BUSINESSEUROPE

DRAFT POSITION PAPER

31/05/21

NIS 2.0 Directive

KEY MESSAGES

- **The annual cost of cybercrime is growing in 2020 this was estimated at EUR 5.5 trillion, the largest transfer of economic wealth in history.**
- **The current NIS Directive has increased cybersecurity awareness and resilience, yet Member State inconsistencies continue, this means Europe's joint situational awareness and crisis response remains insufficient.**
- **The NIS 2.0 Directive vastly widens the scope of the current Directive, whether deemed an essential or important entity blanket obligations apply. Such an expansion should only take place after thorough assessment of the actual risk and impact posed by entities and grading obligations.**
- **Reference to the full Commission Recommendation 2003/361/EC within the proposal should be made so that all micro, small and medium-sized enterprises are covered by the exemptions offered unless defined as an entity of "critical importance".**
- **There is a need for better coordination amongst Member State and Union level authorities to share information, prepare and react to cyber threats. We support the "one stop shop" mechanism in this regard.**
- **Information regarding vulnerabilities should only be made public once mitigation knowledge is available while upholding protection of sensitive business information.**
- **The focus following an incident should primarily be on mitigation. In the interests of cybersecurity capacities and proportionality, we would urge the incident notification timeframe to be extended from 24 hours to 72 hours.**
- **Businesses make a conscious effort to keep their systems secure, but 100% security is not realistic. Incidents will occur while businesses try to defend against malicious attackers. The solution to heighten and broaden more of these measures should be sought in a collaborative approach rather than through imposing draconian one size fits all fines.**

BUSINESSEUROPE a.i.s.b.l.
AVENUE DE CORTENBERGH 168 – BE 1000 BRUSSELS – BELGIUM
TEL +32 (0)2 237 65 11 – FAX +32 (0)2 231 14 45 – E-MAIL main@businesseurope.eu
WWW.BUSINESSEUROPE.EU – Follow us on Twitter @BUSINESSEUROPE
EU Transparency register 3978240953-79

THE NIS 2.0 DIRECTIVE

CONTEXT

The annual cost of cybercrime to the global economy in 2020 was estimated at EUR 5.5 trillion, double that previously reported in 2015. This represents the largest transfer of economic wealth in history. Geopolitical tensions continue to exacerbate this situation. Cyberattacks on infrastructure are now threatening energy, transport, water and food supplies. Not to mention targeting our democracies for political and ideological purposes in order to disrupt effective multilateralism.

The number of connected devices on the planet now outnumber people and are set to grow to 25 billion by 2025 (a quarter of these will be in Europe). Industrial supply chains are also becoming more digitally dependent. The ongoing COVID-19 pandemic has only demonstrated the acceleration towards a more digital society with 40% of employees in Europe teleworking. At the same time, around 40% of Europeans have experienced security related problems with 60% stating they feel unable to protect themselves from cybercrime. Starkly, 83% have never reported a cybercrime.

The current NIS Directive[1] has increased the level of cybersecurity awareness and importance across national authorities and businesses alike. However, while we continue to place great importance on a cyber secure digital economy, overall, the cyber resilience of businesses operating in the Union is too low for the rapidly increasing threats they face. While we continue to support the current risked-based approach of this framework which has contributed towards some identification of cybersecurity threats and applicable technologies to counter them, inconsistencies in resilience across Member States and sectors continue to exist. As a result, only a low level of harmonisation has been achieved. Various national rules exist across the single market which has meant wide reaching implementation costs for cross border businesses but also those only offering their services within the Member State itself. Some Member States have been stricter in setting obligations and enforcement of them than others. Taken together, this means the Union's joint situational awareness and crisis response is insufficient.

