JOURNAL OF CYBERSECURITY

Journal of Cybersecurity, 2023, 1–11
https://doi.org/10.1093/cybsec/tyad009
Research paper

Research paper

Defining the reporting threshold for a cybersecurity incident under the NIS Directive and the NIS 2 Directive

Sandra Schmitz-Berndt *

Faculty of Law, Economics and Finance, Université du Luxembourg, 2721 Luxembourg, Luxembourg

*Correspondence address. 4, rue Alphonse Weicker, L-2721 Luxembourg. Tel: 00352 46 66 44 9666. E-mail: sandra.schmitz@uni.lu

Received 2 June 2022; revised 22 March 2023; accepted 5 April 2023

Abstract

The NIS Directive and sector-specific cybersecurity regulations require the reporting of (security) incidents to supervisory authorities. Following the risk-based approach adopted in the NIS Directive, the NIS 2 Directive enlists as a basic security element the reporting of significant incidents that (i) have caused or (ii) are capable to cause harm, as well as (iii) notifying the service recipients of cyber threats. Although during the interinstitutional negotiations between the European Commission, the European Parliament, and the Council of the European there was consensus that the NIS Directive's reporting framework needs to be reformed, views on the determination of what needs to be reported varied. This paper outlines and analyses the different concepts of a report-worthy significant incident that have been proposed during the legislative procedure for the NIS 2 Directive from a legal and policy perspective. Irrespective of further motives that may inhibit reporting, legal compliance is difficult to achieve where legal requirements are vague. In that regard, the difficulties to determine the reporting thresholds in the past and in the future are addressed. In consideration of the increased attack surface and threat scenario, it is argued that incidents where no harm has materialized should not be treated any different than incidents that have actually resulted in harm in order to acquire the envisaged full picture of the threat landscape and create value for business and society.

Key words: NIS Directive, incident reporting, cybersecurity, NIS 2 Directive

Introduction

The NIS Directive[1] has been the first horizontal legislative measure at EU level aiming to increase the level of the overall security of network and information systems. A central element of the NIS Directive to improve cyber resilience has been the introduction of security measures and incident reporting obligations for key operators of essential services (OES)[2] and certain digital service providers (DSPs).[3]

The NIS Directive had to be transposed into national law by 9 May 2018, by now all Member States have implemented respective legislation. The Directive contributed to improving cybersecurity capabilities at national level, increased cooperation between Member States, and improved the cyber resilience of public and private entities within the sectors encompassed.

However, these improvements seem to be no longer sufficient in light of an expanded threat landscape. The number, magnitude, sophistication, frequency, and impact of cybersecurity incidents are in-

1 Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, OJ L 194, 19.07.2016, pp. 1–30.

2 According to Article 4(4) NIS Directive, operator of essential services means a public or private entity of a type referred to in Annex II of the NIS Directive, which meets the criteria laid down in Article 5(2) NIS Directive.

3 According to Article 4(5) NIS Directive, 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, namely: an online marketplace, an online search engine, or a cloud computing service.

creasing, and present a major threat to the functioning of network and information systems. The European Union Agency for Cyber Security, ENISA, estimates that attacks on supply chains will have fourfold in 2021 compared to 2020 with supply chain security not being specifically addressed by the NIS Directive [1]. In the same time, attacks on cloud service infrastructure have increased fivefold [1]. Threats are diverse with incidents having an impact on a global scale, like the SolarWinds hack, and for instances, ransomware attacks targeting big and small, public and private entities alike [1]. Germany saw a 360% increase of such ransomware attacks in 2021 alone, with a hospital not being able to admit new patients for 13 consecutive days due to a ransomware attack [2]. Also in 2021, 14.8 million malware infections of German systems have been reported to infrastructure providers [2]. Besides the number, the nature of the different incidents is important to gain an impression of existing and evolving threats. Cybersecurity threats concern every legal entity and every natural person in our society. With digital transformation and interconnectedness of society, network and information systems have developed into an essential commodity in everyday life. At the same time, objects are more and more connected adding another risk surface. In light of the increased digitization of the internal market in recent years and the increasing and evolving threat landscape, which both have amplified during the COVID-19 crisis,[4] the European Commission accelerated the speed of the review of the Directive and presented a Proposal for a NIS 2 Directive (NIS 2 Proposal) [3] as early as December 2020. The European Commission was pushing to replace the existing Directive with an instrument that increases harmonization and coherence, while at the same time responding to the expanded cybersecurity threat landscape. During the legislative procedure, some discussion evolved as regards the determination of which kind of incidents have to be reported. Obviously, incidents vary in terms of geographical reach, impact, duration, affected users, etc. and reporting under the NIS Directive was restricted to the most serious incidents. This was perceived as providing an incomplete picture of the threat landscape and challenging early detection as well as preparedness and effective and appropriate defence mechanisms. With the line between cybersecurity and cyberdefence becoming increasingly blurred, information sharing about incidents has become essential for the aforementioned effective and appropriate security mechanisms. While entities may engage in voluntary information sharing with each other, the information shared stays within trusted communities. With mandatory incident reporting remaining an integral part of the NIS 2 Directive, this paper argues that the entities concerned may struggle to determine which kind of events have to be reported to the competent authorities under the Directive; also in the legislative process leading to a NIS 2 Directive, there has been some disagreement between co-legislators as to the scope of reporting. Though there has been consensus on the reporting of serious incidents, opposing views have been expressed as regards the reporting of cyber threats, near misses, and incidents where harm has not materialized. Considering the 'currently persisting insufficiency of cybersecurity preparedness' [3] and incident information as a means to potentially hinder the further spread of incidents, this paper argues in favour of the extension of reporting duties from a legal perspective while also highlighting the problems in determining which events have to be reported. It is concluded that extending the mandatory reporting beyond serious incidents where harm has materialized along with a tiered reporting process may help to overcome the partial reluctance to report. Enforcing reporting is necessary, since low reporting levels result in a flawed picture of the threat landscape, which in turn may impact cybersecurity preparedness. Further, this paper argues that an extension to reporting of incidents where no harm has materialized facilitates the determination of reporting thresholds to achieve legal compliance, while at the same time serving the overall goal of the NIS regulation, namely, increased cyber resilience.

By way of statutory interpretation, the section 'Reporting Obligations: From NIS 1 to NIS 2' of this paper outlines the evolution of reporting obligations from the NIS Directive to the NIS 2 Directive[5] as published in the official journal of the EU on 27 December 2022. Further, the deficits under the NIS Directive in terms of national interpretation of reporting thresholds are addressed. In that regard, the paper focuses on the definition of what has to be reported and does not address questions of alternative reporting schemes, or reporting deadlines and the suggested alignment of timeframes with other instruments, e.g. GDPR.[6] For a full picture of the different positions leading to the final NIS 2 Directive, the reporting obligations under the original European Commission's NIS 2 Proposal are outlined and compared to existing legislation in France and Germany, which already goes beyond the minimum requirements under the NIS Directive. For an all-encompassing overview of the legislative history of the NIS 2 Directive, the paper further outlines the suggested amendments to the NIS 2 Proposal by the European Parliament [4] as well as the Council's compromise text [5]. The section 'The extended reporting obligations: challenges ahead' then addresses the challenges ahead and the question of what should be considered a report-worthy incident also in light of challenges that have been encountered with regard to determining harm under GDPR breach reporting. The section 'Concluding remarks' summarizes the findings in light of the overall aim of the NIS Directive and the NIS 2 Directive.

