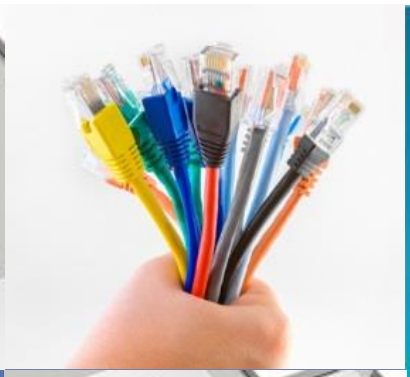



Impact evaluation on the implementation of Article 13a incident reporting scheme within EU

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.

Authors

Dan Tofan (ENISA)
Konstantinos Moulinos (ENISA)
Christoffer Karsberg (ENISA) – survey phase

Contact

For contacting the authors please use resilience@enisa.europa.eu
For media enquiries about this paper, please use press@enisa.europa.eu.

Acknowledgements

The analysis in this document was produced in collaboration with EY Luxembourg (Brice Lecoustey, Alexandre Minarelli, George Tountas and Cédrine Herbin) and based on the input of the following experts: Vassilis Stathoupoulos (ADAE), Manuel Barros (ANACOM), Costin Masiliev (ANCOM), Heidi Kivekas (FICORA/NCSC-FI), Tamas ROKA (NMHH), Vasiliki Mylona (OCECPR), Marios Pantazi (OCECPR), Antonis Antoniades (OCECPR), Matthew Bryant (OFCOM), Karin Lodin and Björn Scharin (PTS), Ulrich Latzenhofer (RTR), Francois Zamora (Orange France), Zerboni Marcello Alessandro Michele (Telecom Italia), Marnix Dekker (former ENISA expert in NIS).

ISBN: 978-92-9204-149-6; DOI: 10.2824/491369

Contents

Executive Summary

In today's interconnected world, telecommunications are transforming the way people engage in their everyday lives. Economic development is strongly related to the existence and well-functioning of the telecommunication networks. Electronic communications services guarantee the smooth transmission of data in this strongly interconnected world by providing the infrastructure for businesses and critical services to run. Electronic communication services also play a significant role in national security, emergency response and in the economic development of a country. As a result, a security incident affecting one of these areas can result in severe consequences.

Art. 13a gave a new momentum in the telecom industry at European level. Being part of the Framework Directive 2009/140[1] EC within the Telecom Package, the set of obligations in the article aims at ensuring the security and integrity of electronic communication networks and services, dealing mostly with prevention of outages or service disruption (availability of the service). Although availability seems to be the main concern of Art. 13a, some countries (as you will notice later) have decided to cover also other types on security incidents within their national legislation (e.g. privacy). By amending the 2002 legislation, the Art. 13a within the 2009 Telecom Package, addresses specific security and resilience obligations for the telecom sector, for the first time in EU, as the 2002 directive had only vague provisions on this area.

As several years have passed since the publication and implementation of the Framework Directive including Art. 13a, an impact evaluation of the new article was the proper thing to do. The evaluation has the purpose of assessing the changes in outcome that can directly be attributed to the provision of Art. 13a, the effects caused by this particular set of obligations within the Telecom Package. The evaluation focused on 5 key areas, where we tried to identify possible outcomes:

- The new security measures implemented in the member states ;
- The transparency resulting from the incident reporting process;
- The learning process resulting from incidents ;
- The level of collaboration between the stakeholders ;
- The harmonization of the procedures within the European Union.

The compendious evaluation we have done within this project has brought to light some important outcomes that have definitely contributed to increasing the resilience and security of the telecommunications infrastructures in Europe. In a European Union which was highly diversified in terms of security measures, Art. 13a brought a certain amount of uniformity in the approach taken regarding security of telecommunication services, but more importantly contributed to strengthening the European telecom infrastructure's resilience and services availability across the EU. The role of ENISA, especially in the coordination of Art. 13a expert group, was most beneficial as it helped considerably in bringing more harmonization within the implementation process and collaboration among stakeholders (NRAs and providers).

Overall, Art. 13a has undeniably contributed to improving the level of security in the telecommunication sector but in a balanced way as some countries were already in line or even ahead of the requirements and

[1] Directive 2009/140/EC of the European Parliament and of the Council of 25 November 2009 amending Directives 2002/21/EC on a common regulatory framework for electronic communications networks and services, 2002/19/EC on access to, and interconnection of, electronic communications networks and associated facilities, and 2002/20/EC on the authorisation of electronic communications networks and services

were already experiencing the expected benefits, whereas other less advanced countries or providers experienced strong benefits in spite of the costs and effort provided.

It was also noted throughout this project that further analysis is needed in order to draw some strong conclusions on next steps that are needed in this area. This report only covers a set of findings that must be further analyzed, by responsible parties, in order to propose concrete recommendations and next steps to be considered by different types of stakeholders.