For this reason, we believe that more harmonisation among Member States is needed; it could be further supported by seeking convergence of cybersecurity methodologies, higher sharing of information and tools, stronger peer-review systems and by enforcing EU guidance in the implementation of the NIS 2.0 Directive. Stronger integration among Member States can have beneficial effects on:

- Implementation of Art 5 for the adoption of policies addressing cybersecurity in the supply chain, guidelines on cybersecurity requirements in public procurement and of policies addressing specific SME needs. As supply chains are cross-border entities, ICT and ICS (Industrial Control Systems) products and services, cross-border deliverables, regulatory hurdles could occur in case of differences between policies of different Member States;

[1] Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union

- Implementation of Art 18 for the development of "Cybersecurity risk management measures" and of Art 19 related to "EU coordinated risk assessments of critical supply chains;
- Implementation of a better supervision and enforcement of the whole NIS 2.0, including industry representation in support of the public-private principle. The peer-review system defined in the Art 16 should be monitored also the alignment of implementations in Member States and in case of misalignment, intervention plans aiming at addressing existing differences.

Creating a successful NIS 2.0:

We need to enhance the resilience of Europe's digital infrastructure and various sectors of the economy that rely upon it. This will involve improving information exchanges between Member State agencies, the European Union Agency for Cybersecurity (ENISA), the Commission, the European Central Bank (ECB) and businesses. Due to the rapidly changing nature of the digital economy and an ever-evolving cyber threat landscape, BusinessEurope supports an update to the current common level framework of cybersecurity across the Union through the NIS 2.0 Directive.

However, this must be achieved in a more proportionate and legally certain manner, particularly as cybersecurity obligations are proliferating for many businesses who will be subject to several potentially overlapping – and potentially conflicting – provisions at once. For example, policy makers should understand that essential entities could be subject to the NIS 2.0 Directive, the draft Directive on the Resilience of Critical Entities (RCE)[2], the EU Toolbox of 5G risk mitigating measures[3], the European Electronic Communications Code (EECC)[4], the General Data Protection Regulation (GDPR)[5], the draft ePrivacy Regulation (ePR), Implementing Regulation (EU) 2015/1998 on cybersecurity in aviation[6], forthcoming EU cyber certification schemes stemming from the Cybersecurity Act (CSA)[7], cybersecurity obligations in the updated Radio Equipment Directive (RED)[8] and Medical Devices Regulation (MDR)[9] as well as national regulatory requirements. Further to this, the forthcoming RCE and Digital Operational Resilience Act (DORA) Regulation[10] for the financial sector is being discussed in parallel. Therefore, BusinessEurope urges the European co-legislators to simplify and streamline Europe's cybersecurity regulatory regime and to avoid unnecessary overlaps or a situation to arise where duplicated or conflicting obligations and information sharing processes would apply. This is even more important considering that NIS 2.0 is a Directive that will need to be transposed into national laws, potentially containing additional discrepancies – and

[2] Proposal for a Directive on the resilience of critical entities
[3] Cybersecurity of 5G networks EU Toolbox of risk mitigating measures
[4] Directive (EU) 2018/1972 establishing the European Electronic Communications Code
[5] Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC
[6] 2015/1998 laying down detailed measures for the implementation of the common basic standards on aviation security, as regards cybersecurity measures
[7] Regulation (EU) 2019/881 on ENISA and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013
[8] Directive 2014/53/EU on the harmonisation of the laws of the Member States relating to the making available on the market of radio equipment and repealing Directive 1999/5/EC
[9] Regulation (EU) 2017/745 on medical devices
[10] Proposal for a Regulation on digital operational resilience for the financial sector

overlaps –at national level. This is important not only for covered entities but for competent authorities and for the well-functioning of the Internal Market.

The improvement of cybersecurity resilience itself must be the primary goal, rather than the bureaucracy or administrative costs that supports it. This is particularly the case for smaller companies, start-ups and freelancers who often lack the financial resources and personnel to implement high-end cyber-risk mitigating measures. Just recently, ENISA identified some major challenges for smaller companies, ranging from lack of cybersecurity awareness to lack of budget and lack of IT cybersecurity specialists. These companies need help improving their cybersecurity rather than far reaching and unrealistic obligations. The cyber resilience gap between larger and smaller businesses should be closed, particularly if the scope is going to be widened so rapidly. To this end, BusinessEurope encourages all EU Member States to provide cybersecurity training and other forms of help targeted at SMEs.

