# Incident notification for DSPs in the context of the NIS Directive

A comprehensive guideline on how to implement incident notification for Digital Service Providers, in the context of the NIS Directive

FEBRUARY 2017

www.enisa.europa.eu European Union Agency For Network and Information Security

# About ENISA

The European Union Agency for Network and Information Security (ENISA) is a centre of network and information security expertise for the EU, its member states, the private sector and Europe's citizens. ENISA works with these groups to develop advice and recommendations on good practice in information security. It assists EU member states in implementing relevant EU legislation and works to improve the resilience of Europe's critical information infrastructure and networks. ENISA seeks to enhance existing expertise in EU member states by supporting the development of cross-border communities committed to improving network and information security throughout the EU. More information about ENISA and its work can be found at www.enisa.europa.eu.

## Contact

For queries in relation to this paper, please use incidents@enisa.europa.eu
For media enquires about this paper, please use press@enisa.europa.eu.

### Legal notice

Notice must be taken that this publication represents the views and interpretations of ENISA, unless stated otherwise. This publication should not be construed to be a legal action of ENISA or the ENISA bodies unless adopted pursuant to the Regulation (EU) No 526/2013. This publication does not necessarily represent state-of the-art and ENISA may update it from time to time.

Third-party sources are quoted as appropriate. ENISA is not responsible for the content of the external sources including external websites referenced in this publication.

This publication is intended for information purposes only. It must be accessible free of charge. Neither ENISA nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication.

### Copyright Notice

ISBN 978-92-9204-204-2, doi 10.2824/002714

# Table of Contents

Executive Summary 4

1. Introduction 6

1.1 Goal and Objectives 6

1.2 Target audience 6

1.3 Methodology 6

1.4 Terminology 7

2. General information about the NISD 8

2.1 Background of the NISD 8
2.1.1 Short history 8
2.1.2 Overview 8
2.1.3 The light-touch approach 9

2.2 Stakeholders involved 10
2.2.1 Digital service providers (DSPs) 10
2.2.2 National authorities 14
2.2.3 Cooperation group 15
2.2.4 CSIRTs Network 15
2.2.5 ENISA 16
2.2.6 EU Commission 16

3. Incident notification process for DSPs 17

3.1 The NISD incident notification provisions for DSPs 17
3.1.1 Incident notification as part of the overall incident management process 18

3.2 Types of incidents covered by the NIS directive 19

3.3 Parameters used to measure impact of incidents 22
3.3.1 Number of users affected by the incident 23
3.3.2 Duration of the incident 25
3.3.3 Geographical spread 25
3.3.4 Extent of the disruption of the functioning of the service 26
3.3.5 Extent of the impact on economic and societal activities 27
3.3.6 Other issues related to parameters 27

3.4 Determining substantial incidents 28
3.4.1 Proposed procedure/algorithm for determining the impact of incidents 29

4. Conclusions 31

Annex A - Proposal on how to determine the impact of incidents 33

# Executive Summary

The NIS Directive is the first piece of EU legislation specifically aimed at improving cybersecurity throughout the Union. By ratifying a definite number of obligations across the EU, the Directive will help ensure a consistent approach to cybersecurity *"with a view to achieving a high common level of security of networks and information systems within the Union so as to improve the functioning of the internal market".* The main points of the NIS Directive can be summarised as follows: **improved cybersecurity capabilities at national level, increased EU-level cooperation, security measures and incident reporting obligations for Operators of Essential Services (OES) and Digital Service Providers (DSP).** The scope of this study is limited to relevant provisions of the NIS Directive on Digital Service Providers (DSPs) and their current activities in this field.

According to one of the provisions of the NISD, Member States must ensure that DSPs notify the competent authority without undue delay of any incident having a substantial impact on the provision of a service. In determining the "substantial impact", the Directive mentions just five indicators to be used without providing other details.

As the Directive provides only a sketchy description of the incident notification concepts and the overall process, the main goal of this document is to develop a set of guidelines for all concerned stakeholders (EU level authorities, public, private), aimed at supporting the implementation of the NIS Directive requirements regarding mandatory incident notification for Digital Service Providers.

A useful description of the roles and responsibilities of all stakeholders involved is provided. From DSPs to EU level bodies involved, each part plays an important role in securing EU's cyber future. National authorities are responsible for managing the process at their level, while the Cooperation Group is established as a body that will support and facilitate strategic cooperation and the exchange of information among Member States. The interaction between involved bodies becomes crucial as the information flow regarding incidents must be properly assured throughout EU.

Establishing a clear view of the incident notification process, is a must for a proper implementation. Such a view, compiled from all requirements of the Directive, is included in this document. Certain aspects such as the main EU establishment of an DSP, cross border cooperation, the public awareness about incidents, relationship with law-enforcement are all explained. For a better understanding, the possible place occupied by the mandatory incident notification process within the generic incident management practices is explained.

Knowing what incidents have to be reported is equally important in the reporting process. As the Directive provides only some theoretical concepts that must be followed when reporting incidents, the current guidelines give an exhaustive description of the incident types covered by the NISD.

Further on, clarifications on the parameters that must be used when notifying are also important in the reporting process. The notions provided by the Directive are supplemented with technical interpretations and tips on how to apply them. A simple notion as "number of users" can raise multiple issues when trying to apply it to search engines or cloud providers.

Although at first sight we might consider the incident reporting topic as straightforward and easy-going, the current study has uncovered serious issues that must be addressed while implementing the DSP incident reporting provisions of the NISD. The multitude of technical approaches mirrored the numerous discrepancies between types of DSPs and the corresponding business models adopted, thus creating a deep pool of sometimes incompatible variables that must be taken into account when approaching such a regulation. For example, a simple parameter imposed by the Directive, such as "number of users", can mean different things to different types of providers, from simple visitors or registered individuals to corporate users and dependant services.

EU's first DSP incident notification requirements as part of the first EU wide set of rules on cyber-security are a major step forward towards achieving a common level of cyber-security across the Union. In a perpetually fluctuating technological landscape that affects our livelihoods while having increasing economic and societal impact as a whole, a first step, in understanding the real threats and vulnerabilities that we have to confront, has been taken through the adoption of the NISD along with its two main requirements: mandatory incident notification and minimum security measures. From now on, a "small steps" approach must be applied in implementing the Directive, that has to undergo periodic reviews and updates.

This document provides preliminary guidelines on how incident notification provisions for DSPs could be effectively implemented across the EU. Based on valuable input from Member States and companies directly impacted by the Directive, this guideline arises from their good practices in matters such as identifying types of incidents, parameters and thresholds. The overall result is an outline technical proposal that can tentatively be used in the implementation process.

At the same time, this guideline serves as a technical input to the foregoing process of adopting the implementing act that will further specify details regarding the incident notification provisions of the NISD.

# 1. Introduction

## 1.1 Goal and Objectives

The main goal of this document is to develop a set of guidelines for all concerned stakeholders (EU level authorities, public, private), aimed at supporting the implementation of the NIS Directive (hereafter referred to as "the Directive" or "NISD") requirements regarding mandatory incident notification. The scope of this study is limited to relevant provisions of the NIS Directive on Digital Service Providers (DSPs) and their current activities in this field.

## 1.2 Target audience

The target audience of this work is as follows:

- EU Commission, as this document will serve as a technical input to the process of defining the implementing act following up the Directive.
- Relevant EU national authorities, as this document can provide guidelines and good practices for implementing the NISD provisions at national level.
- Digital Service Providers (DSPs), as this document can provide guidelines and good practices on properly implementing the NISD provisions at provider level.

## 1.3 Methodology

The underlying study presented in this report involved a three-tiered methodology, thus consisting of a primary desktop research reviewing the relevant literature, a subsequent online questionnaire-based information-gathering tier that included DSPs and national authorities as interviewees, and a final set of in-depth interviews to address more nuanced and detailed issues that could not have been captured in the survey. The approach aimed to collect all the available information regarding the practices employed by EU national agencies and DSPs in their capacity of incident management and response actors as well as their views on how incident notification could be implemented efficiently in the context of the provisions prescribed by the NISD. This approach facilitated the structuring of a basic documentation that was later adjusted within the context of the NIS Directive (NISD) and based on previous ENISA expertise in the area on incident reporting.

| | |
|---|---|
| Number of participants member states | 22 |
| Number of participants DSPs | 20 |
| Additional documentation used | ENISA work within the areas:<br>- Incident reporting for telecom sector (Art. 13a).<br>- Incident reporting for trust services providers (Art. 19 eIDAS). |

**NOTE**: ENISA generally employs in-depth ***QUALITATIVE ANALYSIS*** (deep dive) to describe, in detail, specific situation using policy analysis tools such as interviews, surveys and desktop research and provide insights into the problem or helps to develop ideas or hypotheses for potential quantitative research. ENISA is not a research agency and does not engage in extensive statistical analyses. ENISA is a technical advisory agency to the European Commission and to the EU Member States and, in this capacity, uses the simplest appropriate methods to measure variables that are conclusive for the decision making process and for policy implementation. Therefore, the agency's focus is not that the samples used ought to be statistically significant but that the policy process involves all relevant stakeholders and that the consultation process is comprehensive and thorough. Policymaking and policy implementation generally involve a constant bargaining process between decision makers and policy implementers, and here is where ENISA engages in enhancing the constructive dialogue and clarifying technicalities in order to increase the chances of smooth implementation and achievement of policy goals.

## 1.4 Terminology

| | |
|---|---|
| Digital service | Service within the meaning of point (b) of Article 1(1) of directive (EU) 2015/1535 of the European Parliament and of the Council1 which is of a type listed in Annex III |
| Digital Service Provider (DSP) | Any legal person that provides a digital service |
| Essential Services | Services essential for the maintenance of critical societal and economic activities. |
| Incident | Any event having an actual adverse effect on the security of network and information systems |
| Incident handling | All procedures supporting the detection, analysis and containment of an incident and the response thereto |
| Incident impact | All effects of the incident concerning confidentiality, integrity or availability of information, assets or services. Impact may be described in a qualitative or quantitative way |
| Incident parameters | Set of incident characteristics which allow to unambiguously identify specific incident and allow to effectively handle the incident through the entire incident management process |
| Incident Reporting | Part of incident Management process involving the information sharing between the organization affected by a cyber-incident and relevant authority responsible for gathering information about cyber incidents and, in some cases, also for incident mitigation. Used interchangeably with incident notification in the current document. |
| Incident threshold | Specific kind of incident sub - parameter used to measure incident impact in an objective manner. Incident thresholds are used combined with measurable parameters, each parameter may have its individual thresholds assigned to indicate the level of impact. |
| Incident type/category | One of incident parameters describing the general type/category of incident. Incident type/category is assigned during the incident categorization |
| Network and information system | An electronic communications network within the meaning of point (a) of Article 2 of directive 2002/21/EC. Any device or group of inter–connected or related devices, one or more of which, pursuant to a program, perform automatic processing of digital data. Digital data stored, processed, retrieved or transmitted by elements covered under points (a) and (b) for the purposes of their operation, use, protection and maintenance |
| Network and information security directive (NIS Directive od NISD) | The NIS Directive is the first piece of EU legislation specifically aimed at improving cybersecurity throughout the Union. This in itself represents a very significant step in the approach to securing EU information systems. Full text here. |
| Representative | Any individual or legal person established in the Union explicitly designated to act on behalf of a digital service provider not established in the Union, which may be addressed by a national competent authority or a CSIRT instead of the digital service provider with regard to the obligations of that Digital Service Provider under this directive. |
| Stakeholders | All entities that are directly or indirectly affected by provisions of NIS directive |

# 2. General information about the NISD

## 2.1 Background of the NISD

### 2.1.1 Short history

The current approach to CIIP and resilience within the EU has its roots in the Commission Communication of 2009 entitled 'Protecting Europe from large-scale cyber-attacks and disruptions: enhancing preparedness, security and resilience '[1], together with a number of accompanying policy documents that essentially built up and further refined this approach.[2][3][4]

Subsequently, in 2013, the Commission released the Cybersecurity Strategy of the EU[5], which laid out a number of fundamental principles underlying the EU approach to cybersecurity followed by 5 strategic priorities. The proposal for the NIS Directive was thus made under the first strategic priority 'Achieving Cyber resilience'.

