulnerability disclosure. Strengthening the coordination between reporting natural and legal persons and manufacturers or providers of ICT products or ICT services is particularly important for the purpose of facilitating the voluntary framework of vulnerability disclosure. Coordinated vulnerability disclosure specifies a structured process through which vulnerabilities are reported to the manufacturer or provider of the potentially vulnerable ICT products or ICT services in a manner allowing it to diagnose and remedy the vulnerability before detailed vulnerability information is disclosed to third parties or to the public*".

Consequently, it is important for entities – especially manufacturers or providers of ICT products or services – to be able to receive vulnerabilities reported by third parties. This means that entities should implement a Vulnerability Disclosure Policy (VDP) – also known as Responsible Disclosure Policy.

A vulnerability disclosure policy "*establishes the communications framework for the report of discovered security weaknesses and vulnerabilities*"[112] enabling involved parties to exchange data in a secure and consistent way.

[112] https://www.bugcrowd.com/blog/vulnerability-disclosure-policy-what-is-it-why-is-it-important/

3.3.10.1 Supply Chain Due Diligence

Regarding Article 21(2)(d) concerning "*supply chain security*" the concrete implications of the requirements remain unclear, since it is unclear how an entity shall ensure that "*direct suppliers or service providers*" comply with the requirements deemed necessary by the EU Commission. Consequently, an entity should not be held liable if a supplier or service provider is non-compliant, especially if that entity ensured that the supplier or provider maintains a risk-based level of cyber resilience.

Furthermore, recital 85 notes that "*entities have been the victim of cyberattacks and where malicious perpetrators were able to compromise the security of an entity's network and information systems by exploiting vulnerabilities affecting third-party products and services*". Consequently, entities not falling under the scope of NIS 2 offering such products and services might also be affected by the legislation, especially if they offer their products and services to customers who fall under the NIS 2 scope and are therefore required to undertake supply chain due diligence on their suppliers. Recital 86 outlines that "*managed security service providers in areas such as incident response, penetration testing, security audits and consultancy*" have also been targeted by cyberattacks and therefore essential and important entities should exercise increased diligence.

Consequently managed security service providers (MSSPs) falling under the expanded scope/sectors of the Directive should be prepared for assessments/audits by their NIS 2 customers regarding the general cybersecurity and information security risk management practices and information security policies they follow.

NIS 2 therefore directs entities to be extra diligent in their selection of MSSPs.

3.3.11 Union Level Coordinated Security Risk Assessments of Critical Supply Chains (Article 22)

Coordinated security risk assessments of critical supply chains should be based on genuine risks and take a vendor-independent approach. Identified critical ICT services, systems or products should focus on core and sensitive functions. Finally, the measures proposed following the execution of the analysis must be proportionate and always foresee a sufficient implementation period.

3.3.12 Reporting Obligations (Article 23)

A cornerstone of European Union cybersecurity legislation (mandatory) is the reporting of cybersecurity incidents.[113] The NIS Directive introduced, in 2016, notification rules for cybersecurity incidents for operators of essential services in a wide range of critical sectors. Before the NIS Directive, rules on incident reporting were already in place for: a) telecom providers (under the Telecom Framework directive), b) trust service providers (under the eIDAS regulation), c) payment service providers (under the Payment Services directive), d) manufacturers of medical devices (under the Medical Devices regulation), and for data controllers under the General Data Protection Regulation (GDPR). Extending the established reporting channels to the national competent authorities, by including CSIRTs is not expected to significantly strengthen EU's cyber-resilience.

Furthermore, although it is as necessary that all actors have the necessary information to able to respond to a threat and thus contribute to enhanced cyber-resilience, the fact that Article

[113] https://www.enisa.europa.eu/topics/incident-reporting

23(2) requires from essential and important entities to include in their communications potentially affected recipients of their services, creates an additional burden to them. It remains thus to be seen whether this paragraph will significantly strengthen EU's cyber-resilience, or whether entities should focus on incidents with real consequences for users of their services.