Moreover, a clear role for the industry in the defining process of cybersecurity at EU level is still missing. Both the CSA and the proposed new Cybersecurity Strategy mention industry as a trusted partner (eg. inclusions in the Joint Cyber Unit or of the European Cybersecurity Competence Network and Centre (CCCN)), but then fail to provide a significant role for the industry in the NIS 2.0 proposal so that entities which provide cybersecurity products and services required in the digital environment are included. The new strategy in particular details ways to cooperate with institutional agencies and end-users and mentions industrial cooperation only briefly whereas we believe they should be viewed as credible partners that cooperate directly with policy makers. Therefore, we believe the Art 12 cooperation group would benefit from the involvement of a wide range of industrial stakeholders, including SMEs, to contribute to the implementation of the NIS 2.0 Directive and furthering cybersecurity policy in general.

As a key societal stakeholder, BusinessEurope outlines its reaction to the Commission's proposal for the NIS 2.0 Directive, below:

SCOPE

The current NIS Directive permits Member States to identify operators of essential services which fall under its scope. However, NIS 2.0 will broadly widen its scope to many sectors that are pre-defined. This means that all businesses that fall under the categories listed within the NIS 2.0 Annexes and are therefore either: essential or important, will have to apply its provisions. This also includes businesses with more than 50 employees and/or a EUR 10 million annual turnover. As a result, a huge number of businesses, even those that have a low risk towards supply chains and essential services, will have to implement far-reaching cybersecurity requirements as stipulated in Art 18.

While we are not opposed to expanding the scope of the Directive per se, indeed we agree to the inclusion of the public sector as an essential entity, we believe that further regulating businesses should only take place after a more thorough assessment of the risk and impact they pose and then grading obligations to those risks as necessary. Simply listing additional business sectors in Annex 2 and applying all provisions to them is currently disproportionate to the possible risk posed. It will also represent a large cost, particularly at a time when businesses are continuing to struggle through the COVID-19 crisis. In its impact assessment, the Commission estimated that new businesses covered under NIS 2.0 would need to increase their IT spend by 22%with a 12% increase for

businesses currently under its scope. Differentiating between essential and important entities as well as ex-ante and ex-post measures could also achieve greater legal certainty as for now all categories seem to apply the same obligations to each business, regardless of their application or risk.

Clearer and concise definitions of all entities that fall in scope as Essential Entities and Important Entities is required. Greater clarity that the Directive only applies to entities operating within the EU, is also required.

Therefore, BusinessEurope urges policy makers to reference the full Commission Recommendation 2003/361/EC within Art 2(1) so that micro, small and medium-sized enterprises are covered. This would mean businesses with an annual turnover of 50+ million EUR or more than 250 employees would fall under the scope of the Directive. However, this exemption would not apply, regardless of size, if the micro, small or medium-sized enterprise was of critical importance to the continuity of the essential activity of an essential entity. This new addition to Art 2(2) of "critical importance" should be defined by considering whether the entity offers a good or service that is of vital importance for the essential entity to continue its essential tasks. By focusing more on the criticality of an entity rather than only its size, the NIS 2.0 Directive would be more proportionate while simultaneously achieving the Directive's goal of increasing cyber-resilience.

The proposed definition of "network and information systems" (Art 4(1)(b)) does not specify that the *"device or group of inter-connected or related devices"* are only those devices that are integrated into the IT and digital Industrial Control Systems of an essential or important entity. Since the aim of the NIS 2.0 Directive is to ensure, confidentiality, integrity, availability and operational capacity of essential and important entities, the respective definition should be limited to those devices that are of paramount importance for guaranteeing these goals.

However, in expanding the scope and number of service providers classified as essential entities, the current proposal does not take common practices into account where one essential service provider is the user or client of another essential service provider's services. The contractual obligations of service providers in these circumstances are not acknowledged, which could lead to legal ambiguity and/or overlap in reporting obligations. Under the current proposal an essential service provider would have to report to the regulator without having the necessary information or overview of end-users affected. We would recommend including a clarification in NIS 2.0 similar to that in the current NIS Directive *"where an operator of essential services relies on a third-party digital service provider for the provision of a service which is essential for the maintenance of critical societal and economic activities, any significant impact on the continuity of the essential services due to an incident affecting the digital service provider shall be notified by that operator"* (Art 16(5)). In addition, liability exemptions or safe harbours for notifying incidents should be maintained in consistency with Articles 14(3) and 16(3) of the NIS Directive. Otherwise, if mandated, a reporting obligation would amount to a breach of contract and risk reputational loss.