From 2013 through to 2015, the Commission, the Parliament and the Council, in the framework of the EU legislative process, discussed the Directive intensely. Consequently, the European institutions reached an informal political agreement on the NIS Directive on December 7, 2015. Member States (the Committee of Permanent Representatives (COREPER)) endorsed this agreement on December 18. On January 14, the European Parliament's IMCO committee voted in favour of the NIS Directive (34-2).

The Directive entered into force in August 2016, and the Member States must transpose it to national legislation by May 9, 2018.

### 2.1.2 Overview

The NIS Directive is the first piece of EU legislation specifically aimed at improving cybersecurity throughout the Union. This in itself represents a very significant step in the approach to securing EU information systems.

By ratifying a definite number of obligations across the EU, the Directive will help ensure a consistent approach to cybersecurity *'with a view to achieving a high common level of security of networks and information systems within the Union so as to improve the functioning of the internal market'.*

The main points of the NIS Directive can be summarised as follows:

- **Improved cybersecurity capabilities at national level:** Each Member State should take actions in the following areas:
  - Adopt a **national strategy on the security of network and information systems** defining the strategic objectives and appropriate policy and regulatory measures.
  - Designate one or more **national competent authorities** for the NIS Directive and a national single point of contact, to monitor the application of the Directive at national level.

[1] Commission Communication of March 2009, "Protecting Europe from large-scale cyber-attacks and disruptions: enhancing preparedness, security and resilience", COM (2009)149.

[2] "Achievements and next steps: towards global cyber-security" adopted on 31 March 2011 and the Council Conclusion on CIIP of May 2011 ( http://register.consilium.europa.eu/pdf/en/11/st10/st10299.en11.pdf )

[3] Council resolution of 18 December, 2009 'On a collaborative approach to network and information security (2009/C 321 01)

[4] Council Conclusion on CIIP of May 2011 ( http://register.consilium.europa.eu/pdf/en/11/st10/st10299.en11.pdf )

[5] Joint Communication on the Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, available at: http://eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_en.pdf

  - Designate one or more **Computer Security Incident Response Teams** (CSIRTs) for comprehensive incident management nationwide.
- **Increased EU-level cooperation:**
  - **Establishes an EU level** Cooperation Group, to support and facilitate strategic cooperation and the exchange of information among Member States and to develop trust and confidence.
  - Establishes an EU level network of the national CSIRTs and CERT-EU, in order to contribute to the development of confidence and trust between the Member States and to promote swift and effective operational cooperation. ENISA will provide the secretariat of the group.
- **Security measures and incident reporting obligations for operators of essential services and digital service providers:**
  - Identified operators of essential services (OESs) and digital service providers (DSPs) will have to take appropriate security measures and to notify serious incidents to the relevant national authority.

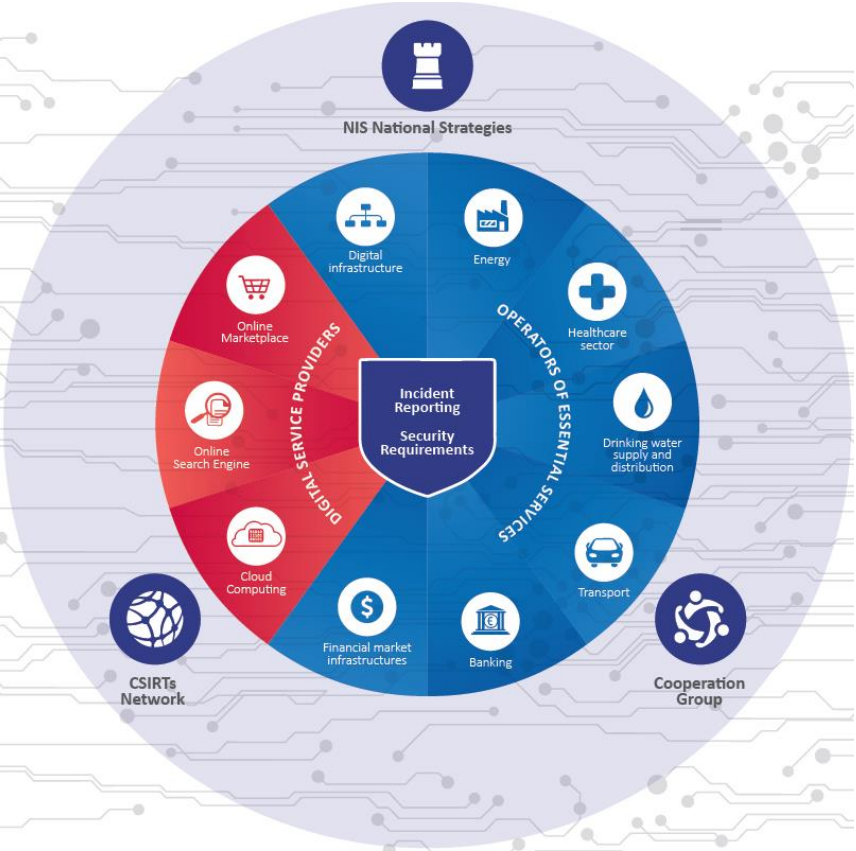

Fig. 1 - Graphical overview of the NIS Directive.

### 2.1.3 The light-touch approach

In light of the NISD provisions, it is considered that the operators of essential services (OES) are critical for the proper functioning of the internal market. On the other hand, DSPs, as first hand providers for the OES, should have lighter provisions in place, i.e. not as strict as the OES. To this extent, a light-touch approach is deemed appropriate for DSPs.

Although recital 60 of the NISD introduces the concept of light-touch approach and reactive ex-post supervisory activities, the notions were not perceived by the community as being sufficiently explained, leaving plenty of room for interpretation. Amongst the related references, we could mention “competent authority concerned should therefore only take action when provided with evidence […] that a digital service provider is not complying with the requirements of this Directive, in particular following the occurrence of an incident.

The competent authority should therefore have no general obligation to supervise digital service providers"[6].

However, applying a light touch approach should not prevent a specific authority from being fully able to exercise its supervision authority upon a DSP, should the case require it. For example, applying fewer provisions for DSPs as compared to OES might not be beneficial if certain limits are exceeded. Overall, securing the unabridged chain of services that support the internal market should be the top priority when implementing the NISD.

In this respect, the light-touch approach aims at avoiding overburdening the DSPs while not hampering the capacity of the EU to react to cybersecurity incidents in a swift and efficient manner. Therefore, there are reasons to be concerned that a significant lowering in the requirements of incident notification (types of incidents, parameters to be used) could result in hindering the capacity (at EU or national level) to follow up on specific incidents threatening the functioning of the internal market at various levels. For instance, a hostile attack (or even a malfunction) that affects a financial system by means of a number of anomalies produced at the level of a specific cloud service provider (that provides services to the financial system) might not be appropriately comprehended if not all accountable entities went by the same incident reporting policies. The financial entity would then report issues related to the could provider, but the reporting system would not allow a clear and full understanding of the overall causes that led to damages to the internal market.

The prevalent understanding of the 'light-touch' approach is as follows:

- Member States are not allowed to impose any further security or notification requirements on digital service providers, besides the ones foreseen in the directive (Art. 16 (10) ).
- Jurisdiction is based on the criteria of main establishment of a DSP within only one Member State, meaning that it has to comply only with the national rules of one MS. (art. 18). If the DSP does not have an establishment within EU, it can choose one Member State.
- Only ex-post supervision is allowed from the competent authority (art. 17 (1) ), when provided with evidence that a digital service provider does not meet the requirements laid down in Article 16. There is no general obligation to supervise digital service providers on a regular basis.
- The minimum security requirements for DSPs should be lighter than those of the OES, and they should remain free to take the measures that they deem appropriate.

This interpretation of the light-touch approach was presented by Commission's representatives, during ENISA's Network and Information Security Workshop in Bratislava, 17-18.10.2016.

## 2.2 Stakeholders involved

The DSPs incident notification process, as described by the NISD, exposes a number of stakeholders involved. This subchapter identifies them, for a better understanding of their role.

### 2.2.1 Digital service providers (DSPs)

A "digital service" is defined by the Directive (EU) 2015/1535 as "any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services"[7]. Nonetheless, for the scope of the NISD, DSPs are limited to only three types of services: cloud, online market places and search engines.

Their inclusion within the NISD is not purposeless as the aim of the directive is to "achieve a high common level of security of network and information systems within EU, so as to improve the functioning of the

[6] NIS Directive, Recital 60.

[7] point (b) of Article 1(1) of Directive (EU) 2015/1535.

internal market". Given that most of these systems are privately operated, their inclusion in the provisions of the NISD was more than necessary. As they are the owners or administrators of the underlying systems of what we currently name Internet or Digital Society, it is reasonable to believe that they have to play an important role in assuring the cyber-security of our digital market and they will be the first ones having to adopt measures. Recitals 35 and 44 of the NISD provide some insights in this respect.

Baseline security measures and mandatory incident notification will be applied to DSPs within the context of the NIS Directive. Further explanations on DSPs and their services can be found in section 2.2.1.

Digital Service Providers (DSPs) as for the purpose of the Directive are providers of the following three types of digital services: online marketplace, online search engine, cloud-computing service. The main technical characteristics of a digital service, as defined by Directive (EU) 2015/1535 are the following:

- Offered at a distance.
- Offered by electronic means.
- Offered at the individual request of the recipient of services.

These three particular types of DSPs were selected for regulation through the NISD due to their importance (or, better said, criticality) for the smooth functioning of many EU businesses (internal market). As mentioned by recital 48 of the Directive "*a disruption of such a digital service could prevent the provision of other services which rely on it, and could, thus have an impact on key economic and societal activities in the Union. Such digital services might therefore be of crucial importance for the smooth functioning of businesses that depend on them and, moreover, for the participation of such businesses in the internal market and cross-border trade across the Union*". To conclude, the three types of services were chosen to be regulated due to the increasing number of businesses carried on in the Union that fundamentally rely on them for the provision of their own services.

Given their cross-border nature, recital 57 states that Member States should not proceed with any identification of the DSPs as the directive will apply to all providers in scope. Yet, the directive refers chiefly to their legal identification, which should be carried out through the Directive itself or its subsequent implementing acts. Nonetheless, the technical identification and classification is a necessity for every national authority, so that cases where DSPs evade the provisions of the Directive (because of improper identification) can be avoided.

The identification is a critical issue due to the cross-border nature of the providers. One provider can operate within many Member States but with only one main establishment within the Union, as explained by recital 64. In such cases, the national authority supervising the main establishment is responsible for overseeing the activities of the particular DSPs and the services provided in the EU.