Regarding the criteria for establishing whether or not an incident classifies as significant, Article 23(3) includes incidents that are capable of causing real consequences. Combined with the fact that an in-depth analysis of the incident is required in order to produce meaningful or conclusive information about the incident, it remains to be seen whether this will be available within 24 hours.

Similarly, although the prolongation of the reporting period to 72 hours for some incidents is much appreciated, it remains to be seen how feasible is to place an incident in one of the three categories ("*unlawful or malicious acts or could have a cross-border impact*") established in Article 23(4)(a), also considering that companies should focus on measures to minimise the implications of a successful cyber-incident/attack, rather than having to fulfil reporting obligations.

Allowing CSIRTs to ask for multiple "*intermediate reports on relevant status updates*" creates unnecessary regulatory and compliance burden to entities and establishes a huge amount of bureaucracy. Therefore, the requested intermediate and final reports should be limited in length (not more than two pages) and ideally fused into one final report following the incident handling completion.

3.3.13 Use of European Cybersecurity Certification Schemes (Article 24)

Although Article 24(1), makes it clear that the producer of an ICT product, service or system is obliged to certify it, rather than the essential or important entity that utilises it, and "*in the absence of appropriate European cybersecurity certification schemes adopted in accordance with Regulation (EU) 2019/881 of the European Parliament and of the Council (*[42]*)*", the inclusion of internationally recognised certification schemes, significantly broadens the possible basis for certification beyond cybersecurity schemes developed based on the EU Cybersecurity Act[42].

However, smaller essential or important entities having to rely only on certified products, services or systems will prove costly without necessarily enhancing their cyber-resilience.

The details are still to be worked out, but Article 24(3) states that "*the Commission may, after consulting the Cooperation Group and the European Cybersecurity Certification Group, request ENISA to prepare a candidate scheme*".

Furthermore, in the context of Article 24(2) the Commission is provided with more leeway, as cybersecurity certifications are introduced/mandated via delegated acts, as opposed to the implementing acts required by the Council, which gave governments more control.

3.3.14 Registry of Entities (Article 27)

All information shared by the Member States' single points of contacts with ENISA should be handled with the highest degree of confidentiality, while effective cybersecurity measures, should be implemented to protect the confidentiality and integrity of the information stored in the registry.

3.3.15 Cybersecurity Information-Sharing Arrangements (Article 29)

In order to ensure the protection of the potentially sensitive nature of the information shared, such as intellectual property and business foreground knowledge, the extent and scope of information-sharing arrangements needs to be clearly defined. Moreover, Member States with the support of ENISA, should make it be possible for all essential and important entities to join such cybersecurity information sharing arrangements.

3.3.16 Voluntary Notification of Relevant Information (Article 30)

Providing benefits to entities when reporting cybersecurity incidents, will result in an increase of the amount of notifications, thereby allowing the national competent authorities to gain a more holistic picture of the current cyber threat landscape.

A motivation for entities to voluntarily notify relevant information, is the quality of advice they receive from their competent authorities (CSIRT), as regards handling the incident and additional measures. Thus, is it important for CSIRTs to be transparent about the expected service level, but also the quality of their offered services, as this might have a broader impact, than solely the mandatory incident reporting obligations of Article 23.

3.3.17 Supervision and Enforcement Measures in Relation to Essential (Article 32) and Important Entities (Article 33)

Considering the shortage of qualified cybersecurity professionals, it seems unlikely that enough qualified professionals will be available to conduct "*regular and targeted security audits*" of essential and important entities across the European Union. Instead this requirement might reduce the overall cyber-resilience across the Union, as cybersecurity professionals will conduct (lucrative) audits rather than support entities in enhancing their cyber-resilience.

Regarding, the "*security scans*" referred to in Article 32(2)(d) and Article 33(2)(c) they should not be intrusive neither unannounced as, if done incorrectly, they could trigger a cyber incident of their own. Besides that, the "*fair and transparent risk assessment criteria*" does not provide the required legal certainty, increasing the risk of non-compliance when implementing the NIS 2 Directive.