We believe assistance for SMEs to comply with the rules aimed at strengthening cyber resilience is needed. Member States should provide such assistance via governmental policies & security agencies, addressing the specific needs of SMEs, in relation to guidance and support in improving their resilience to cybersecurity threats. The scope of Art 5(2)(h) should therefore be extended to SMEs also under the scope of this draft Directive.

We welcome the approach to address cyber and non-cyber-related concerns surrounding essential entities by simultaneously proposing the NIS 2.0 Directive and the RCE. However, it must be ensured that the scope of both directives as well as the respective definitions correspond with one another. The Commission and Member States should provide critical and essential entities with one single point of contact (SPOC) where these entities are supposed to register, and where they can notify both cyber-incidents and incidents according to Article 13(1) of the RCE Directive. The current approach of different means to identify such entities risks creating a fragmentation which increases implementation costs for these entities. BusinessEurope supports measures that achieve harmonisation and the risk-based approach.

Moreover, while software providers cannot control exactly how businesses will use their services, it's important to ensure trusted supply chains in support of the objectives of this Directive. A risk-based approach should also underpin what levels of security requirements are required here. The Commission and ENISA, supported by the Cooperation Group should provide more guidance on how essential and important entities can scrutinise supply chains and build higher levels of cyber resilience through making use of certification schemes under Cybersecurity Act and/or international standards, such as IEC 62443, which subjects services, software and hardware supply chains to security risk assessments.

COORDINATED FRAMEWORKS

We support the need for better coordination amongst Member State and Union level authorities in order to share information, prepare and react to cyber threats. We support the "one stop shop" mechanism within Art 7 in this regard. The notification procedure for data breaches within the GDPR, with a lead authority, could serve as a useful regulatory model in this sense. Further to this, Art 8(3) aims to achieve this for businesses that are in scope as an essential and/or important entity, through enabling a SPOC in each Member State. Creation of a SPOC for businesses in this manner will make it much clearer, particularly for businesses newly brought into the scope of this framework, to understand which national authority should be their cybersecurity interlocutor. Some countries have already created one-stop-shop (OSS) incident mechanisms that could serve as an example to create similar ones (eg. Spain). We wholly support this one-stop-shop initiative as it should contribute to the simplification of business reporting and reduce administration costs.

However, we consider that the OSS initiative needs to be extended to electronic communications services (ECS) providers, including number-independent interpersonal communications services (NI-ICS) providers (as defined in Article 2 of the EECC[11]). Failure to extend the OSS initiative in Art 24 to such providers creates a disproportionate regulatory burden and runs counter to the NIS 2.0 proposal which should ensure a technology neutral approach. Applying the OSS initiative under Art 24 of the NIS 2.0 Directive proposal also to NI-ICS providers would simplify and streamline the security and notification obligations, as is envisaged by NIS 2.0 Directive, and greatly improve on the current, diverse and diverging, obligations under the EECC. However, the one-stop-shop should avoid creating unnecessary administrative burdens for ECS and NI-ICS.

The creation of a public central database that collects and displays information in relation to vulnerable ICT products or services and their severity of vulnerability as to how they were compromised, ENISA's "European Vulnerability Register", seems like a positive

[11] Directive 2018/1972

development, as long as it aligns with security best-practices surrounding vulnerability disclosure. It should also leverage the experiences gained through the development of other similar initiatives such as the Common Vulnerabilities and Exposure (CVE)[12] database or the NIST National Vulnerability Database (NVD).[13] We are also unclear as to whether entities must report vulnerabilities to ENISA or national CSIRTs and whether 3rd country reporting is still permitted.