Reporting obligations: from NIS 1 to NIS 2

Incident reporting obligations are not new in EU legislation. As regards for instance, the Telecoms sector and here specifically electronic communications networks and services, obligations to report security breaches have been existent at EU level for more than a decade.[7] Also in the highly harmonized banking and finance sector, reporting obligations preceded the NIS Directive.[8] In contrast to the in general rather restricted scope of application of interventions in these sectors,

4 COVID-19 also led to an increase of non-malicious incidents due to migration to the cloud [1].

5 Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive, OJ L 333, 27.12.2022, pp. 80–152. The NIS 2 Directive enters into force on 16 January 2023 and becomes applicable on 18 October 2024. The NIS 1 Directive is repealed with effect from 18 October 2024.

6 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 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 (GDPR), OJ L 119, 04.05.2016, pp. 1–88.

7 See Article 13a(3) Directive 2002/21/EC as last amended by Directive 2009/140/EC of 25 November 2009 on a common regulatory framework for electronic communications networks and services (Telecom Framework Directive), OJ L 337, 18.12.2009, pp. 37–69; Article 4(2) Directive 2002/58/EC as last amended by Directive 2009/136/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (e-Privacy Directive), OJ L 337, 18.12.2009, pp. 11–36, and Commission Regulation (EU) No 611/2013 of 24 June 2013 on the measures applicable to the notification of personal data breaches under Directive 2002/58/EC of the European Parliament and of the Council on privacy and electronic communications, OJ L 173, 26.06.2013, pp. 2–8.

8 Cf. Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for

the scope of the NIS Directive is much wider and the obligations apply to certain DSPs and entities operating in seven sectors identified as key in the functioning of the internal market. While most reports and literature either focus on the types of approaches to share incident information [6], address information sharing from an economics perspective [7–9], and/or discuss the lack of incentives to report to authorities [7–10], the initial prerequisites for triggering the obligation to report to national authorities are hardly addressed. Prior to the adoption of the NIS Directive, ENISA [6] acknowledged that entities struggle to determine what kind of events they need to share with authorities due to the vagueness of traditional regulation. In that regard, ENISA [6] recommended in 2015 in view of the Proposal for a NIS Directive that Member States should clearly define the situations in which mandatory reporting is needed. The following section addresses in how far the latter has been achieved with the adoption of the NIS Directive. In order to close the existing gap in the literature on incident reporting, the analysis from the NIS Directive to the NIS 2 Directive focuses on the events and their respective thresholds that trigger reporting from a legal perspective while also addressing how the leeway granted to Member States in transposing the Directive challenges the determination of thresholds for the reporting entities.

Reporting obligations under NIS 1: incidents with significant or substantial impact

In order to increase the cyber resilience of OES and DSPs under the scope of the Directive, the NIS Directive introduced an obligation to report security breaches for these kind of entities. In fact, security breach reporting, also known as incident reporting, is deemed a 'hallmark of EU cybersecurity legislation' [11]. Accordingly, Article 14(3) NIS Directive requires Member States to ensure that OES notify, without undue delay, the competent authority or CSIRT of incidents having a significant impact on the continuity of the essential services they provide. Article 16(3) NIS Directive introduces a similar obligation with regard to DSPs, which must notify any incident having a substantial impact on the provision of a service that they offer within the EU.

Article 4(7) NIS Directive defines an incident as 'any event having an actual adverse effect on the security of network and information systems'. Since an adverse effect can easily be attained, the reporting obligation in terms of OES is limited to 'incidents having a significant impact on the continuity of the essential service they provide' [Article 14(3) NIS Directive]. In any case, some harm must have materialized since there must have been an effect on the continuity of the service. In order to determine the significance of an impact, Article 14(4) NIS Directive provides a list of parameters that shall be taken into account, namely, '(a) the number of users affected by the disruption of the essential service; (b) the duration of the incident; (c) the geographical spread with regard to the area affected by the incident'. In that line, Recital 27 of the NIS Directive specifies that the number of users affected by the disruption relate to the users relying on that service for private or professional purposes; their use of the service 'can be direct, indirect, or by intermediation'. When Member States assess the impact that an incident could have on economic and societal activities or public safety, in terms of degree and duration, Recital 27 recommends consideration of the time that is likely to elapse 'before the discontinuity would start to have a negative impact'. The impact assessment must further consider sector-specific factors of which some are enlisted in Recital 28 of the NIS Directive; for instance, a sector-specific factor in the sector 'processing and supply of water production' would relate to the volume and number and types of users supplied, including e.g. hospitals, public service organizations, or individuals, and the existence of alternative sources of water to cover the same geographical area. The consideration of sector-specific factors already indicates that there is room for divergent interpretation depending on where the Member States puts its emphasis.

A challenge when determining what kind of situations have to be reported lies in the different approaches in the transposition of the Directive by Member States as well as (in some cases) pre-existing legislation [12]. In addition, the identification process of OES varies across Member States, which in turn results in fragmentation, i.e. an entity may fall within the scope of the Directive in Member State A, but not in Member State B due to different assessment criteria [13].[9] As a consequence, an entity may have to report an incident in State A but not in State B. The same issues arise when determining whether an incident has to be reported because it surpasses the threshold of 'significant'. This is not only due to the fact that the size of entities encompassed varies between Member States. Focusing on the assessment methodology to determine the 'significance' of an impact, variations across Member States also exist as to whether the notion of significance is defined at all, and if so, by whom. For instance, in Luxembourg, the regulatory authority determines the significance for each sector in a regulatory order following a public consultation.[10] In contrast, in Denmark, every sector defines what constitutes a significant impact [12]. Most Member States lack further guidance as to the determination of significance. At EU level, guidelines on notification of OES incidents [14], published by the NIS Cooperation Group (NIS CG),[11] provides some general guidance addressed at Member States on how incident notification provisions could effectively implemented across the EU. As regards the 'significant impact' of an incident, the guidelines suggest to take into account the parameters listed in Article 6(1) NIS Directive, i.e. those factors that are used to determine the significance of 'a disruptive effect' [14]. Accordingly, when determining the significance of an impact on the service, Member States shall also consider (a) the dependency of other OES sectors on the service provided by the affected entity; (b) the impact that incidents have, in terms of degree and duration, on economic and societal activities or public safety; (c) the market share of the entity concerned; and (d) the importance of the entity for maintaining a sufficient level of the service, taking into account the availability of alternative means for the provision of that service. The guidelines

electronic transactions in the internal market (eIDAS Regulation), OJ L 257, 28.08.2014, pp. 73–114; Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market (PSD2), OJ L 337, 23.12.2015, pp. 35–127.