When competent authorities "*adopt binding instructions*" as referred to in Article 32/33 (4)(b), they must consider the existing and ever increasing shortage of qualified cybersecurity professionals and thus provide companies with realistic time-limits "*for the implementation of such measures and for reporting on their implementation*".

Regarding the "*temporary suspensions or prohibitions imposed pursuant to*" Article 32(5), the special treatment foreseen for public administrations entities is not in the right direction, considering the increasing amount of cyber-attacks/incidents targeting them. Leading officials in public entities should also be held responsible for cybersecurity related misconduct, just like their private sector counterparts.

Compared to NIS, NIS 2 provides more detailed rules on the powers of national authorities responsible for the cybersecurity supervision and enforcement tasks.[114]

[114] https://www.insideprivacy.com/cybersecurity-2/new-eu-cyber-law-nis2-enters-into-force/

3.3.18 Budget Increase

The NIS 2 Directive will inevitably result in increased costs for affected organizations. According to the projections detailed in the impact assessment (IA)[97] that accompanies the NIS 2 proposal (PART 1/3 pages 72 and 73), in the medium-term (three to four years of NIS 2 implementation), it is expected that:

a) "*the new sectors to be added to the NIS scope would entail about 22% increase in their ICT security spending*"
b) "*For the sectors currently covered by the NIS Directive… about 12% increase in the ICT security spending*";

At the same time, NIS 2 would result in a "*reduction in cost of cybersecurity incidents by EUR 11.3 billion*".

For relevant authorities per Member State at central level, an estimated "*increase of about 20-30% of resources (including staff)*" is expected in the short and medium term.

At the same time recital 52 promotes "*the introduction and sustainable use of open-source cybersecurity tools*" for SMEs, "*facing significant costs for implementation*". Costly cybersecurity applications or tools are often unfeasible while cybersecurity awareness and risk-management measures are usually low among SMEs. To this end "*SMEs need guidance, assistance and support because of the rising ransomware and supply chain attacks, and potential spill-over effects on critical sectors for which SMEs act as suppliers*"[115].

3.4 Recommended Action Plan for Entities

Entities/organisations can use the following action plan for ensuring compliance with NIS 2:

1. Determine if your organisation falls under the scope of the NIS 2 Directive (Article 2).
   - The NIS 2 Directive distinguishes two types of entities: a) Essential Entities (EE), detailed in Annex I b) Important Entities (IE), detailed in Annex II.
   - Determine if your organisation size makes you regulated under NIS 2;
2. Check if your organisation falls under another national legislation/legal act specific to your sector and whether there are any additional security requirements, which would potentially need to be implemented;
3. Verify whether national legislation implementing the NIS 2 Directive applies, in addition to sector specific legislation/legal acts;
4. If your organisation does not fall under the scope of the NIS 2 Directive, check whether your suppliers or business customers are subject to the new rules;
5. Raise awareness on "management bodies" about NIS 2 administrative sanctions and fines, since entities can be subject to fines up to €10 million or 2% of their total turnover worldwide, whichever is higher (the same as a GDPR fine for a less serious violation). Worst case scenario for non-compliance could result in a combination of breach notification costs, GDPR fines, NIS 2 fines, negative publicity and loss of service availability;
6. Educate employees at all levels, focusing on top managers, about cybersecurity risk management and risk ownership;
7. Plan for the budget increase;