The main findings of the study are the following, grouped into categories:

The scope of Art. 13a

1. Current lack of precise information within Art. 13a and Telecom Directive, as regards the types of networks and services that should be covered, has led to some differences among national implementations within member states. Although, the level of harmonization seem to be satisfactory, the differences within services covered by member states could represent obstacles in achieving the overall or specific objectives stated within the Telecom Package. Further assessments in this area are needed (more details in section 2.1.2. and Annex I) in order to establish possible next steps.
2. More than half of the respondents (54%) considered that Art. 13a cannot sufficiently and clearly cover by itself security of electronic communications, but together with Art. 4 in the e-Privacy Directive.

Appropriate security measures for providers:

1. The majority (45%) of the respondents (NRAs) considered that Art. 13a has led to stronger security measures within the sector, but further analyses are needed as more than half of them (55%) do not share this opinion, 23% stating “no” and 32% “do not know”.
2. Almost 60% of the respondent NRAs are not aware of the areas where the providers have improved the most, in terms of security measures.

Transparency in incident reporting

1. The approach of providers towards NRAs as regards the implementation of Art. 13a mandatory incident reporting regulations was mostly collaborative. Withal the majority of the respondent NRAs are satisfied with the quality of the information provided by the operators in their incident reports and declared that they are receiving reports as expected.
2. Bringing more clarity to the incident reporting process, by issuing guidelines and additional legislation – 73%, was by far the most effective method of improving transparency.

Learning and improving based on reported incidents

1. NRAs mostly use the incident reporting process as a tool in learning/improvement, but mostly for internal purposes such as compliance, internal statistics and improve regulations. The use of annual incident statistics as an input for evaluating risk at national or sectorial level is not a common approach among NRAs (more details in section 5.1. and 5.3).

Collaboration between the actors

1. The establishment and development of Art. 13a expert group, under ENISA coordination, turned out to be a successful and helpful experience (more details in section 6.3.), as appreciated by 80% of the respondents. The operation and development of the group should definitely be continued, under ENISA’s coordination.

2. Bi-directional communication with the population in the incident reporting process is poorly addressed by both NRAs and providers. Further analyses should be carried in order to determine the necessity of developing such processes (more details in section 4.3.).
3. The amount of resource employed by NRAs in the cross-border collaboration area appears to be low (more details in section 6.3.).

Harmonization of practices within the EU

1. Over 80% of the surveyed NRAs declare that they are satisfied with the current level of harmonization within the EU, which sustains also national specificities, and do not think that an improvement is needed in present.
2. ENISA's work, together with Art. 13a expert group, in the area of guidelines and good practices, was considered useful by up to 70% of the respondent NRAs, as it supported the achievement of a mature level of harmonization.

Impact evaluation based on reported incidents

1. More and more reported incidents (at ENISA level) are caused by third party failures (more details in section 8.2.), meaning they are caused by parties out of provider's direct control, but within the provider's supply chain.
2. The main root cause for incidents at EU level in 2014 and years before, is "system failures". Further assessment needs to be done in this area, in order to identify more detailed causes and security measures that can be adopted.

1. Introduction

1.1. Background

In today's interconnected world, telecommunications are transforming the way people engage in their everyday lives. Economic development is strongly related to the existence and well-functioning of the telecommunication networks. Electronic communications services guarantee the smooth transmission of data in this strongly interconnected world by providing the infrastructure for business services to run. Electronic communication services also play a significant role in national security, emergency response and in the economic development of a country. As a result, an outage in any one of these areas can result in severe consequences.

The Telecom Package represents the EU's regulatory framework for electronic communications, and is, according EU Commission's website, "[…] *a series of rules which apply throughout the EU member states. It encourages competition, improves the functioning of the market and guarantees basic user rights. The overall goal is for European consumers to be able to benefit from increased choice thanks to low prices, high quality and innovative services*"[2]. The Telecom Package was adopted in November 2009, as a review of the European Union Telecommunications Framework 2007 – 2009.

Art. 13a, of the Directive 2009/140 EC, is part of the Telecom Package and aims at ensuring the security and integrity of electronic communication networks and services, dealing mostly with prevention of outages or service disruption (availability of the service). This is partially achieved through requiring telecommunication service providers to take the appropriate technical and organizational measures to manage the risks posed to security of networks and services, guarantee the integrity of their networks (ensure the continuity of supply of services provided over those networks) and notify the competent national regulatory authority (NRA) of a breach of security or loss of integrity that has had a significant impact on the operation of networks or services.

Published in 2009, Art. 13a required that the deadline for the transposition should be up to 2011. However, the transposition timeframe and process significantly varied from one country to the other. As a matter of fact, countries maturity level, national legislation complexity and process impacted some countries in their ability to comply with the deadlines, resulting in certain gaps between countries overtime. Today, the majority of countries implemented the provisions of the Art. 13a, in one way or another, besides one country. Art. 13a also designates ENISA, along with the European Commission (EC), as responsible bodies for collecting notifications received and actions taken within member states, under the provisions of national implementations of Art. 13a. Besides this specific mandate, according to the directive, ENISA should also contribute to the "harmonization of appropriate technical and organizational security measures by providing expert advice" and by "promoting the exchange of best practices".