9 The fragmented approaches across the Union regarding the identification of OES also contributes to uneven levels of preparedness [12].

10 For example, Règlement ILR/N22/1 du 22 février 2022 portant définition des modalités de notification et des critères des incidents ayant un impact significatif sur la continuité des services essentiels du secteur transport—sous-secteur transport ferroviaire; Règlement ILR/N21/2 du 04 octobre 2021 portant définition des modalités de notification et des critères des incidents ayant un impact significatif sur la Continuité des services essentiels du secteur eau potable.

11 The NIS CG was established by Article 11 NIS Directive and is composed by representatives of the EU Member States' national cybersecurity authorities, the European Commission and ENISA. Its mandate under the NIS Directive aims at facilitating the dialogue between different bodies responsible for cybersecurity in the EU; the NIS CG is for instance the forum where common cybersecurity challenges are discussed and coordination on policy measures is taking place.

provide some guidance as to how these factors should be interpreted at national level and addresses the challenges posed in some sectors in applying the parameters,[12] however, they are neither binding nor specific enough for entities to rely on.

Fragmentation across EU Member States is not limited to diverging levels of guidance and diverging interpretations of 'significant', but also a direct result of various Member States having a reporting regime in place that goes much further than required by Article 14 NIS Directive. In these Member States, reporting is not restricted to 'incidents having a significant impact on the continuity of the essential service they provide' (Article 14(3) NIS Directive), but also incidents that only have the potential to cause harm.

In Germany, with its pre-existing legislation, § 8b IV BSIG[13] requires operators of 'critical infrastructures'[14] to report '1. incidents regarding the availability, integrity, authenticity and confidentiality of their information technology systems […] which have resulted in a failure or material impairment of the functionality of the critical infrastructures operated by them; as well as 2. significant incidents regarding the availability, integrity, authenticity and confidentiality of their information technology systems […] which may result in a failure or material impairment of the functionality of the critical infrastructures operated by them'. The explanatory memorandum to the IT Security Act 1.0, which introduced the aforementioned provision, outlines that an incident requires that there has been an interference of such a kind that the affected technology can no longer carry out its foreseen function or that the interference at least targeted the functioning [15]. An incident can thus also be established where an attack has only been attempted or been successfully defended by security measures. Similarly, the French implementation of the NIS Directive requires OES to report incidents that 'have or are likely to have, considering the number of users and the geographical area affected and the duration of the incident, a significant impact on the continuity of these services'.[15]

Accordingly, the 'significance' threshold varies from clear-cut sector-specific guidance regarding significant impact to incidents that have not materialized but have the potential to have a significant impact. The later exceeds the requirements of Article 14(3) NIS Directive, that there must have been a service disruption for a certain time across a certain area, which impacted economic and societal activities or public safety.

In contrast to Article 14(3) NIS Directive, which applies solely to OES, the reporting obligation for DSPs in Article 16(3) relates to incidents that have 'a substantial impact' on the provision of a service 'that they offer within the Union'. In order to determine whether the impact of an incident is substantial, the following parameters in particular shall be taken into account: (a) the number of users affected by the incident, in particular users relying on the service for the provision of their own services; (b) the duration of the incident; (c) the geographical spread with regard to the area affected by the incident; (d) the extent of the disruption of the functioning of the service; and (e) the extent of the impact on economic and societal activities (Article 16(4) NIS Directive). One year ahead of the transposition deadline of the NIS Directive, ENISA specified the parameters used to measure the impact of an incident in a guideline [16]. In consideration of the difficulties of determining the 'substantial impact', the Commission adopted the Commission Implementing Regulation (EU) 2018/151[16] also before the transposition deadline. Article 4 of the Commission Implementing Regulation sets forth that an incident has a substantial impact where at least one of the following situations has taken place: (a) the service provided by a digital service provider was unavailable for >5 000 000 user-hours, whereby the term user-hour refers to the number of affected users in the Union for a duration of 60 minutes; (b) the incident has resulted in a loss of integrity, authenticity, or confidentiality of stored or transmitted or processed data or the related services offered by, or accessible via a network and information system of the digital service provider affecting >100 000 users in the Union; (c) the incident has created a risk to public safety, public security, or of loss of life; and (d) the incident has caused material damage to at least one user in the Union where the damage caused to that user exceeds EUR 1 000 000. Recital 10 of the Regulation clarifies that the cases laid down in this Regulation 'should be considered as a non-exhaustive list of substantial incidents'. Comprehensive guidelines on quantitative thresholds of notification parameters could however be set up in the future based on the lessons learnt from the application of the Regulation and best practice information collected by the NIS CG.[17] It has to be noted that Implementing Regulations are directly applicable and need not be transposed into national legislation, which ensures a coherent approach across Member States.

The NIS Directive in practice

With increased reliance on digital technologies during the COVID19-pandemic, the review of the NIS Directive, originally foreseen for completion in May 2021 [Article 23(1) NIS Directive], accelerated and resulted in a proposal for a NIS 2 Directive as early as December 2020. The review [12] disclosed that the variety of sectoral approaches 'challenges a common regulatory approach in the EU', which in turn hampers the activity of operators that offer their service cross-border. Within the public consultation in course of the NIS Directive review process, a general agreement among stakeholders could be observed in terms of reporting thresholds for both, OESs and DSPs, being set too high to trigger the notification obligation. According to [12], a significant number of national competent authorities 'called for harmonizing reporting thresholds' for incidents since 'hardly any incident in the past two years has attained one of the established thresholds'.

In fact, with no uniform approach across Member States regarding reporting thresholds, the number of reports received by different national authorities varies significantly. According to [12], in 2018, the Hungarian authority received 900 incident reports compared to Lithuanian authorities receiving 10 000. However, these numbers do not seem to reflect the number of actual 'significant' or 'substantial'

12 The NIS CG for instance recognizes that the variables that they outline are sometimes incompatible since a simple parameter may mean different things to different types of providers [14].

13 Act on the Federal Office for Information Security (Gesetz über das Bundesamt für Sicherheit in der Informationstechnik [BSIG]).

14 Instead of 'essential services', the German implementation of the NIS Directive uses the notion 'critical infrastructures' as a pure linguistic variation.

15 Article 7 Act No. 2018–133 of 26 February 2018 on various provisions for adapting to European Union law in the field of security (Loi no 2018–133 du 26 février 2018 portant diverses dispositions d'adaption au droit de l'Union européenne dans le domaine de la sécurité).

16 Commission Implementing Regulation (EU) 2018/151 of 30 January 2018 laying down rules for application of Directive (EU) 2016/1148 of the European Parliament and of the Council as regards further specification of the elements to be taken into account by digital service providers for managing the risks posed to the security of network and information systems and of the parameters for determining whether an incident has a substantial impact, OJ L26, 31.01.208, pp. 48 et seq.