[115] https://www.linkedin.com/pulse/new-nis2-directive-what-means-smes-cyen/

8. Review the cybersecurity measures (requirements) outlined in Article 21(2) and identify those that need to be implemented;
9. Arrange for amendments to the security, risk management and incident response policies to achieve and document compliance with NIS 2;
10. Streamline incident reporting, by defining and documenting their Incident Response Plan, including procedures and policies;
11. Assess supply chain security and determine the contractual obligations you should require from your suppliers or business customers;
12. Make sure there is a business continuity, such as backup management and disaster recovery, and crisis management plan, in the case of a major cyber incident;
13. Implement an Information Security Management System (ISMS) taking into consideration NIS 2;
14. Encourage secure development practices. Considering that the NIS 2 Directive aligns with the EU Cybersecurity Act[42], the security and privacy of products and services should be by default and by design, in other words from their very conception. This means that entities should focus on training their developers on secure development practices and frameworks, either by raising awareness about it or involving the CTO, and the SOC teams or internal security experts and enthusiasts;
15. Set up a Vulnerability Disclosure Policy (VDP); and
16. Conduct regular and targeted security audits;

3.5 Recommended Action Plan for CSIRTs

3.5.1 Incident Response

As indicated by their name, incident response is a key service offered by CSIRTs. However, it depends on what CSIRTs consider as ‘incident’. Article 6(6), of the NIS 2 Directive, defines ‘incident’ as “*an event compromising the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the services offered by, or accessible via, network and information systems*”. Given this broad definition, CSIRTs need to follow an incident classification system. ENISA offers a reference for an incident classification taxonomy (ENISA, 2018)[116]. FIRST offers another taxonomy, classifying incident per category[117] (e.g. Denial of service, compromised information, internal hacking, and others), their sensitivity and criticality.

3.5.1.1 Service Level Transparency

CSIRTs offer a wide array of services, from hands-on approaches to advisory and coordination on incident handling. At the same time the service level depends on factors such as the available resources, their organisational model, culture etc. Additionally CSIRTs do not treat every incident equally, as some follow established incident matrix methods, in order to prioritise the handling of the incidents (such as CERT-FR[106]), while others follow the ENISA scaling for incident classification (such as RIA[106]). CSIRTs also have different escalation procedures depending on the severity of the event.

Consequently, transparency of the type, the expected level and the quality of the offered services, the competence and expertise, the entities under their responsibility, and other

[116] https://www.enisa.europa.eu/publications/reference-incident-classification-taxonomy
[117] https://www.first.org/resources/guides/csirt_case_classification.html

relevant information may positively impact the voluntarily notification of relevant information as discussed in 3.3.16.

3.5.1.2 Automation

Given the expected increase in incidents reporting under the NIS 2 Directive, incident response automation is foreseen to become an additional objective for CSIRTs. There are several approaches and offered solutions aiming at automating incident response.

Automation can support CSIRTs/CERTs to:[118] a) reduce workload or improve quality of the tasks to be performed, b) gather intelligence, analyse, and provide notifications about current threats, associated risks and potential remediation actions, c) provide situational awareness, d) provide actionable threat intelligence. However, there are several risks lying with an increased degree of automation. Consequently, CSIRTs should aim for a balance between automation and human in the loop, since every incident has its own unique characteristics.

3.5.1.3 Leverage Expertise from Cybersecurity Ecosystem

CSIRTs should leverage expertise from the cybersecurity ecosystem of their respective countries, by making use of the services of private consultants. However, CSIRTs should be able to ensure the reliability, independence, expertise and the competence of the consultants used. ANSSI Security VISA[119], BSI's volunteer Cybersecurity Network[120], NCSC-UK Cyber Assessment Framework (CAF) assured products & services[121] and NCSC-UK Certified Cyber Professional (CCP) assured service[122] are prominent examples on how CSIRTs can ensure that the provided consultants have the necessary competency and to ensure the quality and comparability of the evaluations/examinations, audits, and services.