Given the light touch approach for DSPs, micro and small businesses will be excluded from implementing the NISD. Governmental services (i.e. cloud) are also excluded from the NISD.

The following subchapters represent a non-binding technical description that aims at supporting national authorities in properly identifying, from a technical point of view, the DSPs and their provisioned services, in the specific context of the NISD.

#### 2.2.1.1 Online market places

Recital 15 and art. 4. (17) of the NISD try to shape a definition of online market places meaning services that "allow consumers and traders to conclude online sales or service contracts with traders, and is the final destination for the conclusion of those contracts". Intermediaries and price comparison services are excluded from this definition, leaving only platforms where the actual online shopping can be concluded. There are no special provisions as to what can be sold through online market places, so it applies to all types of contracts (products and services). Although from a technical perspective most online marketplaces use a website or web related technologies for delivering their services, it should not be a restriction in this sense, as mobile application stores make use of other technologies also.

The technical identification of online market places should not be an issue, as all necessary details are provided by the regulation itself.

Below you can find a series of example lists of online marketplaces. These lists are not exhaustive and are only provided for illustrative purposes, and should not, by any means, be taken as exhaustive when implementing the NISD.

- https://en.wikipedia.org/wiki/List_of_mobile_software_distribution_platforms
- https://en.wikipedia.org/wiki/List_of_online_marketplaces
- http://myappmag.com/online-shopping-websites/
- http://www.techradar.com/news/internet/the-uk-s-top-100-shopping-websites-603428

#### 2.2.1.2 Search engines

Recital 16 together with art. 4 (18) provide a comprehensive definition of search engines: "a digital service that allows users to perform searches of, in principle, all websites or websites in a particular language on the basis of a query on any subject in the form of a keyword, phrase or other input, and returns links in which information related to the requested content can be found". It is also very clearly mentioned that search functionalities limited to in-site search and price comparison websites should not be considered search engines.

Therefore, the technical identification of search engines is not considered problematic.

The link below provides a sample list of search engines. The list is not exhaustive and only for illustrative purposes, and should not be taken as exhaustive when implementing the NISD:

- https://en.wikipedia.org/wiki/List_of_search_engines

#### 2.2.1.3 Cloud computing services

Recital 17 and art. 4 (19) provide a clear and straightforward theoretical definition of cloud computing.

The cloud computing is a particular type of computing service that uses shared resources in order to process data on-demand. Through the shared resources, we hereby refer to any kind of hardware or software components (e.g. networks, servers or other infrastructure, storage, applications and services) that are released on-demand to users for processing data. The NISD mentions three properties that a cloud computing service must display in order to be technically identified as a cloud service:

- ***shareable computing resources***: *computing resources that are provided to multiple users who share a common access to the service, but where the processing is carried out separately for each user, although the service is provided from the same electronic equipment*. In a nutshell, when many users are utilizing the same physical infrastructure for processing data the first property is met.
- ***scalable resources***: *computing resources that are flexibly allocated by the cloud service provider, irrespective of the geographical location of the resources, in order to handle fluctuations in demand*. This means that the pool of resources used by the provider can be extended or reduced at any time, depending on the user requirements. Thus, data centres or single components within one data centre could possibly be added or removed if the total amount of computing or storage capacity needs an update.
- ***elastic pool of resources***: *computing resources that are provisioned and released according to demand in order to rapidly increase and decrease resources available, depending on workload.* A more straightforward definition could be: "the degree to which a system is able to adapt to workload

changes by provisioning and de-provisioning resources in an autonomic manner, such that at each point in time the available resources match the current demand as closely as possible"[8].

ENISA has been covering the cloud area for several years now[9]. Comprehensive guidelines on specific topics within the cloud area can be found here. Seemingly, one useful guideline on the basics of cloud computing can be found here.

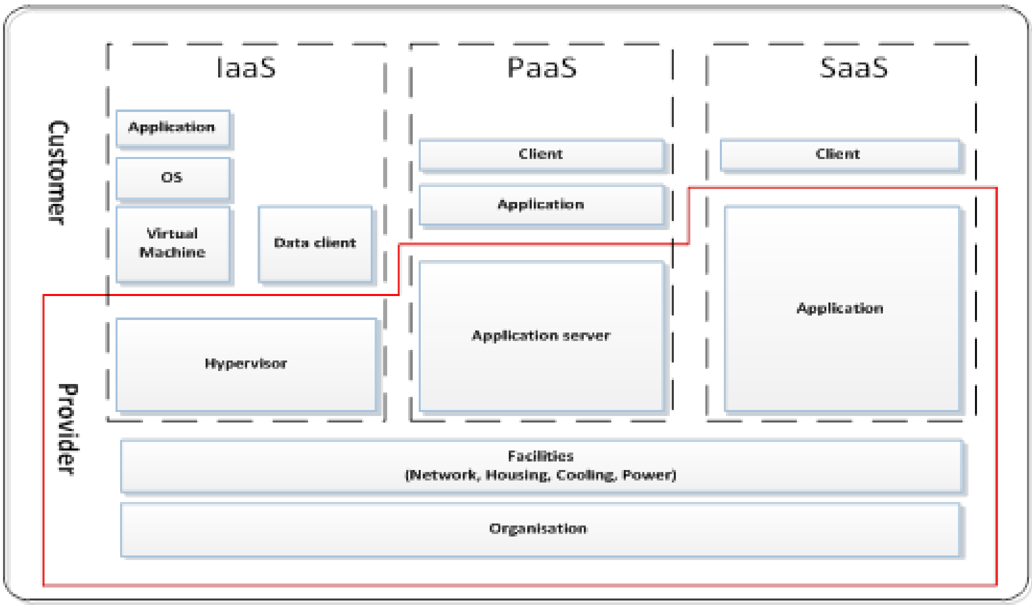

Fig. 2 – Service models and assets in cloud computing

One provider can apply three classic cloud service models[10], as listed below. Since the NISD did not exclude any of the three, the provisions will be applicable to each type of service model.

- **Infrastructure as a Service (IaaS)**: the provider delivers computing resources (virtual hardware), accessible online. There are two types of resources: processing power (including network resources), and (block) storage (memory resources). In this model, the user usually has access to components such as virtual machines, physical servers, storage, load balancers, network equipment etc. Examples include Amazon's Elastic Compute Cloud, Google's Compute Engine, Amazon Simple Storage Service, Rackspace etc.

  An indicative list of IaaS providers in the EU can be found here.

- **Platform as a Service (PaaS)**: the provider delivers a platform, or more precisely, servers, for customers to run applications on. PaaS providers sometimes offer a software development tool for the platform. Examples of applications running on these platforms are scripts (PHP, Python, e.g.) or byte code (Java servlets, C#). In this model, the user usually has access to components such as web servers, application servers, development tools, databases etc. Examples include Google App engine, Microsoft Azure, Amazon Elastic Beanstalk, etc.

[8] Nikolas Roman Herbst, Samuel Kounev, Ralf Reussner, Karlsruhe Institute of Technology, "Elasticity in Cloud Computing: What It Is, and What It Is Not", available at: https://sdqweb.ipd.kit.edu/publications/pdfs/HeKoRe2013-ICAC-Elasticity.pdf
[9] https://www.enisa.europa.eu/topics/cloud-and-big-data/cloud-security
[10] ENISA, Could Security Guide for SMEs, available at: https://www.enisa.europa.eu/publications/cloud-security-guide-for-smes

An indicative list of PaaS providers in the EU can be found here.

- **Software as a Service (SaaS)**: the provider delivers full-fledged software or applications, via the internet. Applications range from email, document editors, customer relationship management (CRM) systems, virtual desktops, games and so on. SaaS can often be accessed with a browser or a web services client. Duly note should be taken that it is quite common for SaaS providers to run their applications on an IaaS or PaaS from another provider. An example is the video streaming site Netflix (SaaS) which runs on Amazon AWS computing services (PaaS/IaaS).

There are also several classic cloud deployment models. Although the technical architectures are similar (even identical in some cases) the business model applied provides the following classification:

- **Public cloud**: Typical cloud open to the public (individuals and companies), generally accessible from the Internet.
- **Private cloud**: a cloud operated for a single organisation. Typical for large organisations that want to remove some privacy or other security related concerns that characterize public clouds.
- **Hybrid cloud**: A mixture between public and private (e.g. private cloud making use of several functionalities offered by a public cloud).
- **Community cloud**: cloud used by several stakeholders/organisations (e.g. within the same industry).

The NISD does not differentiate the various deployment models, but considering the definition of the digital service (see 2.2.1) we can sensibly conclude that the Directive aims at regulating mainly the public clouds. Nevertheless, depending on particular circumstances, hybrid and community clouds can also be included in the NISD provisions.

### 2.2.2 National authorities

As main responsible for driving, improving and securing the digital market, national governments are also considered key stakeholders in assuring the security of network and information services. They are accountable for developing the legal and institutional framework capable of managing the security of their national digital market. Thus, from identifying the key players and current threats to imposing minimum security measures and mandatory incident notification requirements, their overall role is to ensure that the level playing field (in terms of cyber-security) at the national level is achieved.

Moreover, national authorities are all governmental bodies operating at national level that are responsible for the implementation and monitoring of the NIS directive. Consequently, according to the directive, each Member State shall assign at least three roles relevant for network and information security. These roles are as follows:

- **Single point of contact**: each Member State shall designate a national single point of contact on the security of network and information systems that shall exercise a liaison function to ensure cross–border cooperation with the relevant authorities in other Member States and with other EU level bodies. Member States may assign this role to an already existing authority. Where a Member State will designate only one competent authority, that competent authority shall also be the single point of contact.
- **National CSIRT**: Each Member State must designate one or more CSIRTs, which shall comply with the requirements set out in point (1) of Annex I to the Directive, covering at least the sectors referred to within the directive (shown in Fig. 1).
- **National competent authorities**: in order to cover all requirements of the NISD, all Member States must designate one or more national competent authorities on the security of network and information systems covering at least the sectors referred to in Annex II and the services referred to in Annex III. Countries can decide for nominating just one authority covering all sectors and services described in the NISD, or many covering specific areas/sectors/services.

Therefore, as inferred from the text of the Directive, several configurations are possible. Member States can have only one body covering all requirements (it must be a national CSIRT, a single point of contact and cover all sectors), two or more bodies, splitting the roles amongst each other.

### 2.2.3 Cooperation group

As defined within the Directive, the role of the Cooperation Group (CG) is to support and facilitate ***strategic cooperation*** and the exchange of information among Member States and to develop trust and confidence. As cross-border cooperation is a key factor in achieving an EU wide high common level of security of networks and information systems, the existence of this group is a real necessity.

The CG shall be composed of Member States representatives, the EU Commission and ENISA. The Commission shall provide the Secretariat. Where appropriate, the Cooperation Group may invite representatives of the relevant stakeholders to participate to its works.

Among the tasks that fall within the CG's competencies are:

- Provide strategic guidance for the activities of the CSIRT network.
- Exchange best practices on topics related to: capacity building, incident notification, security measures, awareness raising, training, R&D.
- Discuss capabilities and preparedness of Member States.
- On a voluntary basis, evaluate national strategies on the security of network and information systems and the effectiveness of CSIRTs.
- Collect and examine, on an annual basis, the incident summary reports sent by Member States.
- -
- Discuss about standardization issues with representatives from the relevant European Standardization Organizations.
- Exchanging best practice with regard to the identification of operators of essential services by the Member States, with ENISA's assistance.