17 Cf. Recital 10 Commission Implementing Regulation (EU) 2018/151.

incidents since the annual report of the NIS CG[18] only enlists a total of 432 incidents across the EU Member States in the round of annual summary reporting of 2019 [11]. Considering the size of Member States and the extension of reporting obligations to incidents that only may have a substantial impact, also the number of reported incidents from France and Germany are rather low. ANSSI, the French national competent authority for NIS security, received 2287 reports in 2020 [17], while its counterpart in Germany, the BSI, only lists 419 incident reports under § 8b IV BSI Act in its 2020 annual report [18]. In contrast, the Belgium CERT received 7433 reports in 2020 [19], however—as with the aforementioned numbers from Hungary and Lithuania, it remains unclear how many of the reports relate to mandatory reports under the Belgian NIS law since CERT.be states that this number also encompasses inter alia assistance requests for advice to deal with incidents and early warnings from partner organizations. In response to an information request in December 2021, the Luxembourgish NIS authority, the ILR,[19] confirmed that no incident reports have been received so far, although Luxembourg is the place of main establishment in the EU of many internationally operating DSPs meaning that these DSPs fall under Luxembourgish jurisdiction for services provided in the EU.[20]

The fact that the available statistics show low reporting levels seems to confirm earlier presumptions [9] that mandatory reporting regardless of the sanction level does not incentivize entities to report security incidents to authorities.

Reporting obligations under the European Commission's NIS 2 Proposal: potential harm and cyber threats

The NIS 2 Proposal seeks to respond to the criticism of fragmentation by reforming the existing reporting regime [20]. The divergences in incident reporting thresholds are to be eliminated by more precise provisions, including a tiered plan, on the incident reporting process [see Article 20(4) NIS 2 Proposal]. Besides the reporting of significant incidents, Article 20(2) NIS 2 Proposal also foresees the mandatory reporting of 'significant cyber threats' in order to get a full picture of the threat landscape. According to Recital 24 NIS 2 Proposal, this additional information should aid Member States to adapt their level of preparedness and be adequately equipped 'to prevent, detect, respond to, and mitigate network and information incidents and risks'.

In contrast to the NIS Directive, which defined an incident as 'any event having an actual adverse effect on the security of network and information systems', Article 4(5) NIS 2 Proposal provides a more sophisticated definition setting forth that an incident means 'any event compromising the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the related services offered by, or accessible via, network and information systems'. With the elimination of the different treatment of entities providing essential and entities providing digital services, the NIS 2 Proposal no longer utilizes the notion of 'substantial impact' in relation to incidents that affect DSPs. Instead, irrespective whether the entity is important or essential,[21] the reporting threshold is the 'significant impact on the provision of their services' [Article 20(1) NIS 2 Proposal]. Pursuant to Article 20(3) NIS 2 Proposal, an incident shall be considered significant if '(a) the incident has caused or has the potential to cause substantial operational disruption or financial losses for the entity concerned, (b) the incident has affected or has the potential to affect other natural or legal persons by causing considerable material or non-material losses'. This means that an incident might be considered significant even if the harm has not materialized. This goes far beyond of the reporting obligation under the NIS Directive and mirrors the approach taken in France and Germany outlined above.

The mandatory reporting of incidents with the potential to cause substantial or considerable harm is not the only major change in relation to report-worthy circumstances. As mentioned above, under Article 20(2) NIS 2 Proposal, the reporting obligation is extended to encompass 'any significant cyber threat that those entities identify that could have potentially resulted in a significant incident'. A cyber threat is defined in Article 4(7) NIS 2 Proposal as a cyber threat within the meaning of Article 2(8) Regulation (EU) 2019/881 (Cybersecurity Act), which means 'any potential circumstance, event or action that could damage, disrupt or otherwise adversely impact network and information systems, the users of such systems and other persons'. Extending the mandatory reporting to significant cyber threats is based on the assumption that cyber threats are becoming more complex and sophisticated, and good detection and prevention measures depend to a large extent on regular threat and vulnerability intelligence sharing between entities. Information sharing is considered as fundamental for increased awareness on cyber threats, which, in turn, 'enhances the entities' capacity to prevent threats from materializing into real incidents and enables the entities to better contain the effects of incidents and recover more efficiently'.[22] In that regard, the Commission concluded that lacking guidance at Union level seems to have prevented such information sharing due to uncertainty over compliance issues for instance under competition law rules.[23]

Reporting obligations under the European Parliament Draft Resolution: throwback to NIS Directive

Key changes to the Commission's proposal relate to the reportable incident and the notification procedure. The European Parliament Draft Resolution [4] is rather critical towards any extension of reportable incidents and opposes the proposed mandatory reporting of significant cyber threats.[24] The same applies to the reporting of incidents that have the potential to cause harm.[25] Instead, the European Parliament Draft Resolution suggests to replace the proposed parameters to determine the significance of an impact with more precise, yet sector-unspecific, parameters, namely '(a) the number of recipients of the services affected by the incident; (b) the duration of the incident; (ba) the geographical spread of the area affected by the incident; (bb) the extent to which the functioning and continuity of the service is affected by the incident; (bc) the extent of the impact of the incident on economic and societal activities'.[26] These parameters are a duplication of the parameters that currently exist in relation to

18 According to Article 10(3) NIS Directive, the national single points of contacts shall submit a summary report on the national notifications received to the NIS CG on an annual basis.

19 The ILR is the regulatory authority for all sectors excluding the financial sector.

20 These DSPs include diverse entities of the Amazon group for instance Amazon EU S.à.r.l., Amazon Services Europe S.à.r.l.,

21 Instead of distinguishing between OESs and DSPs, the NIS 2.0 Proposal distinguishes between entities that are considered essential and such that are considered important.

22 Recital 67 NIS 2.0 Proposal.

23 Cf. ibid.

24 Amendment 195 European Parliament Draft Resolution.

25 Amendments 197 and 198 European Parliament Draft Resolution.

26 Amendments 197 to 201 European Parliament Draft Resolution.

the determination of a 'substantial impact' under Article 16(4) NIS Directive.

The limitations in comparison to the Commission Proposal are based on the assumption that the requirement to report incidents that only have the potential to cause harm or affect others is 'unrealistic' [21]. Concerns relate to competent national authorities being overwhelmed by receiving too many notifications, which in turn could divert attention and limit security resources away from the essential tasks of actually examining and handling incidents [21].

As regard the extension of reporting obligations to significant cyber threats, the Rapporteur Bart Groothuis argues in its first draft report that entities may find it impossible to know if a cyber threat 'could have potentially resulted in a significant incident' [21]. Further, the Rapporteur emphasizes that a cyber threat needs to be distinguished from a report-worthy cyber incident as they are not the same thing [21]. Fear is expressed that concerns relating to compliance and liability will discourage the activities of threat hunters [21]. Accordingly, the European Parliament suggests the sharing on a voluntary basis of potential incidents and near misses with a near miss meaning 'an event which could have caused harm, but was successfully prevented from fully transpiring'.[27] Pursuant to Article 26(1) of the European Parliament Draft Resolution, a 'near miss' does not impose additional obligations but only empowers entities to exchange information.