Another means to engage and leverage the expertise and know-how of the private sector, is through Public-Private Partnerships (PPPs) that as mentioned in recital 55 can "*assist the competent authorities in developing state-of-the-art services and processes including information exchange, early warnings, cyber threat and incident exercises, crisis management and resilience planning*". An innovative example in this area is the French Cyber Campus[123] that brings "*various stakeholders physically together to stimulate innovation and sustainable industrial successes. The objective is to build a new centre of gravity for cybersecurity and digital trust in France and Europe.*"[124]

3.5.1.4 Training Programs

As already mentioned CSIRTs would need to increase their staff by 10-15%. In the short term recruiting new personnel is expected to be difficult mainly due to the lack of personnel with the available skills and training. Especially for smaller countries the majority of cybersecurity experts are often absorbed by the private sector. Consequently, CSIRTs should update their training programs in order to ensure a stable stream of incoming or available personnel,

[118] https://www.enisa.europa.eu/events/cti-eu-event/cti-eu-event-presentations/supporting-csirt-capabilities-and-reduce-manual-operations/

[119] https://www.ssi.gouv.fr/en/actualite/the-anssi-security-visa-by-the-french-national-cybersecurity-agency/

[120] https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Cyber-Sicherheitsnetzwerk/cyber-sicherheitsnetzwerk_node.html

[121] https://www.ncsc.gov.uk/section/private-sector-cni/products-services

[122] https://www.ncsc.gov.uk/information/certified-cyber-professional-assured-service

[123] https://campuscyber.fr/en/

[124] https://www.ssi.gouv.fr/uploads/2019/10/campuscyber-rapport-en.pdf

either through post-secondary/advanced education programs, or training programs for existing personnel that wishes to move internally to incident response departments, or by training employees of essential entities.

3.5.1.5 Quality and Accuracy of Information

Quality and accuracy of the information shared is pivotal. Some form of responsibility could be placed on the reporting entities to address this issue. This can be achieved through a legal obligation, when transposing the NIS 2 Directive, in the national law. However, care must be taken so that entities not sharing accurate or as much information about an ongoing incident are not over-penalised, as such information might only be available months after the incident was recorded. A qualification of the responsibility to share accurate information to 'the best of knowledge' of the reporting entity and/or without intention to misguide the CSIRT could address the risk of over-penalisation.

3.5.2 International and National Cooperation

According to Articles 10 and 11 of the NIS 2 Directive, CSIRTs should establish and participate in international and national cooperation relationships and cooperation networks for information sharing and operational support. A common ongoing practice among CSIRTs is to maintain trust on the basis of a prior personal contact. However, considering the foreseen increase of the CSIRTs and constituencies under the NIS 2 Directive, this practice will become eventually more challenging.

CSIRTs should publish guidance written in simple terms for non-expert audience, on their web-sites, in order to assist organisations to remain resilient to information security events and incidents. Additionally CSIRTs should examine sharing information on cybersecurity incident handling best practices via sectoral ISACs.

European and international cooperation networks include the:

a) **CSIRTs Network** established on the basis of Article 12 of the NIS Directive and maintained in NIS 2 (Article 15);
b) **TF-CSIRT**[125] that "*promotes collaboration and coordination between CSIRTs in Europe and neighbouring regions*" and "*promotes the use of common standards and procedures for handling security incidents, and coordinates joint initiatives where appropriate*". The task force further liaises with FIRST, ENISA, other regional CSIRT organisations, as well as defence and law enforcement agencies. TF-CSIRT runs a 'Trusted Introducer' program that "*serves as clearinghouse for all security and incident response teams*";
c) **European Government CERTs (EGC) group**[126] that has a technical focus. It forms an "*informal association of governmental CERTs in Europe*" and is "*part of an international environment*" since "*many EGC teams are members of FIRST and TF-CSIRT*";
d) **Forum of Incident Response and Security Teams** (FIRST)[127] is a non-for-profit organisation and "*aims to foster cooperation and coordination in incident prevention, to stimulate rapid reaction to incidents, and to promote information sharing among*

[125] https://tf-csirt.org/tf-csirt/
[126] https://egc-group.org/
[127] https://www.first.org/

members and the community at large". There are two types of participants in FIRST[128]: full members and liaison members. FIRST has demanding membership criteria: new members must be nominated by existing members;

3.5.2.1 Confidentiality of Information

When sharing sensitive/confidential information with different actors (authorities, essential or important entities, etc.) CSIRTs, should ensure the confidentiality of information. This can be achieved either through anonymization or be ensuring that relevant actors have access only to the necessary information. To this end CSIRTs could/should prepare two types of incident reports: a) an internal report with confidential information, and b) a public report sharing only what is necessary for the targeted audience.