BusinessEurope urges policy makers to ensure that when disclosing vulnerabilities, ENISA must cooperate with the respective manufacturer of a product or the provider of a service and inform them prior to any public disclosure. We believe that Art 6 should only make vulnerabilities public if mitigation knowledge is available and mitigations are sufficiently deployed to reduce the possibility of users to be attacked (while protecting business sensitive information). Otherwise, hackers could exploit the disclosed information which would have serious repercussions for Europe's cyber-resilience. In addition, a clear deadline should be included so that businesses have sufficient time to fix the vulnerability. Therefore, a timeframe should be established for how quickly ENISA must notify the manufacturer and how long the manufacturer has to review the requests, respond to them and roll out a solution, if necessary. References to businesses reporting the vulnerabilities should be avoided. Further to this, we remain concerned with ENISA's resources to carry out this task efficiently across Europe and indeed worldwide. Instead, we would promote that ENISA coordinates information collected by agencies across the Member States, but it is the security agencies in the corresponding Member State itself that has the contact with the relevant entities to fulfil these obligations.

Reporting vulnerabilities should not be a one-way street. Public entities should also report their knowledge on vulnerabilities as well. Article 6 should oblige government agencies from Member States to immediately report any information on vulnerabilities or backdoors in IT products to the respective businesses and/or ENISA. Currently it is the case that government agencies frequently hold back such knowledge which represents a significant threat to Europe's cyber-resilience. This is especially the case when serious vulnerabilities in ICT products or services utilised in critical entities are concerned. Moreover, CSIRTs must never have the power to suppress or delay the disclosure of a detected vulnerability when carrying out their obligations under Art 10(2).

According to Art 15, ENISA will publish a biennial report on the state of cybersecurity in the Union. The report shall include the development of cybersecurity capabilities across the Union, the current state in the Member States, propose a cybersecurity index and policy recommendations. BusinessEurope urges ENISA to refrain from publishing a biennial report that includes mainly general information long after the fact. Rather, ENISA should publish online up-to-date information on cybersecurity incidents. An improved daily updated, holistic situation picture as well as daily updated, sector-specific warnings would significantly help essential and important entities to benefit from the data aggregated by national competent authorities, and thereby, to better protect their business processes. Such information would help essential and information entities to support their cybersecurity risk mitigating measures.

RISK MANAGEMENT & REPORTING

BusinessEurope recognises that management bodies are responsible for the cybersecurity strategy of an essential or important entity. This step will help to significantly increase the awareness for cybersecurity issues among top-level

[12] https://cve.mitre.org/
[13] https://nvd.nist.gov/

management. However, it is important to note that the Commission recognises members of management bodies of essential entities and important entities have IT security personnel that possesses the necessary qualifications to develop and implement an entity's cybersecurity strategy. Consequently, it has to be questioned whether members of management bodies have the respective training or whether reports by IT security personnel are equally sufficient to provide members of management bodies with in-depth information. Moreover, personal accountability for non-compliance seems a step too far, especially if the goal is to ensure appropriate cybersecurity awareness in companies across sectors.

However, if the Commission regards a mandatory IT security training necessary for members of management bodies, it should swiftly define what constitutes "sufficient knowledge and skills", in order to provide guidance on which skills are considered adequate to implement. Moreover, such recommendations must be the same across the EU to ensure that members of management bodies are not confronted with diverging requirements across the Single Market or repetitive trainings across different Member States.

Policy makers should introduce a clear definition of "management bodies". Furthermore, Art 29(5)(b) and 29(6) exceed the usual liability for business related negligence and could result in personal liability at employee level and professional bans. We recommend removing these provisions. Article 17(1) already holds the management of regulated entities accountable for failure to comply with their risk management duties. It should at least be made clear that other employees are not covered by such personal liability.

The risk management obligations placed on businesses within Art 18 helpfully take a risk-based approach, however, what is required of businesses in Art 18(2) is far too detailed and could lead to disproportionate burdens for some businesses. This removes discretion as to how this duty of care should be offered by certain businesses depending on their risk profile. Furthermore, the list of required obligations does not depict how compliance with them can be properly demonstrated.