The position of the Parliament obviously departs from the Commission Proposal when reporting is limited to incidents that have caused harm. Even though voluntary reporting is encouraged, the Rapporteur is concerned that 'medium and large entities can potentially have tens or even hundreds of significant cyber threats in a single day' and reporting these would be burdensome and may interfere with the effectiveness of the response [21]. As a compromise, the Parliament proposes that important entities (IEs), and essential entities (EEs) shall inform the recipients of their services of incidents or known risks and corresponding mitigation measures on a 'best efforts' basis.[28]

Reporting obligations under the Council's General Approach: a compromise text

In November 2021, the Council of the European Union published its position on the NIS 2 Proposal [5]. The Council Approach partly diverts from the European Parliament's Draft Resolution in terms of restricting reporting obligations: while the idea of mandatory reporting of significant cyber threats is abandoned,[29] the Council Approach retains the obligation to report incidents that (a) have caused or have the potential to cause 'severe' operational service disruption, or financial losses, or (b) have affected or have the potential to affect other natural or legal persons by causing considerable material or non-material losses.[30] As regards the voluntary reporting of near misses and cyber threats, the Council's Approach replicates the position of the Parliament. The compromise seeks to respond to concerns expressed by Member States that it would overburden entities covered by the NIS 2 Directive and lead to overreporting, if the reporting of significant cyber threats became mandatory. Instead, the Council proposes in Article 20(2) that IEs and EEs shall notify the recipients of their services that are potentially affected by a significant cyber threat of the threat and any measures or remedies that those recipients can take in response to that threat.

Reporting obligations under the final NIS 2 Directive

The NIS 2 Directive replicates the Council's General Approach on incidents that are considered to be significant and that trigger the notification obligation in its Article 23(1) and (3). Changes to the Council's compromise text mainly relate to the wording of the respective provision when 'the potential to cause/affect' is replaced by 'capable of causing/affecting'. Further, the obligation to notify the service recipient of measures or remedies that they should take in response of a significant cyber threat is adopted [Article 23(2) NIS 2 Directive]. Also, the approach to voluntary information sharing of cyber threats and near misses is maintained in Article 30 NIS 2 Directive (for an overview of the evolution see Figure 1).

It has to be noted that security requirements and reporting obligations relating to cybersecurity incidents will be deleted in some sector-specific acts so that these obligations are united under the NIS 2 umbrella.[31] This eliminates many of the issues previously encountered when determining whether a sector-specific act provides measures with equivalent effect and can therefore be deemed lex specialis under Article 1(7) NIS 1 Directive (and in the future under Article 4 NIS 2 Directive, respectively).[32]

The extended reporting obligations: challenges ahead

The new reporting obligations come at a price. In transposing the NIS Directive into national law, most Member States refrained from introducing reporting obligations that go beyond the minimum requirements of the Directive. This means that in consequence also the existing reporting infrastructure is adapted to a regime where only the most serious incidents are reported. This section addresses the general challenges ahead for Member States at an organizational level, stressing that a future increase in the number of reports can also be linked to further factors beyond a lower reporting threshold. It then assesses in how far the lowering of the reporting threshold to encompass incidents where no harm has materialized may facilitate legal compliance by eliminating some of the vagueness encountered under the NIS Directive. In that regard, it is outlined that even where reporting requirements, at a first glance, seem to be rather clear, these may give rise to problems when determining an interference in the legal sense and the line between actual harm and potential harm becomes blurred. Where lines are blurred, there is a strong likelihood that—in addition to economic reasons to refrain from reporting—this vagueness also deters entities from incident reporting. Against

27 Amendment 47 European Parliament Draft Resolution.

28 See Article 20(2) European Parliament Draft Resolution.

29 Instead Article 20(2) of the Council's General Approach foresees that 'essential and important entities shall notify, without undue delay, the recipients of their services that are potentially affected by a significant cyber threat of any measures or remedies that those recipients can take in response to that threat. Where appropriate, the entities shall also notify those recipients of the threat itself'.

30 See Article 20(3) Council's General Approach.

31 Article 42 NIS 2 Directive amends the eIDAS Regulation in that Article 19 on security requirements applicable to trust service providers is deleted with effect from 18 October 2024; Article 43 NIS 2 Directive amends Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code (EECC) in that Article 40 on security of networks and services, and Article 41 on the implementation and enforcement of Article 40 are deleted with effect from 18 October 2024.

32 As regards the assessment whether a sector-specific Union act has equivalent effect and therefore has prevalence, see [22].

	NIS Directive	European Commission NIS 2 Proposal	Parliament Draft Resolution	Council General Approach	NIS 2 Directive
Definition of incident	'any event having an actual adverse effect on the security of' NIS	'any event compromising the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the related services offered by, or accessible via,' NIS		'an(y) event compromising the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the services offered by, or accessible via,' NIS	
Reporting of incidents	Significant (OES)/substantial (DSPs) impact: harm must have materialised since effect on the continuity of the service required	Significant impact on the provision of services: incidents that • have caused/the potential to cause operational disruption or financial losses • have affected/the potential to affect other persons by causing considerable losses	Parameters to consider when determining the significance enlisted in Art. 20(3) incl. inter alia number of recipeents of the services, incident duration	Similar to NIS 2 Proposal	
Reporting of cyber threats	No	Yes, if cyber threat is significant	No, but information of service recipients of 'incidents and known risks' and measures or remedies to take	No, but information of service recipients of significant cyber threat and measures or remedies to take	

Figure 1: Overview of the evolution of reporting obligations from NIS 1 to NIS 2.

this background, the importance of notifying also incidents with 'potential harm' is highlighted.

Challenges for Member States at an organizational level

When the European Parliament's approach rejected any extension of the existing reporting obligations based on the assumption that not every incident is report worthy and the reporting of potential incidents may inhibit the effectiveness of the concerned entity's response, it also considered the challenges for competent authorities in handling the incident reports. While overreporting cannot be ruled out, no evidence has been presented that the requirement to report any 'incident that did not cause harm' challenges the handling of actual incidents. In fact, German law already foresees such reporting; yet, there is no evidence to suggest that this has resulted in overreporting. As mentioned above, the German national NIS authority only received 419 incident reports in total from June 2019 to May 2020 [18]. Further, the French regulator 'only' had to handle the aforementioned 2287 reports [17], which obviously also included incidents that only have the potential to cause harm since the German and French notification requirements are similar. One must also consider that incidents, which have the potential to cause significant harm are usually more sophisticated incidents than for instance a mere phishing attempt of which millions if not billions happen per day. A phishing attempt would neither under the NIS Directive, nor the NIS 2 Directive be report worthy since both have in common that they require that the incident has materialized, meaning in short that there must have been some interference with the confidentiality, integrity, or authenticity (CIA) of the network and information systems.[33] However, if a simple phishing attempt has been successful, the determination of the impact or potential impact is equally difficult.