3.5.2.2 Information Sharing

According to Article 10(4) CSIRT shall "*exchange relevant information with sectoral or cross-sectoral communities of essential and important entities*". This is achieved through information sharing networks in the form of ISACs for the sectoral information sharing, based on Public-Private Partnerships (PPPs) that as mentioned in recital 55 "*can provide an appropriate framework for knowledge exchange, the sharing of best practices and the establishment of a common level of understanding among stakeholders*".

The information shared at ISACs "*spans strategic, tactical, operational and technical levels; spans all phases of the cyber incident response cycle (proactive, pre-emption, prevention, preparation, incident response, recovery, aftercare/ follow up); is highly dynamic; crosses the boundary of public and private domains; and concerns sensitive information which can be potentially harmful for one organisation on the one hand, while being very useful to others*"[129].

In order to maintain trust among members of the various information sharing networks, a good practice is approval by (voting or recommendation) from existing members.[106] Next to membership requirements, smaller working groups, can create circles of trust, which decide what information to share with the other members of the community. Information sharing should also take place to the correct audience first to avoid notification fatigue of the constituencies, and second to ensure that sensitive information is communicated to those that will be benefitted from it.[106]

3.5.3 Technical Measures

3.5.3.1 IT Infrastructure Investments

CSIRTs technical capabilities and tasks are mandated under Article 11(3) and (5), indicating that CSIRTs should be equipped with the appropriate technical capabilities to perform their tasks. Consequently, CSIRTs should prioritise IT infrastructure investments, since investing in additional staff is not sufficient. Furthermore, CSIRTs should ensure that appropriate tools are available as they enable and facilitate their work. ENISA's SIM3v1 self-assessment tool "*helps CSIRTs to self-assess their team's maturity in terms of 44 parameters of the SIM3 v1 model*"[130] and provides a list of following tool parameters as important factors to assess the maturity of a CSIRT (T-1 to T-10).

[128] https://www.first.org/members/

[129] https://publications.tno.nl/publication/34616508/oLyfG9/luiijf-2015-sharing.pdf

[130] https://www.enisa.europa.eu/topics/incident-response/csirt-capabilities/csirt-maturity/csirt-survey

CSIRTs should also make use of a Malware Information Sharing Platform (MISP)[131], due to its capacity to share information in a timely manner both with targeted as well as selected audience. Unfortunately, not all private organisations are familiar with MISP.

3.5.3.2 Standardised Practices

As discussed in 3.3.6 CSIRTs should “*promote the adoption and use of common or standardised practices, classification schemes and taxonomies in relation to incident-handling procedures, crisis management and coordinated vulnerability disclosure“*. Having standardising practices will help CSIRTs with the evaluation of an incident and the sharing of information with other authorities (CVD).

[131] https://www.misp-project.org/

4 Summary

Following the recent reform of the NIS Directive this study identified the **contributions** to the EU cybersecurity regulatory landscape as well as the **implications for system and infrastructure security**, including an **action plan for entities**, to help them comply with NIS 2, **and for Computer Security Incident Response Teams** (CSIRTs) in the performance of their tasks. The key findings of the study, include:

a) **Expanded scope**, as the "*directive applies to public or private entities which are medium-sized enterprises and which provide their services or carry out their activities within the Union*". NIS 2 extended scope now includes more sectors and services of vital importance for key societal and economic activities, including providers of public electronic communications services, digital services, waste water and waste management, chemicals, food, manufacturing of critical products, pharmaceutical manufacturers, postal and courier services, space and public administration, both at central and regional level. The expansion of the scope covered by the new rules, that effectively oblige more entities and sectors to take cybersecurity risk management measures, will help **increase the level of cybersecurity in Europe in the medium and longer term**[Error! Bookmark not defined.].