### 2.2.4 CSIRTs Network

The work undergone at the strategic level by the CG is to be complemented by a technical/operational part developed by the CSIRTs network. The official role of the CSIRTs network is to contribute to the development of confidence and trust between the Member States and to promote effective ***operational cooperation***.

The CSIRTs network is composed of representatives from Member States' national CSIRTs, ENISA and CERT–EU. ENISA will provide the secretariat of the group and the Commission can take part in the network as an observer.

Among the tasks that fall within the CSIRTs Network's competencies are:

- Exchange information on services, operations and cooperation capabilities.
- Exchange and discussing information related to incidents and associated risks (on request, on a voluntary basis).
- Identify a coordinated response to an incident (on request).
- Providing MS support in addressing cross–border incidents (on a voluntary basis).
- Issue guidelines concerning operational cooperation.
- Discuss, explore and identify further forms of operational cooperation (risks and incidents, early warnings, mutual assistance, coordination).
- Discuss the capabilities and preparedness of certain CSIRTs (on request from that CSIRT).

### 2.2.5 ENISA

With more than 10 years of experience in dealing with cyber-security issues across EU, ENISA has touched upon almost all areas and sectors regulated through the NISD. Because of the work it has carried out in the past, ENISA is ideally positioned to assist the Member States in implementing the NIS Directive once it is adopted. The role of ENISA is to assist all stakeholders in implementing the NISD.

### 2.2.6 European Commission

The European Commission is the executive body of the European Union and it represents the interests of all EU Member States. One of its main roles is to put forward legislation, which is then adopted by the co-legislators, the European Parliament and the Council of Ministers, as in the case of the NISD.

Digital Society, Trust and Cybersecurity within is one of the areas where the Commission (DG CONNECT) has an active role, through the NISD but also through other legislative acts.

Through the NISD, the Commission will assure the secretariat of the Cooperation Group and will follow up on the effective implementation of the new regulation across EU. It will also have to adopt the secondary level legislation, meaning the implementing acts necessary to assure the uniform implementation of the directive across EU.

# 3. Incident notification process for DSPs

## 3.1 The NISD incident notification provisions for DSPs

The incident notification requirements for DSPs are defined within Art. 16, (4) to (9). The incident notification process should be in line with the following requirements:

- Member States must ensure that DSPs notify the competent authority without undue delay of any incident having a substantial impact on the provision of a service. The notification must include all information necessary so that the national authority can determine the significance and any cross-border impact. Although not directly specified within the NISD it is reasonable to take into account a two-step notification process: one immediate with a small amount of information and one with full details, at a later stage.
- By reason of the light touch approach that has to be followed when implementing the Directive, the DSPs will have to comply only with the regulation within one Member State, the one where the main establishment is located. In this way, a certain level of harmonisation ought to be achieved as providers will have to relate to only one authority and one set of rules across EU.
- In determining the “substantial impact” incidents, the following indicators will be used: the number of users affected by the incident (with a focus on the ones 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; (e) the extent of the impact on economic and societal activities. It is understandable that the provider must have access to all this information, so that the reporting can be done properly.
- Significant incidents affecting OES networks and systems caused by incidents affecting DSPs’ infrastructures are theoretically considered distinct incidents, therefore the reporting activities should also be distinct.
- If one incident concerns two or more Member States, the responsible authority shall inform the authorities within the other Member States. Moreover, although not specifically mentioned within the NISD, the communication should take place only through the national authorities or national CSIRTs.
- The public should be informed about individual incidents by the national authorities or by the provider, in case “public awareness is necessary in order to prevent an incident or to deal with an ongoing incident, or where disclosure of the incident is otherwise in the public interest”[11].
- The single points of contact should submit an annual incident summary report to the Cooperation Group (CG). The report should contain the number of notifications, their nature and actions taken (Art. 10 (3) ).
- The Commission will further specify applicable parameters and thresholds though implementing acts. Formats and procedures relevant for notification requirements could also be further specified through implementing acts, if necessary.
- Any incidents related to criminal activities should be reported to law enforcement authorities, as encouraged by recital 62 of the NISD. “Where appropriate, it is desirable that coordination between competent authorities and law enforcement authorities of different Member States be facilitated by the European Cybercrime Centre (EC3) and ENISA”[12].
- Given the light touch approach for DSPs, micro and small DSPs will be excluded from implementing the incident notification provisions. Governmental services (i.e. cloud) are also excluded.

[11] Art. 16 (7), NISD.

[12] NISD, Recital 62

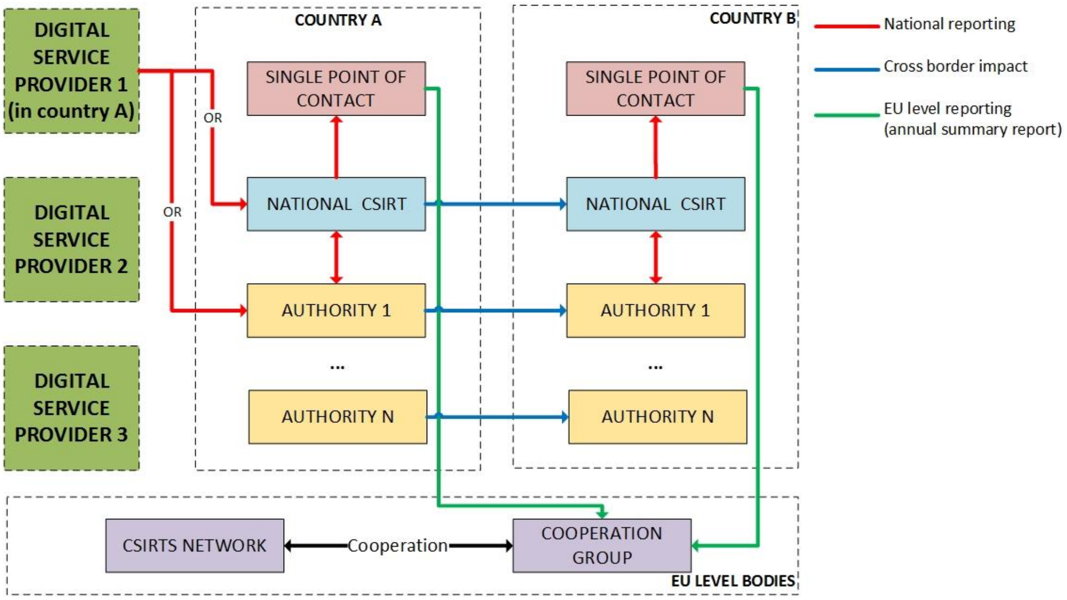

Fig. 3 - The overall incident notification process at EU level

### 3.1.1 Incident notification as part of the overall incident management process

***Information security incident management*** is defined by ISO/IEC 27000:2016 as "***processes for detecting, reporting, assessing, responding to, dealing with, and learning from information security incidents***". The importance of the topic is also thoroughly acknowledged through another specific standard ISO/IEC 27035, totally dedicated to information security incident management. In fact, 65% of the DSPs that responded to our stock-taking exercise declared using at least one of the two standards in their internal incident management activities, with ISO/IEC 27035 being the most common of the two.

According to the ISO/IEC 27035 standard, the incident management process is divided in five phases, as follows:

- Plan and Prepare – policies, plans, procedures, commitment at top management.
- Detect and Report – monitor, detect and report.
- Assessment and Decision – analysis and decision regarding course of action.
- Response – containment, eradication, recovery, resolution, closure.
- Lesson Learnt – improvements.

Due note should be taken when deciding where the new reporting activities provisioned in the Directive should be registered. Although there is a "Detect and report" phase this mostly refers to inside reporting, i.e. activities undergone within the organisation. Unfortunately, the outside reporting for compliance is rarely touched by the standards in use.

The incident notification process brought by the NISD is, first of all, mandatory, therefore DSPs have to comply with it as a consequence of them operating in the EU. As a consequence, it could work in the standard as an additional "incident notification for compliance". On the other hand, reporting in the sense of the provisions of the Directive, has to be carried out "without undue delay". Thus, introducing this additional phase within the overall organisational incident management process might become problematic when dealing with time constraints. In these particular cases, incident notification for compliance could constitute part of the "Detect and Report" phase, the "Assessment and Decision" or "Response" phases, depending on the internal structure, policies and procedures of a particular organisation.

## 3.2 Types of incidents covered by the NIS directive

Defining the scope in terms of types of incidents to be covered is difficult as long as terms are not properly clarified and there is no direct mention in the legislation. In order to help the cybersecurity professional community to get an accurate response to several issues that might arise during the implementation of the NISD, various definitions and provisions must be revisited. Therefore, in the following, we will try to summarize the basic applicable concepts.

As mentioned by the NISD (Art. 4 - definitions) an ***incident*** "*means any event having an actual adverse effect on the security of network and information systems*".

Similarly, article (4) defines the ***network and information systems***, by which we understand *interconnected systems that process, transmit and store data* so as to provide a digital service.

*Further,* ***security of network and information systems*** is defined as the "*ability of network and information systems to resist, at a given level of confidence, any action that compromises the availability, authenticity, integrity or confidentiality of stored or transmitted or processed data or the related services offered by, or accessible via, those network and information systems*".

*On the other hand****, adverse effect*** is a concept not defined within the Directive. Nonetheless, we can consider the general sense of the words that is preventing success or development, harmful, unfavourable[13].

In addition to the definitions above, a notion that needs clarification is ***substantial impact***, a concept that clearly marks the starting point of incident reporting activities. The notion is used in Art. 16 (4) that states that DSPs will have to "notify […] without undue delay […] any incident having a substantial impact on the provision of a service". Furthermore, the directive indicates that substantial impact must be determined based on 5 parameters (explained in next subchapter).

By combining the 5 notions highlighted above one can develop a comprehensive idea on the types of incidents that have to be considered within the context of the NISD. An overall definition can be summarised as follows:

**Any incident affecting the availability, authenticity, integrity or confidentiality of data stored, transmitted or processed by a digital service provider (DSP) through network and information systems, which has a substantial impact on the provision of the digital service offered.**

For clarity, in the following, we will try to depict various examples and specific types of incidents that we consider that shall be reported when reaching the critical thresholds.

In case of ***availability***, the interpretation is quite straightforward. If the services provided become unavailable to the customers for a certain period, then the incident should be reported under the provisions of the Directive.

As an example, we could consider the 2016 Dyn incident. The outcome of this particular attack was that several DSP services became unavailable worldwide (mostly North America and Europe) due to a DDoS attack against a common DNS service provider (Dyn) that was servicing the numerous DSPs affected. Consequently, the failing of the Dyn DNS services triggered an outage in the services offered by the DSPs that were using this particular DSN service in order to provide their own services. Were this kind of incident to happen in the EU after the transposition of the NISD into national legislation, all affected DSPs should report the

[13] https://en.oxforddictionaries.com/definition/adverse

outage. Meanwhile individual DNS service providers can be identified as operators of essential services (OES) under the NISD, in this specific situation the biggest blow was felt at the DSP level.