Obviously, to avoid that the national competent authorities are overburdened, they need to be respectively equipped, and capable to handle incidents with significant impact in due course. In that regard, one needs to consider that the new mandatory reporting procedure follows a tiered plan with an early initial warning within 24 hours of becoming aware of a significant incident followed by the actual notification within 72 hours, an intermediate report upon request and final report at a later stage. Where applicable, the initial warning shall contain information whether the incident is 'suspected of being caused by unlawful or malicious acts' [Article 23(4)(a) NIS 2 Directive]. The new tiered notification procedure requires the national competent authority/CSIRT (depending on whether the CSIRT or authority is competent for receiving notifications) to interact with the notifying entity. According to Article 23(5) NIS 2 Directive, the competent authority/CSIRT shall provide, without undue delay and where possible within 24 hours of receiving the early warning, a response to the notifying entity, which must include initial feedback on the significant incident and, upon request of the entity, guidance or operational advice on the implementation of possible mitigation measures. The CSIRT is also tasked to provide additional technical support if the entity concerned requests such support [Article 23(5) NIS 2 Directive]. Further guidance is foreseen in the case of a criminal nature of the incident (ibid). The actual notification pursuant to Article 23(4)(b) NIS 2 Directive consists of an update of the information submitted through the early warning and should indicate an initial assessment of the incident, including its severity and impact, as well as indicators of compromise, where available. Upon request of the competent authority/CSIRT, the notifying entity may also deliver an intermediate report.

Further tasks of the competent authority/the CSIRT relate to the forwarding of information in case of cross-border impact, and to decide on whether public disclosure is necessary. This means that the authority/CSIRT is attributed an active role in the incident-handling process for which the corresponding resources are necessary.

33 The original NIS 2.0 Proposal [3] foresaw in Article 20(2) a mandatory reporting of at least 'significant' cyber threats 'that could have potentially resulted in a significant incident'. The Council compromise [5] suggested a mandatory notification of the potentially affected recipients of the services provided; this notification, however, related to the information about measures and remedies to take in response to that threat.

Besides increased engagement in the incident-handling process, national authorities will also have to adapt their capacities to the overall cyber threat scenario.

With warnings issued about soaring cyber threat levels, based on growing digitalization and most recently as a consequence of the war on Ukraine [23, 24], reports are likely to increase.

Finally, not only soaring cyber threat levels may challenge incident-handling, but also the sheer number of entities that fall under the scope of the NIS 2 Directive: new sectors are added and a uniform size-cap rule for entities that fall under the scope of the Directive is set. Article 2 NIS 2 Directive foresees that the Directive applies to public and private EEs and IEs of a type referred to in Annexes I and II of the Directive, which provide services or carry out activities within the EU and which meet or exceed the threshold for medium-sized enterprises within the meaning of Commission Recommendation 2003/361/EC.[34] Accordingly, any possibility to employ quantitative or qualitative thresholds related to the service provided is eliminated. With the size-cap rule, the increase of entities is estimated between seven-fold [25] to forty-fold [26] compared to the status quo. Accordingly, the main challenge for national competent authority relates to the number of entities that face an obligation to report incidents as well as in general, the supervision of these entities. With the foreseen tiered reporting process, in particular smaller entities may request the support and guidance that they are now entitled to.[35]

Accordingly, the NIS 2 Directive requests Member States to be adequately equipped in terms of both technical and organizational capabilities; this includes the national competent authorities and CSIRTs.

Determining the reporting threshold: the role of 'potential harm'

The NIS 2 Directive remains silent on guidance as to when an incident that has not resulted in harm is nevertheless reportable because the incident is 'capable to cause severe operational service disruption, or financial losses', or is 'capable to affect other natural or legal persons by causing considerable losses'. In how far the determination of potential significant harm will prove difficult in practice remains to be seen. In that regard, it is of interest to look at the practice of those Member States that already require such extensive reporting.

Further, reference to the mandatory data breach reporting under the GDPR with regard to a recent vulnerability serves to exemplify that the report-worthiness of an incident/breach may be judged independent from the materialization of harm. Finally, a further argument relates to state of the art security mechanisms that may result in a successful defence of an attack, but does not prevent the attack to succeed at another important or essential entity.

Determination of 'potential harm' under national legislation

As outlined above, Germany and France already require the reporting of incidents with potential harm under national legislation. In Germany, the legislator enlisted as examples for reportable incidents: vulnerabilities, malware, and attacks on the IT security even if the latter have been successfully defended [15]. As guidance, the legislator enlisted in the explanatory memorandum examples for incidents that do not require reporting, such as: daily occurrent spam, common malware that is detected by standard antivirus scanners as well as common technical defects [15]. The determination of whether the harm or potential harm has passed the threshold of significance has to be conducted by the entity. In Germany, significance may be established when incident-handling requires the designation of additional staff or assistance by third parties [15]. Entities should also ask themselves whether reporting could secure a timely warning of other potentially affected critical entities. Accordingly, for instance, the notification of a detected vulnerability that has not resulted in harm becomes reportable if third parties can be affected by the vulnerability—which, if commercial software is used, will commonly be the case.

Determination of 'potential harm' under the GDPR in the context of a vulnerability

The determination of harm may also be difficult even where a reporting obligation seems 'pretty straightforward'. This could recently be observed in the context of the GDPR. Article 33(1) GDPR requires the notification of personal data breaches to the supervisory authority unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Article 4(12) GDPR defines personal data breach as a 'breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed'. Vulnerabilities in Microsoft Exchange servers were exploited to deploy backdoors and malware in widespread attacks (Hafnium Exchange-Hack). On 2 March 2021, Microsoft released patches to tackle four critical vulnerabilities in Microsoft Exchange Server software [27]. Taking advantage of the vulnerability, meant that access to email accounts was possible and data could be compromised, which obviously interferes with privacy. The question arose whether the event had to be reported under Article 33(1) GDPR; it had to be determined whether a breach of security requires actual unauthorized access or whether it is sufficient that access is possible. A vulnerability that is still present, is still exploitable; obviously fixing a known vulnerability is a required mitigation measure [28]. Patching the system constitutes an organizational and technical measure for preventing an attack and is as such a required technical security measure under Article 32 GDPR.[36] Taking into account the EDPB Guidelines on Examples regarding Data Breach Notification [28], it becomes clear that a known vulnerability does not have to be reported to the supervisory authority where personal data has not been accessed since it does not pass the threshold of constituting a risk to the data subjects. However, the breach should be documented in accordance with Article 33(5) GDPR. As regards the aforementioned Hafnium Exchange-Hack, several German data protection supervisory authorities (DPAs) issued opinions on whether entities or individuals concerned by the vulnerability are obliged to file data breach reports. There was consensus that a report has to be filed when harm materialized, meaning that the system was actually compromised and a risk to the rights and freedoms of natural persons could be established [29, 30]. However, two DPAs went a step further, requesting a breach notification for the failure to patch the vulnerability in due time [31]. The Bavarian DPA argued that a data breach notification would be mandatory if the patch released by Microsoft on 2 March 2021 was not implemented by 9 March 2021 [31, 32]. So even if the system in place was not compromised, i.e. no advantage

34 Commission Recommendation 2003/361/EC of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises, OJ L 124, 20.05.2003, pp. 36 et seqq. Some exception applies for instance in the area of national security, public security, defence, or law enforcement.

35 Cf. [12] suggesting that SMEs need more support and guidance as they may not have the capacity to comply with the NIS Directive.