b) **Increased risk management** requiring from "*essential and important entities to take appropriate and proportionate technical, operational and organisational measures to manage the risks posed to the security of network and information systems*";

c) **accountability of top management** for non-compliance with the NIS 2 requirements, resulting in serious consequences, including management liability and administrative fines;

d) **Alignment with sector-specific legislation**, in particular, the regulation on digital operational resilience for the financial sector (DORA) and the directive on the resilience of critical entities (CER);

e) **Streamlined reporting obligations,** requiring from public or private entities that are victims of cyberattacks to declare within 24 hours an early warning to the CSIRT or, where relevant, their competent authority, followed by a submission of an incident notification "*without undue delay and in any event within 72 hours after having become aware of the incident, with the aim, of updating information submitted in the early warning notification*". This will make it possible to assess the importance and seriousness of the cyberattack, while avoid over-reporting and creating an excessive burden on the entities covered;

f) **Imposition of fines**, as in the event of non-compliance with the rules established by the NIS 2 Directive, entities can be subject to fines up to €10 million or 2% of their total turnover worldwide, whichever is higher (the same as a GDPR fine for a less serious violation);

g) **Formal establishment of the European Cyber Crises Liaison Organisation Network** (EU - CyCLONe), which will support the coordinated management of large-scale cybersecurity incidents and crises;

h) **Voluntary peer-review mechanism** aiming to strengthen mutual trust and learning from shared experiences in the Union, achieving a high common level of cybersecurity;

i) **Security of supply chains and supplier relationships**, by ensuring that risk is managed within these processes;

j) **Upgraded tasks and powers of CSIRTs**, as they undertake new roles while expanding existing ones under the NIS Directive. CSIRTs tasks and powers are expanded from monitoring and analysing incidents to providing, upon request, assistance to entities, collecting and analysing forensic data and providing dynamic risk and incident analyses. In addition, proactive scanning of public networks and Coordinated Vulnerability Disclosure (CVD) tasks have been added to the tasks of CSIRTs.

The NIS 2 Directive **aims to set the baseline for cybersecurity risk management measures**, **harmonizes the cybersecurity requirements** and **implementation of cybersecurity measures** in all EU Member States, **addresses security of supply chains and supplier relationships**, includes **incident reporting obligations** for essential and important entities in all EU Member States and introduces **accountability of top management** for non-compliance with the NIS 2 requirements. It is an ambitious piece of legislation that requires a lot from companies and Member States in achieving a high common level of cybersecurity across the EU. Like its predecessor it is a challenging and costly task, but considering the "*annual cost of cybercrime to the global economy is estimated to have reached €5.5 trillion by the end of 2020*"[132], it is a small price to pay.

The NIS 2 Directive will care the resilience and incident response capacities of public and private entities, competent authorities and the EU as a whole and will ensure stronger risk and incident management and cooperation.

The enforcement of NIS 2 is not scheduled for tomorrow. Nevertheless, entities falling under the scope of the NIS 2 Directive should start working on compliance now, as some of the work might take more time than planned. The majority of the work to be done should be organized along the following three pillars: a) Governance, b) Incident Detection and Response, and c) Security Testing. Entities should investigate whether the fall under the scope of the NIS 2 Directive. If they fall under scope of the Directive, they should explore the organisational, financial and technical phases/steps that will be obliged to implement for complying with the Directive. Their actions should revolve around the cybersecurity measures (requirements) outlined in Article 21.

Member States, including their CSIRTs and national cybersecurity offices, will have to adapt to the increased tasks and number of entities. This will require additional capacity, in terms of human and financial resources to fulfil the increased tasks, as well as attracting expertise that may not be possible due to the lack of resources or a lack of candidates with the right skills and qualifications. Use of automated tools for scanning or information sharing must comply with the human rights principles, established in the EU Charter of Fundamental Rights, and in national constitutions of Member States, including the right to privacy and data protection.

[132] https://www.europarl.europa.eu/news/en/headlines/security/20221103STO48002/fighting-cybercrime-new-eu-cybersecurity-laws-explained