Art 18(2)(g) refers to the use of cryptography and encryption. We agree that the EU should support the advancement and utilisation of cryptographic methods where necessary. These methods (eg. end-to-end cryptography), protect businesses from industrial espionage and citizens from cybercriminals. These methods should be promoted on a voluntary basis, appropriate to risk and the technology, however, policy makers should not legislate for weakening cryptographic measures (eg. backdoors). Otherwise, this could weaken Europe's digital sovereignty and give potential authoritarian regimes the ability to oppress citizens and business.

Businesses will also be responsible for others in their supply chains. Art 18(3) worryingly obliges businesses to take account of vulnerabilities specific to each supplier and services provider in their supply chain. This will be challenging for many businesses who will fall under this NIS 2.0 proposal as they exist within large global supply chains where they have little control over other businesses that operate within them. We ask for guidance in this regard as to how businesses falling under the scope of this framework can achieve better levels of security in their supply chains in a practical and proportionate manner.

Alternatively, trusted supply chains could be determined in advance through making use of certification schemes under Cybersecurity Act and/or international standards, such as IEC 62443, which subjects services, software and hardware supply chains to security risk assessments. Clarification of how liabilities and compliance operations are shared

along the value chain from the back-end manufacturers up to the front-end operators would also be useful. At the same time, we would like to express the opinion that to achieve better cybersecurity resilience and verifiable compliance of supply chains is best dealt with through use of and reference to technical requirements via industry standards rather than the use of non-technical requirements.

Regarding Art 18(4), we would like to stress that the time taken to rectify should be in line with the risk, meaning that undue delay would not always be necessary. The risks associated with the non-compliance should be assessed without undue delay, but the implementation time for corrective measures should and must depend on the risk associated with the non-compliance and the effort needed to implement the corrective measures. As a result, this paragraph should be rephrased to reflect such an approach in relation to compliance actions by authorities.

The reporting obligations within Art 20, compared to the current application of the NIS Directive, seem overly extensive. In some provisions, even impractical. For example, Art 20(2) obliges businesses to notify CSIRTs of significant cyber “threats” that could result in a “significant incident”. The obligation to report potential future events – detached from any parameters regarding the likelihood and/or foreseeability of the future event arising – seems unreasonable and even unmeasurable for a business to truly carry out with accuracy and therefore demonstrate compliance particularly when it is not clear what CSIRTs are going to do with that information. It is also far from clear as to when a threat becomes “significant” and offers little cybersecurity capacity building. This adds to the unjustified burdens of reporting on businesses and will be legally uncertain to apply in practice.

While the need for reporting obligations between businesses and authorities is generally understood in order to build cybersecurity capacities, Art 20(2) also obliges businesses to inform customers. This could cause unnecessary distrust of digitalisation on a wider scale once the incident has been solved. Therefore, we believe information should only be sent to customers impacted in a private manner. We also require clarity on whether this would impact purely business-to-business (B2B) situations. Art 20(7) also provides that the competent authority or the CSIRT may inform the public about the incident or require the reporting entity to do so. Given the potential damage to the entity's reputation, this should not be done in case of potential incidents, since there is no real incident to report and the information could harm the reputation of the entity.

The new 24-hour deadline for businesses to report cyber incident notifications to authorities will be very challenging for the predominant number of entities required within the widened scope of the proposal. Art 20(4)(a) obliges all entities covered by the NIS 2.0 to report incidents “without undue delay”. While the notification itself could be a straightforward procedure if national authorities have sufficient OSS systems, the time period does not take into account the need for the business to perform a sufficient analysis to determine whether the threshold for notification is reached. Further to this, the focus following an incident should primarily be incident mitigation. In the interests of cybersecurity capacities and proportionality, we would urge the co-legislator to amend the incident notification timeframe and extend this current period to 72 hours.