In the case of ***confidentiality***, the situation becomes slightly more complicated mostly because we have additional regulations in place that can overlap with the NISD (e.g. GDPR). Although we can probably draw a theoretical line between incidents falling under GDPR and the ones under NISD, the situation might differ in practice. DSPs might have to report the same incident to both authorities responsible. In theory, GDPR covers the privacy of personal data and the NISD covers the confidentiality of the service offered and the underlying data (which in most cases is personal data). The GDPR has no notion of a 'light touch approach' as used by the NISD.

A common pattern for incidents affecting confidentiality under the NISD could be the following: a cloud service provider suffers sudden breaches of the confidentiality of their customer's data (not necessarily personal data) either during transit or at rest ("man in the middle" type attacks). In this case, continuation of provision of the service could seriously damage the confidentiality of customer data (e.g. product technical specifications, commercial secrets, business plans, commercial contracts etc.) leading to serious impact on their business. Thus, when the confidentiality of services delivered cannot be guaranteed and the critical threshold has been reached, the incident should be reported. On the other hand, incidents that can be classified as simple data breaches but the proper provision of the service is not affected by the breach, should not be reported under the NISD.

An example is provided by the 2011 Dropbox bug[14] that left all their clients at risk for several hours. The renowned cloud storage provider generated a confidentiality incident as a consequence of making an update to its code that supressed the authentication method allowing users to access the data without passwords. For several hours' users were able to log on to the platform only with the username. This glitch exposed all of their customers to an extent that is unknown or was not yet made public.[15]

***Integrity*** of the service or, better said, client data processed through the service is also a type of issue covered by the NISD. It cannot be considered safe to use a cloud service where the integrity of client data or service cannot be assured because of a breach, a technical failure or any other issue. Any kind of event that affects the integrity of client data, if it reaches the critical thresholds to be deemed substantial, has to be reported. A clear case in point was the 2016 Salesforce incident that led to a complete disruption of services and a system crash that consequently led to the temporary wipe out of important customer transactions information. Thus, besides the availability of the service, the integrity of customer data was temporarily affected during the recovery process.[16]

*Finally,* ***authenticity*** is defined by ISO IEC 27000:2016 as the "property that an entity is what it claims to be". Proving the online identity of an entity is mostly done through digital certificates, meaning that incidents falling under the "authenticity" classification have to affect, to some extent, the digital certificate used to prove the digital identity of a particular service. Compromising the digital certificate used by a service can indeed give birth to several other issues, from man in the middle attacks to the risk that the client might be deceived towards using a completely different service (forged). Usually, these incidents can also be classified within other categories. Compromised digital certificates can very well fall within the provisions of the Art. 19 of the eIDAS regulation[17], depending on the circumstances.

*Note: For the rest of the document, for simplicity, we will refer to availability, confidentiality, integrity or authenticity, as the 4 properties or protection goals that a digital service must assure under the NISD.*

[14] https://blogs.dropbox.com/dropbox/2011/06/yesterdays-authentication-bug/
[15] Additional resources: here and here.
[16] Additional resources:  here and here.
[17] https://ec.europa.eu/futurium/en/content/eidas-regulation-regulation-eu-ndeg9102014

Besides the theoretical concepts explained above a standard list of incident types would have been very helpful in this case. Nevertheless, such a list cannot be either comprehensive and could create more confusion at this point. Although some types of incidents might be considered clear enough to be classified as reportable according to the NISD (e.g. DDoS), as the examples above show us, the interpretation might be quite difficult in some cases. An incident must fulfil many requirements in terms of parameters, thresholds and protection goals affected so that it can be categorised as reportable. In this respect a thorough analysis is recommended case by case.

When asked the opinion of DSPs about types of incidents and their root causes that might fall under the NISD, they indicated that most of the issues are not necessarily related to cyber-attacks but more to system failures or human errors. For more details, pls. see charts below.

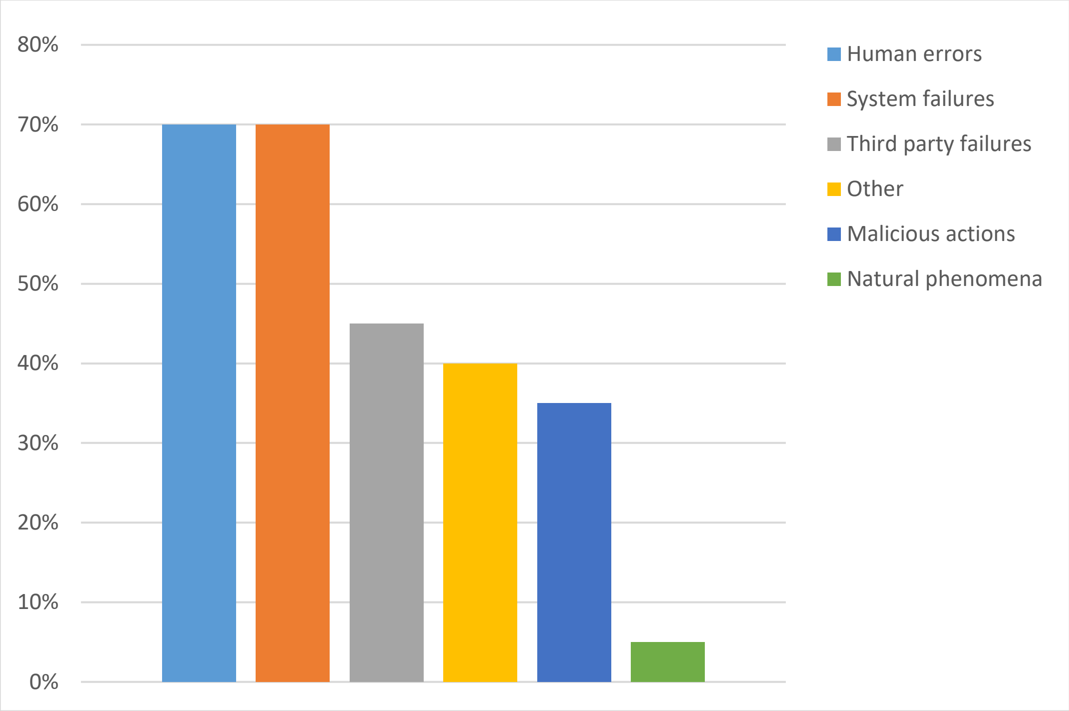

Fig. 4 – Most common root causes for incidents as seen by DSPs.

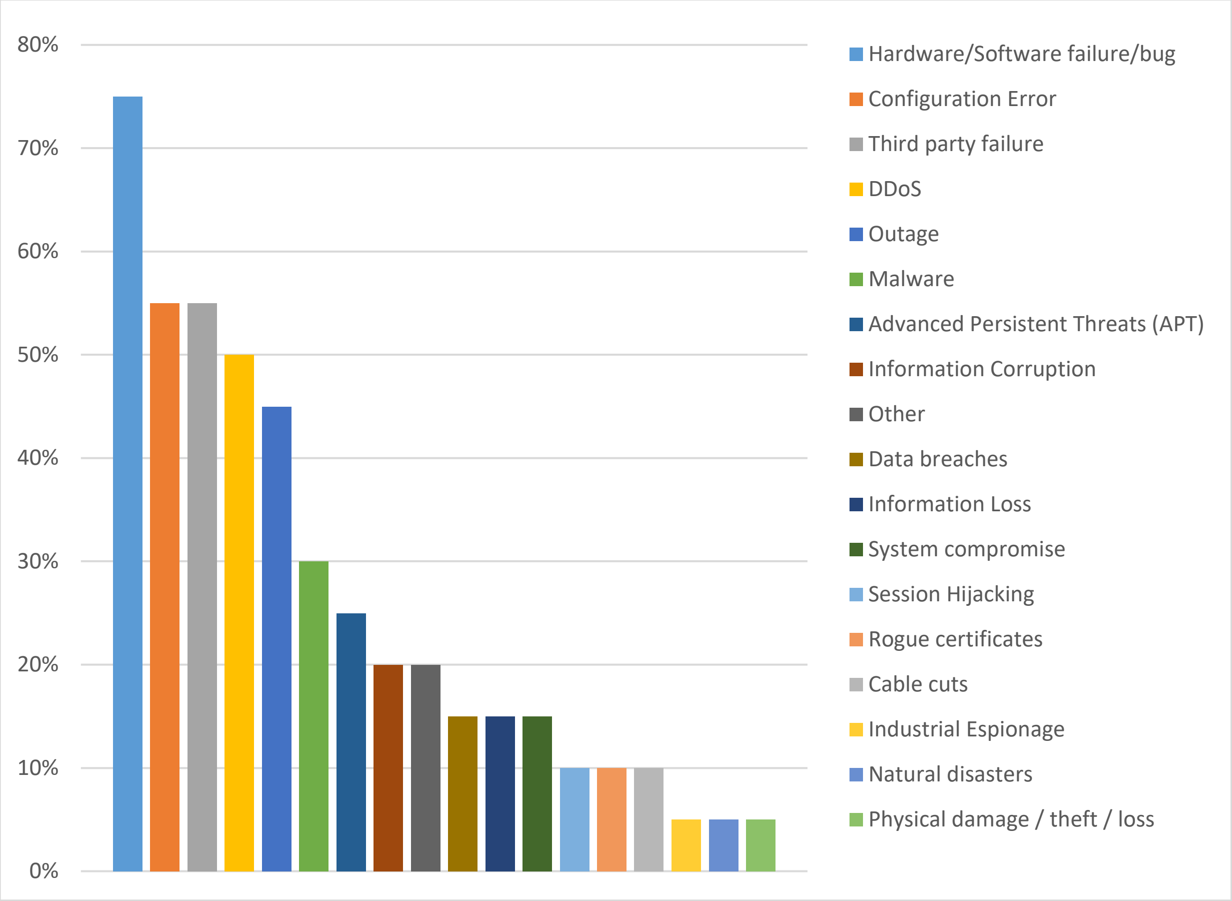

**Fig. 5 – Most common incident types as seen by DSPs.**

## 3.3 Parameters used to measure impact of incidents

In order to ensure a high common level of network and information security across all the EU Member States, the NISD introduces mandatory incident notification obligations, amongst several other requirements. To this end, mainly art. 16 (3) indicates that "digital service providers notify the competent authority or the CSIRT without undue delay of any incident having a substantial impact on the provision of a service […] offered within the Union". An exact definition of a substantial impact of an incident was not included in the approved version of the NISD, however a definite list of parameters that must be taken into account when determining the impact of the incidents are prescribed as follows:

- (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;
- (e) the extent of the impact on economic and societal activities.

As a result of our communication with the community of professionals that will be involved in the implementation of the NISD provisions, we introduce in the following subchapters some explanatory notes on each of the parameters together with potential ways in which they could be measured.