36 Article 32 GDPR requires that controller and processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk.

was taken of the vulnerability, the mere delay in patching the vulnerability was considered to create a legally relevant risk for personal data. Accordingly, even where the law requires an actual breach of security with compromised data, an unpatched vulnerability with no compromised data triggered the reporting obligation. Although the respective DPAs have been criticized [33, 34], the example perfectly highlights the difficulties of establishing the existence of an interference and actual harm or risk; Similar issues arise in the context of the reporting obligations under the NIS Directive, namely, when harm has materialized and thus reporting to authorities becomes mandatory.

The role of 'potential harm' to increase cyber resilience

The assessment of potential materialization of harm and the significance threshold are crucial for determining the obligation to report an incident. In light of the Hafnium Exchange-Hack example, the inclusion of incidents with potential harm renders it obsolete to establish a compromise of data since the mere existence of a vulnerability—which obviously interferes with the CIA of network and information systems—is sufficient to trigger a reporting obligation. This also aids the overarching goal of the NIS Directive, namely, increasing cyber resilience, which can only be achieved if there is at least a full picture of current threats and trends. The necessity to report incidents beyond those that have caused harm also becomes obvious when one takes into consideration the state of the art security mechanisms that entities have to implement under the NIS framework. In that regard, the common practices of the deployment of honeypots as security mechanisms exemplary serves to highlight the impact on reporting obligations. Honeypots are virtual traps to lure attackers, an intentionally compromised computer system allows attacker to exploit vulnerabilities so that the entity concerned can study their behaviour to improve the security of its systems. Such decoy systems inside fully operating networks and servers often form part of an intrusion detection system. In case of an infiltration, an incident in the sense of the NIS Directive could be established, but this incident only has the potential to cause harm since it takes place in a closed system. An incident that did not cause harm at one entity may still constitute a severe threat to another entity. Accordingly, where the non-materialization of harm is the result of appropriate cybersecurity mechanisms, reporting complements the evaluation of the overall threat landscape and may help to prevent, detect, and defend attacks on third-parties. As mentioned before, good detection and prevention measures depend to a large extent on regular threat and vulnerability intelligence sharing.

Concluding remarks

Recital 105 of the NIS 2 Directive states that 'a proactive approach to cyber threats is a vital component of cybersecurity risk management that should enable the competent authorities to effectively prevent cyber threats from materialising into incidents that may cause considerable material or non-material damage'. While for this purpose, the notification of cyber threats is of key importance, the same applies for the notification of incidents with potential harm. The information provided should namely enable the competent authorities not only to support the entity in handling the incident but also to prevent other entities from falling victim to an incident of the same kind. As outlined above, with no necessity to determine the materialization of harm and the new tiered reporting process, reporting is significantly be driven forward under the NIS 2 Directive.

With the NIS 2 Directive entering into force in January, it is still time to recall what the motivation of the original NIS Directive, namely, making Europe fit for the digital age where the cybersecurity threat landscape constantly evolves. The NIS 2 Directive recognizes the significant progress that had been made in increasing the EU's level of cyber resilience, but also acknowledges that it fails to effectively address current and emerging cybersecurity challenges.[37] In order to address emerging challenges, it is necessary to have a full picture of the threat landscape. Cyber situational awareness in the form of threat intelligence is a significant defence component [35]. A substantial part for the acquisition of an all-encompassing picture of current cybersecurity threats and trends is information sharing—either within specific communities or to relevant authorities. Under the minimum reporting requirements of the NIS Directive, the number of reports has been rather low and was restricted to incidents that have resulted in actual harm. The NIS 2 Directive seeks to increase the reporting by extending the obligation to report to incidents that are capable to cause substantial or considerable harm. Important and essential entities operating in the EU will in the future be obliged to report incidents irrespective whether harm has materialized. Along with the tiered reporting process with an initial warning before the actual notification, reporting is triggered at an early stage, where the entity may not even be able to identify potential harm. Further, the tiered reporting process of the NIS 2 Directive also foresees feedback by the competent authorities/CSIRTs to reports that they receive. The legislator recognizes that feedback on an incident and its handling as well as the provision of support may be far more of an incentive to report than a sanctioning regime. At the same time, the in-depth reporting seeks to provide the competent authorities with the possibility to draw valuable lesson from individual incidents and improve over time the cyber resilience of individual entities and entire sectors.[38] During the review process [12], lacking feedback on how the information provided has been handled and guidance to the industry on how to handle incidents was one of the points of criticism by OES. In light of the objectives of the Directive, reporting must become an automatism in the incident response cycle. Where entities may have previously been able to argue that, they may have struggled to establish the 'substantial' or 'significant' harm of an incident, which would have triggered the reporting obligation, issues in determining whether harm has sufficiently materialized are no longer an excuse for late or no reporting. Also, the deployment of state of the art security mechanisms and/or an effective defence of an attack no longer renders reporting obsolete, as threat intelligence information supports effective prevention, mitigation, and defence for third parties and thereby serves the overall aim of the Directive. The burden to determine whether an incident passes the significance threshold in an individual case could have further been alleviated by extending the mandatory reporting to cyber threats. However, since the entities concerned will be under an obligation to inform the recipients of their services about at least significant cyber threats, and thus go public about an identified threat, awareness on cyber threats and the threat landscape will implicitly be raised. The NIS 2 Directive also shows a clear commitment to increased threat intelligence sharing that extends to the encouragement of information sharing in trusted communities.[39]

In sum, a variety of reporting instruments, mandatory and voluntary, will definitely enhance the envisaged cybersecurity preparedness. The extension of mandatory reporting facilitates the determination

37 Cf. Recital 2 NIS 2 Directive.
38 Cf. Recital 101 NIS 2 Directive.
39 See in that regard Article 29 NIS 2 Directive.

of the reporting threshold, while the encouragement of voluntary information sharing contributes to a culture of intelligence gathering, sharing, and awareness raising. Member States are now required to prepare national competent authorities and CSIRTs with the capacities to handle incident reports. Ultimately, it is not necessarily the broad reporting obligation that will challenge national competent authorities in handling and responding to incident reports as it was feared by the European Parliament [21]; moreover, a major challenge lies ahead for national authorities with the enlarged scope of application of the Directive meaning that the number of entities under an obligation to report will tremendously increase.

Funding

This work was supported by the Luxembourg National Research Fund (FNR) [grant number C18/IS/12639666/EnCaViBS/Cole], https://www.fnr.lu/projects/the-eu-nis-directive-enhancing-cybersecurityacross-vital-business-sectors-encavibs/.

Author Contribution

Sandra Schmitz-Berndt (Conceptualization, Investigation, Methodology, Writing – original draft).