Furthermore, under Art 20(4)(c), the timeframe for handing in a final post-incident detailed report to CSIRTs should be prolonged, otherwise entities could be confronted with very time-consuming reporting obligations instead of investing in sufficient resources for vital incident mitigation. Moreover, since the investigation time for a complex cybersecurity incident often amounts to around 6 months, handing in a final report after 1 month is usually not possible. Therefore, the final report should be handed in to the

competent national authorities no later than 1 month after the entity has finished its forensic analysis and has conducted all other measures necessary to ensure business continuity and handling of the notified cybersecurity incident. Such longer deadlines for handing in a final report are pertinent to ensure that companies can focus on mitigating the cybersecurity incident with priority first and then ensuring the full operational capacity of a company is swiftly regained.

Besides international standards and a potential future European legislative act on the security of Internet of Things (IoT) devices, the cybersecurity schemes developed pursuant to the CSA can help to ensure a level of basic cybersecurity across a key technology. However, we remind policy makers that the CSA takes a risk-based approach to the application of the schemes it produces. Schemes that apply to products, services or processes deemed to need a high level of assurance are mandatory.

Yet Art 21 could automatically permit any scheme created under the CSA to be made mandatory at Member State level. This also risks fragmentation on the use of cybersecurity schemes to which the CSA was intended to protect against. We would like to highlight that EU-level certification should take precedence over Member State level certification to the greatest extent practicable (per Art 57 of the CSA). We also recommend that when evaluating whether to make certain cybersecurity schemes mandatory that Article 56.3 and Article 67 of the CSA are closely followed to ensure effective structuring and leveraging of certifications.

In relation to Art 21(2), we recommend conducting public consultations on the content of the delegated acts to ensure transparent and inclusive process by offering formal input from essential and important entities.

ENFORCEMENT

The draft Directive instructs Member States to ensure that administrative fines imposed on essential and important entities are effective, proportionate and dissuasive. High fines on entities are not the most desirable route to a collaborative approach to the major day-to-day challenge of making and keeping network and information systems more resilient to outages and disruptions from cyber incidents. Companies already make a conscious effort to keep their systems secure, but 100% security is not realistic. Incidents will always occur while businesses try to defend against malicious attackers. The solution for more cybersecurity must rather be sought in a collaborative approach in which governments and companies' team up to better oppose and take actions against cyber criminals, including an increase of highly skilled nation-state attackers.

We would plead that fines are not only related to possible flaws in the cyber risk management systems of a company, but that they should also be related to the question whether there is tangible damage as consequence of a cyber incident for which a company could be reasonably held responsible. There should also be a proportional relation between the size of the fine, the caused damage and the type of incident, as with a cyberattack even an entity with excellent cyber risk management and security controls can still become a victim of a nation-state sponsored attacker. Hence, rather than introducing a one-size-fits-all maximum fine, the applicable fine should be differentiated according to the damage caused and the type of cybersecurity management-misconduct. Thereby the co-legislators would adhere to the necessary risk-based approach.

Otherwise, the amount of the penalty payments proposed within Art 31(4) are draconian. The possibility of being exposed to the unwanted attention that a penalty would entail and the subsequent brand damage is already sufficient to achieve compliance. The proposed amount of 10 million EUR may remain in place, but the provision of 2% of global turnover is disproportionate.

In general, the proposed mechanisms of enforcement seem disproportionate. We are concerned that they may demonstrate a lack of trust instead of an intention to continue building on the partnership and cooperation facilitated since the implementation of the 2016 NIS Directive. For example, Art 29(4)(h), (i) refers to “naming and shaming” which could have perverse impacts of non-bona fide actors attempting to game the system. Or Art 29(5)(a) which focusses on “suspension of certification”, which seems disproportionate for low level compliance issues.

In the case of multinationals, with offices/facilities in various member states, sanctions per member state are disproportionate. We would argue that if fines are imposed, and it has a transnational context (the problems for which a fine is imposed are occurring in more than one EU member state), the fine should be capped. This to avoid that each member state can freely impose whatever it seems most suitable as this could potentially lead to draconic fines of a multiple of 2% of group turnover.

Moreover, policymakers should always bear in mind, that the current European enforcement cybersecurity regime punishes the victims rather than the attackers. Hence, instead of fining essential and important entities who are investing huge amounts of resources in strengthening their cyber capabilities and who are the victims of cyber incidents, Member States should impose fines or other penalties on the attackers.

* * *