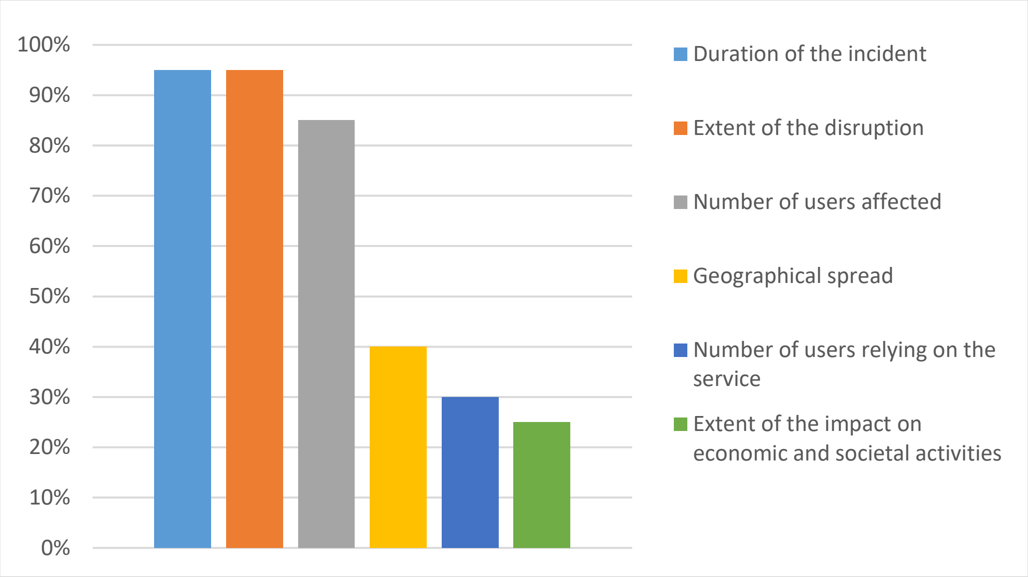

**Fig. 6 – Usage of parameters for measuring the impact of incidents (DSP view).**

### 3.3.1 Number of users affected by the incident

Measurement of the number of users reportedly impacted by a cyber-incident is one of the most important variables in determining its significance. As resulted from the stocktaking we carried out, roughly 85% of the DSPs that responded to our survey are currently using this parameter for measuring impact.

Although it might seem an easy task at a first glance, counting the affected users is not usually an easy task. The text of the NISD does not provide extensive details on how this parameter should be measured and, following our analysis we have taken stock of numerous methods (measuring units) used in practice for counting the actual users affected by an incident. Driven by a business model approach, the DSPs are using methodologies that count users such as normal anonymous visitors to corporate users or even other depending services (through application programming interfaces - APIs).

In summary, the following measurement units were identified during the analysis:

- ***Corporate subscribers*** (companies, corporate services) - used by 95% of the respondents; depending on the services offered it might mean one account used by one client (company) or multiple accounts per client (company) used by different individuals.
- ***Non-subscribers (visitors)*** – used by 60% of the respondents, mostly in the cases where they provide free services, such as search engines. Non-subscribers are non-registered users that access the service intermittently. Not too much information is stored regarding this type of user and their exact number might not be known at a particular point in time (such as in the case of an incident). Generally, estimations are used when needed to identify the number of users at different time intervals.
- ***Reliant services*** (dependant services) - used by 50% of the respondents to the survey, these are counts of online services that rely on the use of a particular service offered by a DSP (e.g. an online market place stored in cloud, an email service stored in cloud, a search engine that uses services provided by other search engines etc.) In such cases, the real number of end users is usually indefinite for the primary provider, and is known only to the depending provider.
- ***Individual subscribers/accounts*** (persons) – used by 45% of the respondents, these subscribers are representing individuals that usually use the services for their personal interest (home users, individual persons).

In most cases, the DSPs have visibility only at the first layer of users benefiting from the rendered service or any other secondary service based on the initial service, i.e. only the users/clients that have directly accessed the initial services and are considered users by the initial DSP are measured. For example, the users of an online store that uses cloud infrastructure to provide its services are only known to the online market place provider. The cloud provider sees just one user/client, the online market place. Below a tentative definition of users within the NISD:

**Users = a person, organization, or other entity that employs a digital service provided by a DSP through network and information systems.**

Within the multitude of user types, the importance/priority of some users over others (therefore priority for data recovery in case of an incident) is mostly business driven, based on contractual agreements and not necessarily based on the importance of the user for the society (i.e. governmental services, financial institutions, critical infrastructures etc.). In fact, most of the respondents are not even aware if they offer services to such entities. Roughly 60% of the DSPs involved in the survey mentioned being aware they provided services to other DSPs, but the percentage got significantly lower when they got asked if they were aware of providing services to essential service operators.

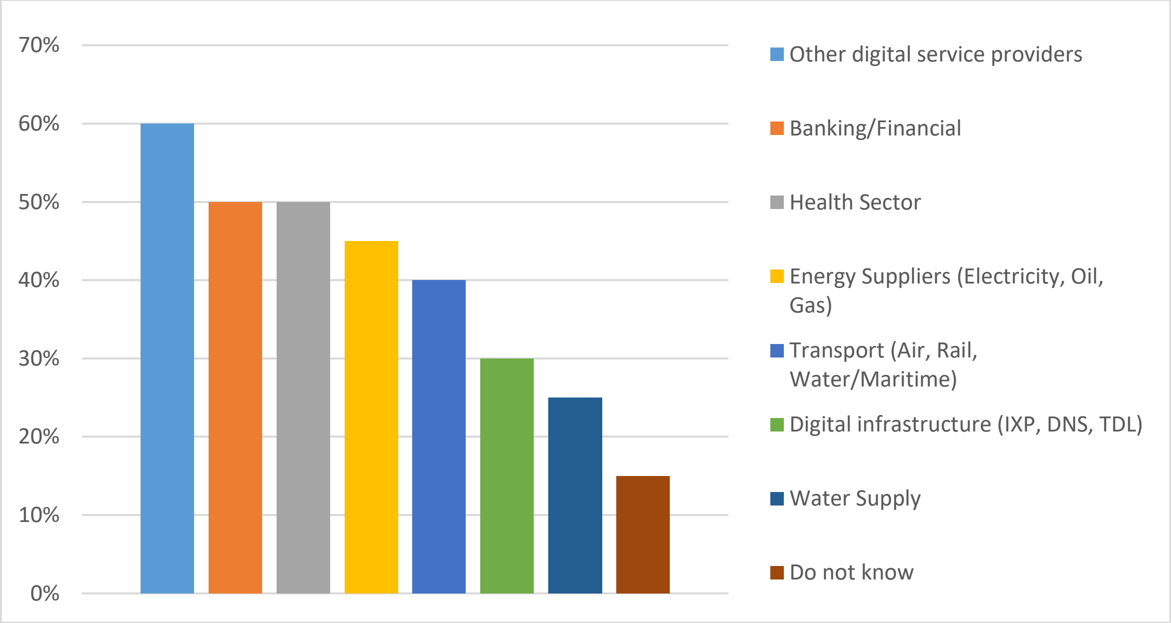

**Fig 7 - Answers to the question: "Which of the following sectors are you aware of using your services in EU countries?"**

Based on the type of the DSP, we could identify a significant variation in the methodology for user counts. For example, cloud service providers were usually more aware of the type and number of users at a particular point in time than search engines were. On the other hand, search engine providers were fully capable of measuring the dependant services (through APIs) but had difficulties with visitors accessing their services sporadically.

Considering the findings above together with the NISD provision as by art. 16 (4) stating that "the obligation to notify an incident shall only apply where the digital service provider has access to the information needed to assess the impact of an incident […]", we must point out that the approach to measure the number of users affected by an incident should be simple and pragmatic, so that DSPs can comply. Asking DSPs to provide information that they cannot obtain or for which they should make considerable efforts to obtain would eventually backfire and practically exclude them from the incident notification obligations.

### 3.3.2 Duration of the incident

Duration (time interval) is a parameter considered of utmost importance and used by all of the respondents. Nonetheless, even for this arguably basic parameter, the survey responses revealed differing practical approaches as to what regards measuring duration and the diverse thresholds applied.

For instance, depending on the incident type, the timer might start from the identification of the breach, or from the service degradation notice. Finalising the incident might be considered the time where all services have been fully recovered (time to recover) or the time when the systems were fully disinfected (in case of malware infections).

In the context of the NISD, since the focus is on the continuity of the service, thus availability and security of provision (in terms of confidentiality, integrity and authenticity) the duration of the incident should be measured (and consequently reported) as starting from the moment when the provision of the service was affected up until the time of full recovery. The reporting should contain the number of minutes (or hours) in which the service provided was not available or, although it was available, it did not meet the confidentiality, integrity or authenticity requirements. For the purpose of respecting the reporting provisions of the Directive, the general term "downtime" might not be a proper term to use as it refers only to availability. Thus we propose the use of "***NIS downtime***" or "***NIS impairment time***" to describe this particular parameter.

**Duration of an incident (NIS downtime) = the period of time when a digital service provided by a DSP is unavailable or unsecured (confidentiality, integrity or authenticity affected).**

### 3.3.3 Geographical spread

The geographical spread is an equally important piece of information to have in order to determine the level of impact. In circumstances where multiple countries are affected by one incident, identifying the causes and finding the best remedies can only be done when a clear picture of the geographical area affected is obtained.

Surprisingly, for the DSPs, the geographical spread is not necessarily a must but rather a nice to have piece of data. Only 40% of the respondents declared using this parameter, but the surprise is even bigger when it comes to how it is measured.

Some providers do use "geographical area affected" as an established parameter to measure impact of incidents, but not necessarily in the conventional political way we think of, meaning identifying regions or countries. The intense use of web related technologies has made this task exceedingly difficult. For a DSP that offers online web access to its services, the identification of the exact countries or geographical areas affected might be impossible without the use of estimations based on previous data.

Regions served by a data centre might be used as a reference, or in some cases continental regions, but these are not limited to EU borders. Although Internet fragmentation[18] is a fact nowadays, whether from technical, commercial or political standpoints, this is not necessarily embraced by DSPs unless there is a business need in this sense. Thus, the capability of identifying the exact countries affected by a particular incident was mentioned by only one participant to the survey.

In terms of applicability, the NISD reporting provisions cover only the 28 EU countries and it might apply in the future to other candidate countries. Needless to say that the DSPs did not build their current technical architecture based on political criteria, and thus they could face some issues in refining the data for reporting purposes only.

[18] http://www3.weforum.org/docs/WEF_FII_Internet_Fragmentation_An_Overview_2016.pdf

Therefore, reporting the geographical area affected by an incident might be challenging for most of the DSPs, especially if they provide services internationally. A simple approach that can be applied by all providers, operating internationally or nationally, is a must in this case. Consequently, a scale of detailing can be applied, starting from a bottom level where only a yes/no answer can be submitted if the incident has affected EU regions, and ending with a top detailed level where countries and regions can be specified, if known.

In any case, asking from DSPs information that they cannot obtain might exclude them from the incident notification obligations.

A tentative definition of the parameter geographical spread, in the context of the Directive is as follows:

**Geographical spread = Member States or regions within EU where users were affected  by impairments (NIS downtime) of the digital service provided by a DSP.**

### 3.3.4 Extent of the disruption of the functioning of the service

The extent of the disruption is a parameter used frequently by DSPs. 95% of the respondents to our stocktaking declared using this parameter.

The extent of the disruption is particularly important because it measures the extent of the damage produced by a particular incident. Not surprisingly, here too DSPs are using a business driven approach, customised depending on the technical particularities of the services provided. The following approaches for measuring the extent of the disruption have been identified during the stocktaking:

- Percentage of services lost (in case of multiple services);
- Percentage of the unavailable infrastructure (servers, datacentres etc.);
- Service degradation (delays in response, intermittent access, acceptable degradation, total disruption)

All approaches are correct and could reasonably be applied when providing any kind of service, not necessarily the ones that are DSP specific. In addition, as one may notice, the term is mostly used to describe availability related issues, although the notion of “disturbance” does not necessarily refer to total disruptions, but also perturbance of normal operation.