References

1. ENISA. *ENISA Threat Landscape*. 2021. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021/@@download/fullReport (13 March 2023, date last accessed).
2. BSI. *Die Lage der IT-Sicherheit in Deutschland*. 2021. https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/it-digitalpolitik/bsi-lagebericht-cybersicherheit-2021.pdf?__blob=publicationFile&v=3, (13 March 2023, date last accessed).
3. European Commission. *Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148, COM(2020)0823 (in the following NIS 2.0 Proposal*.
4. European Parliament. *Draft European Parliament Legislative Resolution on the proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148 (COM(2020)0823—C9-9442/2020—2020/0359(COD)) of 04.11.2021, A9-0313/2021 (in the following: European Parliament Draft Resolution)*.
5. Council of the European Union. *Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive 2016/1148 – General Approach*. 26 November 2021. 14337/21. (in the following: Council Approach).
6. ENISA. *Cyber security information sharing: an overview of regulatory and non-regulatory approaches*. Final version 1.0. December 2015. https://www.enisa.europa.eu/publications/cybersecurity-information-sharing/@@download/fullReport (13 March 2023, date last accessed).
7. Gal-Or E, Ghose A. The economic incentives for sharing security information. *Inform Syst Res* 2005;**92**:186–208.
8. Gordon L, Loeb M, Lucyshyn W. Sharing information on computer systems security: an economic analysis. *J Account Public Pol* 2003;**22**:461–85.
9. Laube S, Böhme R. The economics of mandatory security breach reporting to authorities. *J Cybersecur* 2016;**2**:29–41.
10. Winn JK. Are 'better' security breach notification laws possible? *Berk Tech Law J* 2009;**24**:1133–65.
11. NIS Cooperation Group. *Annual Report NIS Directive Incidents 2019*. CG Publication 03, 2020.
12. European Commission, CEPS, ICF et al. *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), No. 2020-665 final, Final Study Report*.
13. European Commission. *Report from the Commission 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 in accordance with Article 23(1) of Directive 2016/1148/EU on security of network and information systems, COM/2019/546 final*.
14. NIS Cooperation Group. *Guidelines on Notification of Operators of Essential Services Incidents. Circumstances of Notification*. CG Publication 02, 2018.
15. Deutscher Bundestag. BT-Drs. 18/4096. 25 February 2015.
16. ENISA. *Incident notification for DSPs in the context of the NIS Directive*. 27 February 2017. https://www.enisa.europa.eu/publications/incident-notification-for-dsps-in-the-co,ntext-of-the-nis-directive/at_download/fullReport (13 March 2023, date last accessed).
17. ANSSI. *Press release*. 10 June 2021. https://www.ssi.gouv.fr/uploads/2021/06/anssi-press_release-anssi_is_looking_to_the_future.pdf (13 March 2023, date last accessed).
18. BSI. *Die Lage der IT-Sicherheit in Deutschland*. 2020. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2020.pdf?__blob=publicationFile&v=2 (13 March 2023, date last accessed).
19. CERT.be. *Number of notifications CERT.be increased. Press release*. 19 January 2021. https://cert.be/en/news/number-notifications-certbe-increased (13 March 2023, date last accessed).
20. Bitkom. *Bitkom position on the proposal for a renewed Directive on security of network and information systems*. 2021. https://www.bitkom.org/sites/default/files/2021-03/210318_pp_nis-directive-2.pdf (13 March 2023, date last accessed).
21. European Parliament, Committee on Industry, Research and Energy. *Draft Report on the proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148 (COM(2020)0823—C9-9442/2020—2020/0359(COD)) of 03.05.2021, 2020/0359(COD) (in the following ITRE Draft Report)*.
22. Ducuing C. Understanding the rule of prevalence in the NIS Directive: C-ITS as a case study. *Comput Law Secur Rev* 2021;**40**:105514.
23. BSI. *Einschätzung der aktuellen Cyber-Sicherheitslage in Deutschland nach dem Russischen Angriff auf die Ukraine. Press release*. 04 March 2022. https://www.bsi.bund.de/DE/Service-Navi/Presse/Pressemitteilungen/Presse2022/220225_Angriff-Ukraine-Statement.html (13 March 2023, date last accessed).
24. Kolby PR, Morrow M R, Zabierek L. The cybersecurity risks of an escalating Russia–Ukraine conflict. *Harv Bus Rev* 24 February 2022. https://hbr.org/2022/02/the-cybersecurity-risks-of-an-escalating-russia-ukraine-conflict (13 March 2023, date last accessed).
25. European Commission, Commission Staff Working Document. *Impact Assessment Report, SWD (2020) 345 Final, Part 1/3*.
26. Cyber Security Coalition. *NIS-2: Where are you?* 30 April 2022. https://www.cybersecuritycoalition.be/nis-2-where-are-you/ (13 March 2023, date last accessed).
27. Osborne C. Everything you need to know about the Microsoft Exchange Server Hack. *Zdnet* 19 April 2021. https://www.zdnet.com/article/everything-you-need-to-know-about-microsoft-exchange-server-hack/ (13 March 2023, date last accessed).
28. EDPB. *Guidelines 01/2021 on examples regarding data breach notification*. 2021. https://edpb.europa.eu/sites/default/files/consultation/edpb_guidelines_202101_databreachnotificationexamples_v1_en.pdf (13 March 2023, date last accessed).
29. Heidrich J. Exchange-hack: uneinheitliche Position der Datenschutzbehörden zur Meldepflicht. *Heise Online* 11 March 2021. https://www.heise.de/news/Exchange-Hack-Uneinheitliche-Position-der-Datenschutzbehoerden-zur-Meldepflicht-5078453.html (13 March 2023, date last accessed).
30. Hessel S. 'Hafnium' vulnerabilities in Microsoft Exchange: duty of notification and communication in accordance with the GDPR? *Reuschlaw*

March 2021. https://www.reuschlaw.de/en/news/hafnium-vulnerabilities-in-microsoft-exchange-duty-of-notification-and-communication-in-accordanc/ (13 March 2023, date last accessed).
31. BayLdA. *Sicherheitslücken bei Microsoft Exchange-Mail-Servern: Akuter Handlungsbedarf für bayerische Unternehmen—BayLDA empfiehlt: Patchen, Prüfen, Melden!. Press release*. 09 March 2021. https://www.lda.bayern.de/media/pm/pm2021_01.pdf (13 March 2023, date last accessed).
32. BayLdA. *Sicherheitslücken bei Microsoft Exchange-Servern: Weiterhin akute Datenschutzrisiken*. Press release. 18 March 2021. https://lda.bayern.de/media/pm/pm2021_02.pdf (13 March 2023, date last accessed).
33. Hessel S, Potel K. Aktuelle Entwicklungen bei der datenschutzrechtlichen Bewertung von Sicherheitsvorfällen. In: Taeger J (ed.), *Im Fokus der Rechtsentwicklung—Die Digitalisierung der Welt*. Oldenburg: OlWiR, 2021, 279–88.
34. Bitkom. Datenschutzverletzung und Meldung im Kontext des 'Hafnium Hacks'—Leitfaden. 2021. https://www.bitkom.org/sites/default/files/2021-04/210407_datenschutzverletzungen.pdf (13 March 2023, date last accessed).
35. Shin B, Lowry PB. A review and theoretical explanation of the 'Cbyerthreat-Intelligence (CTI) Capability' that needs to be fostered in information security practitioners and how this can be accomplished. *Comput Secur* 2020;**92**:101761.