In this respect and considering the NISD context, the notion of disturbance ought to be adjusted. First of all, the extent of the disruption from an availability standpoint can only cover total disruption of the service or degradation that makes the service unusable. The percentage of infrastructure unavailable, the delays in response or any other related parameters cannot be really taken into account unless the users cannot use the service for a particular period, thus rendering the incident reportable.

Secondly, besides availability the NISD also mentions 3 other protection goals that must be taken into account when assessing the extent of the disruption upon a service: confidentiality, integrity and authenticity. Each of them can be broken down into different levels of detail but for simplicity, it could result better to treat them in a binary approach (yes/no). Consequently, if one or more of the protection goals are affected, and the thresholds are exceeded, incidents should be reported. Nevertheless, sophistication levels can be applied based on a combination of affected protection goals, from one goal affected for the first level, to 4 goals affected for the last level. A detailed description of this approach in presented in Annex A.

Below is a tentative definition of the parameter, in the context of the Directive:

**Extent of the disruption of the functioning of the service = the number of protection goals affected due to an incident disturbing a digital service offered by a DSP.**

### 3.3.5 Extent of the impact on economic and societal activities

Among all parameters enacted in the directive, the extent of the impact on economic and societal activities is the least utilized by the industry. Only 25% of the respondents mentioned measuring such a parameter.

In all reported cases the measurement unit was related to the internal resources spent for fixing the problem. Service credits or amounts deducted from the monthly invoice for the periods of inactivity are mentioned as conducts of measuring the economic impact upon a particular DSP.

Nevertheless, in the context of the NISD, by impact on economic and societal activities we refer to possible damages brought to the functioning of the EU internal market, meaning the encompassing markets in the EU's 28 member states. Individual economic impact on a single DSP might not be relevant in this context. The summed up individual impact felt by each of the affected users might be a response in this case, but this type of information is generally unknown to the DSPs.

In this respect, the problem becomes fairly difficult for the DSPs, as they are often unable to determine this kind of impact. Asking the DSP to collect all this data is probably unreasonable and could require plenty of additional resources and could ultimately prove impossible to do, as affected parties do not always want to share such information. On the other hand, asking the government to collect this data appears also unreasonable as this might be considered as an intrusive approach. In conclusion, measuring the real impact on economic and societal activities in this way is an activity that requires many resources and has high probability of failing due to inconsistent or incomplete data.

As compliance must be achieved and in order to avoid excluding DSPs from the incident notification obligations due to the impossibility to obtain the data, a simple yet straightforward approach should be applied. For example, determining the societal and economic impact based on the recorded effects onto predefined thresholds of users might be an option. Absolute thresholds (e.g. 1 mil users.) or relative thresholds (percentages of population) could therefore be used. You can find a detailed proposal on this topic in Annex A. Below you can find a tentative definition of the parameter, in the context of the Directive:

**Extent of the impact on economic and societal activities = the effects produced by a cybersecurity incident at DSP level that, as a result, affected the overall community, disrupting its normal functioning, generating either economic or social negative consequences.**

### 3.3.6 Other issues related to parameters

During the stocktaking with private sector and public authorities within EU, several concerns were raised regarding some of the provisions that were considered not sufficiently explained within the text of the directive.

One of them is the **noticeable distinction on many areas between the different types of DSPs**. Although the NISD does not strike a difference between the three types of DSPs, most of the private respondents have clearly stated that there should be a rigorous distinction between them due to different factors such as criticality, technical particularities in use and economic and societal impact. At the same time, the NISD does not restrict the adoption of subsequent policies that distinguish between the types of DSPs.

Cloud services are considered the most critical out of the three categories due to their obvious potential for captive consumer patterns. In case of failure, users cannot instantly migrate to another cloud provider.

Obtaining the necessary products and services on time, through online market places, is utterly important, especially for businesses that rely on this kind of service. Nevertheless, in most of the cases (besides the ones where exclusivity is offered to certain online market places) the services or products needed can be found in similar stores, of course at different prices and maybe different delivery times. However, nowadays business good practices regarding supply chain security encourage companies as well as consumers to have at least two alternatives when purchasing certain products or services. Considering this, we may infer that, to some extent, online market places are not generally as critical as cloud services could be, at least not in the majority of the cases.

As for the search engines, the situation is considered even less critical, by the providers themselves even. You can always turn to another provider in case of failure by your favourite search engine. Indeed, it might be an issue in both cases (online marketplaces and search engines) if some other services are dependent on particular providers. Overall though, from total dependency to partial dependency, there are several aspects that the private sector deems important be included in the provisions.

Last, but not least, one issue relates to **the possibility of using different reporting formats and procedures per type of provider**. As explained also in the previous subchapters, there are some technical particularities for each of the three types of providers concerned by the NISD. Not addressing them early on might eventually prove to be a mistake, as some parameters required by the directive cannot be measured in the same way for the different providers (e.g. number of users further explained here). It is indeed the expressed opinion of most of the private sector respondents, along with some Member States respondents, that this technical concern regarding incident reporting for DSPs should be addressed in the implementing act. To this end, different measurement units and different thresholds might be applied, based on the DSP type. The proposal within Annex A takes this requirement into account.

## 3.4 Determining substantial incidents

Art. 16 (3) of the NISD requires DSPs to notify with undue delay “any incident having a substantial impact on the provision of a service”. Further, paragraph (4) of the same article mentions that in order to determine if an incident is substantial, a series of parameters must be taken into account. All those parameters have been explained in section 2.5, but the definition of “*substantial impact*” lies nowhere within the directive. Likewise, the use of thresholds is not properly mentioned within the NISD, neither provisioned nor certainly forbidden. This leaves some room for adaption and customization at national decision-making level, when building second level legislation or other policies in the field.

However, in order to develop an efficient and useful EU-wide incident reporting policy, one must take into account the following:

- The objective of the NISD is to assure a high common level of network and information security across EU. Achieving a common level between Member States usually means adopting some sort of common denominators or, at least, common values to be mutually adopted by all players. This is particularly important for levelling the security across EU countries and offering the community a set of reference values to work with.
- As stated in recital 49 of the NISD “because of their cross-border nature, digital service providers should be subject to a more harmonised approach at Union level”. In this respect, the adoption of implementing acts should facilitate the specification and implementation of such measures in a more harmonised way. To achieve the harmonisation objective DSPs should first undertake a common minimum set of security measures and the same set of incident notification provisions across EU, irrespective of the authority governing upon their activity.
- Article 16 (4) mentions that, in order to determine substantial incidents, a unique set of parameters should be applied no matter the country where the DSP operates. Again, it is reasonable to assume that common thresholds must accompany the adoption of common parameters so that the measurement and, most importantly, interpretations can be reliable, representative and can inform further policy decisions in all Member States.

As a practical and rational conclusion to all three points explained above, it is our understanding that the adoption of common thresholds is necessary in achieving EU level harmonisation in terms of incident notification.

Applying an incident notification policy across EU without having proper thresholds would not help achieve many of the objectives of the directive, i.e. “common level of network and information security”. An incident notification policy without thresholds would only create further confusion and possible discriminatory practices against DSPs due to different approaches adopted by the Member States.

A comprehensive approach based on relative and absolute thresholds should therefore be applied to identify EU-wide incidents that indeed might have a substantial impact on the internal market.

The section below and Annex A contains a full non-binding proposal on how to determine the impact of incidents based on parameters and thresholds.

### 3.4.1 Proposed procedure/algorithm for determining the impact of incidents

The NISD leaves plenty of room for interpretation in what regards incident notification provisions for DSPs. Through this paper we tried to further explain some key concepts and fill in some gaps, with the belief that it could improve the conditions for smooth implementation of the incident notification provisions. One of the main proposals that we presented in section 2.6 was the introduction of thresholds in the incident reporting process.

The purpose of this annex is to describe our **non-binding proposal on how thresholds** could be applied within the context of the NISD.

When reading the current proposal, please take into account the following aspects:

- All requirements of the NISD were taken into account, so that the proposal can seamlessly fit the necessities (i.e. the proposal is based on all parameters proposed by the directive).
- A three level scale of criticality was introduced to better classify incidents according to their impact. Please read Annex A for an explanation of all three levels (RED, ORANGE, YELLOW). Reporting starts from YELLOW.
- A simple yet comprehensive approach was embraced. Simplicity was needed to avoid overburdening the DSPs and national authorities with obtaining data that was not collected organically.
- Due to the diversified (and sometimes contradictory) set of approaches observed from the industry and Member States, identifying a common denominator only by compiling the answers was impossible. The private sector has a business driven approach, sometimes using parameters and thresholds that are not entirely relevant in the context of the NISD (e.g. parameter: percentage of lost services). In this respect, previous ENISA experience in incident reporting schemes was very useful in fine-tuning the results obtained with the overall context of the Directive.
- The proposal is organised as a logical scheme, an algorithm, where all steps must be fulfilled before reaching the final result.
- All thresholds proposed are based on the results of the survey and ENISA’s previous experience. We do understand that in particular cases updates could be needed to reflect real life situations, but this task was beyond ENISA’s capabilities given the resources the time constraints. We do acknowledge that further effort needs to be deployed by ENISA within the Cooperation Group as well as to assist the Comitology Committee’s work in order to achieve optimal values.
- A 2 step reporting approach is proposed, with a preliminary reporting in due time after the incident and a full reporting in 2-3 days after detection.

When trying to determine the impact of an incident the following steps should be applied (graphical view Fig. 8):

1. **STEP 1: Identify the geographical spread of the incident**

   At this level, a DSP should identify if the provision of the service concerned (NIS downtime) was affected within the EU political borders. If a positive result will come out, the countries affected should be identified. Based on the number of countries affected, the colour code of this parameter is to be assigned. At this stage there is no need to identify if users were indeed affected within EU borders, but just to identify if the service was properly accessible in EU Member States.

   Question to answer on STEP 1: Does the incident affect the proper accessibility of the service within EU?

2. **STEP 2: Determine the extent of the disruption**

   The extent of the disruption must be analysed taking into account the 4 protection goals expressed within the Directive: integrity affected (information or output provided altered), confidentiality affected (interception, unauthorized access), availability affected (service degraded, interrupted and/or unusable), authenticity affected (cannot be trusted). Based on the number of affected protection goals the impact colour code is assigned. If an incident can be identified as affecting at least one of the 4 properties above, it shall be classified as YELLOW. If more properties are affected the colour code is attributed accordingly.

   Question to answer on STEP 2: Is the service unavailable, unusable or unsafe to use due to the incident?

3. **STEP 3: Determining the USERTIME**

   The two parameters “number of users affected” and “duration of the incident” were merged into a single one entitled USERTIME. We considered the merge necessary for achieving better flexibility in covering real life scenarios (very long incidents with few users affected or very short incidents with many users affected). USERTIME is based on relative and absolute thresholds. The relative one refers to the percentage of the population being affected in one Member State. In our example it starts from more than 5% for at least one hour, or more than 1% for at least 4 hours. The absolute threshold is measured in fixed values and it has to reach more than 60 million user-minutes per incident. For more details, please see Annex A. For this parameter, no colour code is to be applied. If the critical threshold is exceeded, the incident should be reported. For the purpose of reporting, any type of user can be included, but a classification (based on the types enumerated in section 2.5.1) is to be preferred if the DSP is able to provide one.

   Question to answer on STEP 3: Does the impairment caused by the incident is above the absolute or relative thresholds in terms of USERTIME?

4. **STEP 4: Determining the extent of the impact on economic and societal activities**

   The overall purpose of the NISD is to protect the internal market from damages produced by cyber-incidents. Identifying the real economic and societal impact for every incident is challenging for both DSPs and national authorities, as most of the information needed resides outside their organisations. Therefore, this is mainly an estimative exercise aiming at giving the EU authorities a glimpse into the potential disruptive effects upon the internal market and EU citizens. In this respect, the approach proposed in step 4 is based on predefined levels of affected users. The more users are affected the bigger the potential impact. We do understand that the numbers provided might not be very illustrative for all Member States and further adjusting might be necessary during implementation.

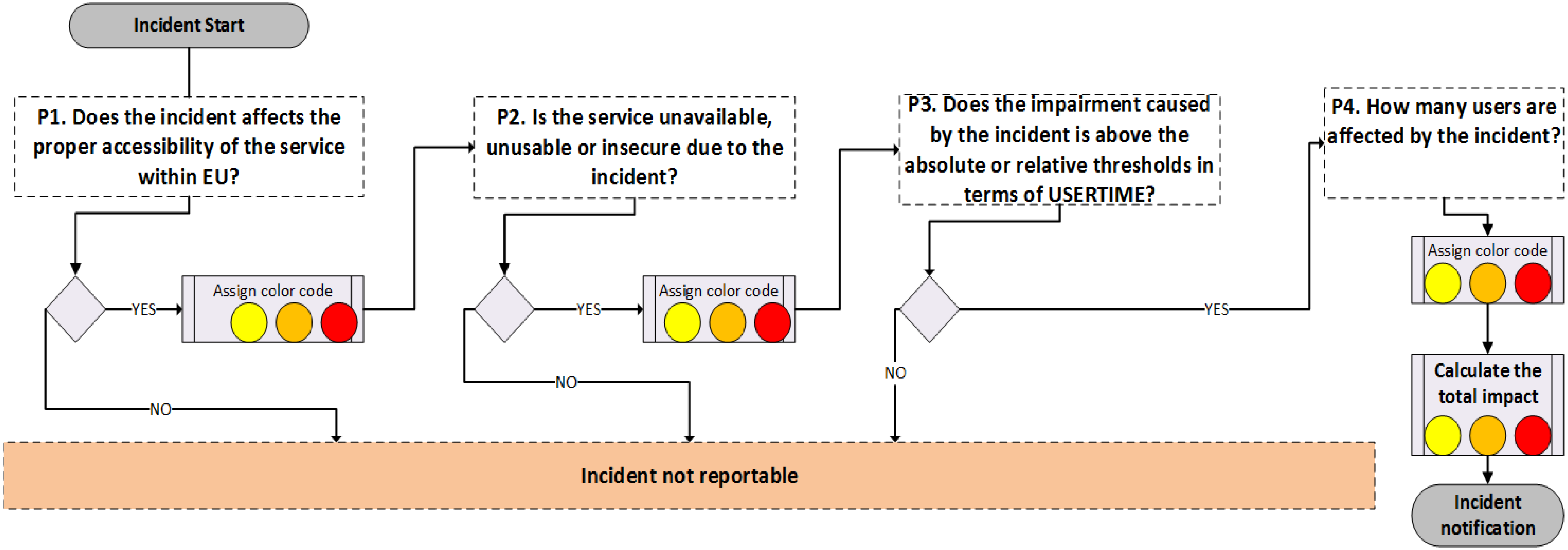
Incident Start
P1. Does the incident affects the proper accessibility of the service within EU?
YES
Assign color code
NO
P2. Is the service unavailable, unusable or insecure due to the incident?
YES
Assign color code
NO
P3. Does the impairment caused by the incident is above the absolute or relative thresholds in terms of USERTIME?
NO
YES
P4. How many users are affected by the incident?
Assign color code
Calculate the total impact
Incident notification
Incident not reportable

Fig. 8 - The incident reporting process

# 4. Conclusions

The current study has uncovered serious issues that must be addressed while implementing the DSP incident reporting provisions of the NISD. The multitude of technical approaches mirrored the numerous discrepancies between types of DSPs and the corresponding business models adopted, thus creating a deep pool of sometimes incompatible variables that must be taken into account when approaching such a regulation. For example, a simple parameter imposed by the Directive, such as “number of users”, can mean different things to different types of providers, from simple visitors or registered individuals to corporate users and dependant services.

Achieving convergence between the myriad of existing approaches while sticking to the formal requirements might be troublesome. Nevertheless, the EU’s first DSP incident notification requirements as part of the first EU wide set of rules on cyber-security are a major step forward towards achieving a common level of cyber-security across the Union. In a perpetually fluctuating technological landscape that affects our livelihoods while having increasing economic and societal impact as a whole, a first step, in understanding the real threats and vulnerabilities that we have to confront, has been taken through the adoption of the NISD along with its two main requirements: mandatory incident notification and minimum security measures. From now on, a “small steps” approach must be applied in implementing the Directive, that has to undergo periodic reviews and updates.

This document provides a preliminary guideline on how incident notification provisions for DSPs could be effectively implemented across EU. Based on valuable input from Member States and companies directly impacted by the Directive, this guideline arises from their good practices in matters such as identifying types of incidents, parameters and thresholds and results in an outline technical proposal that can tentatively be applied across EU.

At the same time, this guideline serves as a technical input to the foregoing process of adopting the implementing act that will further specify details regarding the incident notification provisions of the NISD.

# Annex A - Proposal on how to determine the impact of incidents

| PARAMETER | | CLOUD / ONLINE MARKETPLACE / SEARCH ENGINES | |
|---|---|---|---|
| | | **Algorithm** | **Thresholds** |
| P1 | The geographical spread (area affected by the incident) | **Does the incident affect the proper accessibility of the service within EU? (YES/NO)**<br>*Explanation: If an incident will prevent the proper provision of the service (impairments) within EU borders it shall be considered as fulfilling the requirements of the first step of the algorithm (P1). If particular countries can be determined we will proceed to determine the color code of the incident.* | **RED: all EU countries in EU**<br>**ORANGE: many EU countries**<br>**YELLOW: one EU country** |
| P2 | The extent of the disruption of the functioning of the service | **Is the service unavailable, unusable or unsafe to use due to the incident? (YES/NO)**<br>*Explanation: Assessment should be done by analyzing if the following properties (protection goals) of the service were affected:*<br>- integrity affected (information or output provided altered)<br>- confidentiality affected (interception, unauthorized access)<br>- availability affected (service degraded, interrupted and unusable)<br>- authenticity affected (cannot be trusted)<br>*If an incident can be identified as affecting at least one of the 4 properties above, it shall be classified as YELLOW. If more properties are affected the color code is attributed accordingly.* | **RED: at least three or more properties affected**<br>**ORANGE: at least two properties affected**<br>**YELLOW: at least one property affected** |
| P3 | The number of users affected by the incident<br>+<br>The duration of the incident<br>(USERTIME) | **Does the impairment caused by the incident is above the absolute or relative thresholds in terms of USERTIME?**<br>{ // IF above relative thresholds - see Table 1}<br>OR<br>{ // IF above absolute thresholds<br>( (>= A) AND (>= B) )<br>OR<br>( (>= A) AND (>= C) )<br>} | A=60 mil. user minutes (1 mil. user hours)<br>B=25.000 users OR 10.000 relying users (services)<br>C=1 hour<br>*Relative thresholds in table below.<br>** Color code not applicable for P3.<br>*** Different values might be applied per type of DSP. |

| | | | |
|---|---|---|---|
| | | *Explanation: If the values provided by DSPs (users, time) are above the relative OR absolute thresholds, the incident can be considered as fulfilling the requirements of the third step of the algorithm (P3). NO color codes shall be applied here.*<br>*Algorithm: Incidents above the relative thresholds (Table 1, percentage of the population or percentage of their user base) are reportable. Incidents that are NOT above the relative threshold, but are above the absolute threshold are also reportable. The universal absolute threshold is 60 mil. user minutes per incident but only if it affects more than 25.000/10.000 users or lasts more than one hour. The user minutes are obtained by multiplying the nr. of users affected with the duration of the incident.*<br>*Examples:*<br>- *25.000 users X 60 mins=1.200.000 userminutes=NOT REPORTABLE.*<br>- *25.000 users X 2.400 mins=60.000.000 userminutes=REPORTABLE.*<br>- *1.000.000 users X 59 mins=70.800.000 userminutes=NOT REPORTABLE.*<br>- *1.000.000 USERS X 60 mins=60.000.000 userminutes=REPORTABLE.* | |
| P4 | The extent of the impact on economic and societal activities | **How many users are affected by the incident? (Numeric)**<br>{ // IF above relative thresholds - see Table 1}<br>OR<br>{ // IF above absolute thresholds<br>( (>= A) AND (>= B) )<br>OR<br>( (>= A) AND (>= C) )<br>}<br>*Explanation:*<br>By default, we consider that if users (any kind) are affected by the incident we can talk about a certain economic and societal impact. As determining the real impact might be troublesome for DSPs and Member States also, the proposal is to measure only the number of users affected and use the color code form the next column. | **A=120 mil. user minutes (2 mil. user hours)**<br>**B=75.000 users OR 30.000 relying users (services)**<br>**C=3 hour**<br>**A=90 mil. user minutes (1,5 mil. user hours)**<br>**B=50.000 users OR 20.000 relying users (services)**<br>**C=2 hour**<br>**A=60 mil. user minutes (1 mil. user hours)**<br>**B=25.000 users OR 10.000 relying users (services)**<br>**C=1 hour**<br>*Relative thresholds in table below |

**Table 1 - Proposal for measuring impact of incidents within the NISD**

| Relative threshold | | 1h<…<2h | 2h<…<4h | 4h<…<6h | 6h<…<8h | 8<…<10h | >10h |
|---|---|---|---|---|---|---|---|
| 1%<…< 2% of population | | | | 🟨 | 🟧 | 🟧 | 🟥 |
| 2%<…< 5% of population | | | 🟨 | 🟧 | 🟧 | 🟥 | 🟥 |
| 5%<…< 10% of population | 🟨 | 🟨 | 🟧 | 🟧 | 🟥 | 🟥 | 🟥 |
| 10%<…< 15% of population | 🟧 | 🟧 | 🟧 | 🟥 | 🟥 | 🟥 | 🟥 |
| > 15% of population | 🟧 | 🟧 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 |

***Estimated population per Member State (user base)**

**Color code explanation:**

**Rule for assigning colors= the lowest level color of all parameters decides the overall color code of the incident.**

**RED =** Severe incident affecting the continuity of the services for many people in several MS and causing a very high economic and societal impact (RED for P1, P2, P4).

**ORANGE=** Serious incident affecting many people from one country and causing a high economic and societal impact (ORANGE for at least one of P1, P2, P4 and the others the same or more).

YELLOW= Substantial incident affecting many people within parts of a

ENISA
European Union Agency for Network
and Information Security
Science and Technology Park of Crete (ITE)
Vassilika Vouton, 700 13, Heraklion, Greece

Athens Office
1 Vasilissis Sofias
Marousi 151 24, Attiki, Greece

TP-05-16-086-EN-N

PO Box 1309, 710 01 Heraklion, Greece
Tel: +30 28 14 40 9710
info@enisa.europa.eu
www.enisa.europa.eu

ISBN: 978-92-9204-204-2
doi: 10.2824/002714