As a response to the directive's requirements, in 2010, ENISA, Ministries and NRAs from member states, initiated a series of meetings (workshops, conference calls) in order to achieve a harmonized implementation of Art. 13a of the Framework directive. As a result of these meetings, a group of experts from NRAs, now entitled the Art. 13a Expert Group, reached agreement on three non-binding technical documents providing guidance to the NRAs in the EU member states:

- Technical Guideline on Incident Reporting[3]

[2] https://ec.europa.eu/digital-agenda/en/telecoms-rules (November 2015)
[3] https://resilience.enisa.europa.eu/article-13/guideline-for-incident-reporting

- Technical Guideline on Security Measures[4]
- Technical Guideline on Threats and Assets[5].

The Art. 13a Expert Group continues to meet several times a year, to develop and improve technical guidelines, to discuss upon the implementation of Art. 13a and to share knowledge and exchange views about past incidents, and how to address them.

1.2. Scope

Considering the above, as several years have passed since the implementation of Art. 13a, an impact evaluation of the new regulation is the proper thing to do. The evaluation has the purpose of assessing the changes in outcome that can directly be attributed to the provision of Art. 13a, the effects caused by this particular regulation within the Telecom Package. The ultimate goal of this study is to assess the "as-is" situation and the outcomes produced through implementations of Art. 13a. The results of this study are intended for understanding the impact of the regulation on the European telecommunications industry, and for further improving the security and resilience of the networks and services within the sector.

1.3. Target audience

This report is addressed to:

- policy makers at EU level, including the European Commission and ENISA, in order to help them understand the impact of the regulation on the telecommunications market and EU digital single market and further improve the security and resilience of the sector;
- policy makers within member states, in order to help them better understand the impact of the regulation on their internal market;
- telecommunications providers, in order to help them better understand the impact of the regulation on their business;
- any other stakeholder interested in this policy field;

1.4. Impact evaluation methodology

This report is based on a qualitative survey type approach, consisting of a desktop research, an online surveys and telephone interviews. The approach aimed to collect all the available information regarding the national implementations of Art. 13a and identify the outcomes produced at national and European level. This helped in building a baseline on which the interviews and survey relied upon. With the background set from the desktop research, the interview guides and the survey focused on understanding the point of view of both NRAs and providers in their respective countries. Focus was given in understanding the differentiating factors in each country as well as the successes and failures. The interviews were structure around 5 key areas in order to provide the fullest picture:

- The new security measures implemented in the member states ;
- The transparency resulting from the incident report process;
- The learning process resulting from the incidents ;
- The level of collaboration between the stakeholders ;
- The harmonization of the procedures within the European Union.

Respondents: 22 respondents (exclusively NRAs) for the online survey, 14 participants for telephonic interviews (both NRAs and providers).

[4] https://resilience.enisa.europa.eu/article-13/guideline-for-minimum-security-measures
[5] https://resilience.enisa.europa.eu/article-13/guideline_on_threats_and_assets

2. Status of Art. 13a implementation

2.1. Introduction to Art. 13a

2.1.1. Requirements

Art. 13a states that the EU member states shall ensure that telecom service providers "take appropriate technical and organisational measures to appropriately manage the risks posed to security of networks and services" and "take all appropriate steps to guarantee the integrity of their networks, and thus ensure the continuity of supply of services provided over those networks".

A closer look on the article, will reveal 3 terms: "security incidents", "security breaches" and "integrity losses":

- Paragraph 1 requires "that measures shall be taken to prevent and minimize the impact of security incidents on users and interconnected networks"
- Paragraph 2 requires providers to "take all appropriate steps to guarantee integrity of their networks, and thus ensure the continuity of supply of services".
- Paragraph 3 requires "to notify the competent national regulatory authority of a breach of security or loss of integrity that has had a significant impact on the operation of networks or services"

The use of the term integrity in the article text may be confusing to some readers. We refer to the definition in technical literature on networks and network interconnections[6], which defines integrity "as the ability of the system to retain its specified attributes in terms of performance and functionality". Integrity of networks would be called availability or continuity in most information security literature[7]. In this document we call these types of incidents simply "security incidents" or "incidents" and we use the following definition in this document: ***a breach of security or a loss of integrity that could have an impact on the operation of electronic telecommunications networks and services.***

In this respect, although we may assume that Art. 13a relates mostly with the availability of the service, as its main purpose is to "ensure the continuity of supply of services", the text of the article allows certain interpretations as regards to the scope. According to the graph below (Fig. 1), ***the requirements related to continuity/availability of the services has been implemented by 100% of the surveyed NRAs***. Nevertheless, some countries have made a step further and covered in their national implementation other security concepts than availability, such as confidentiality (Fig. 1).

Furthermore, telecom service providers have the obligation to notify the competent NRA regarding any breach of security or loss of network integrity that has a significant impact on the operation of networks or services. In this case also, ***100% of the NRAs implemented an incident reporting process for any disruption/ outages in the electronic communications networks and services***, while a minority (20%) also included breaches impacting information confidentiality or denial of services attacks not necessarily impacting the availability of the electronic communications (as shown in Fig. 2). This requirement is also followed by all EU member states along with some EFTA members also.

[6] Ward, K, 1995, 'The Impact of Network Interconnection on Network Integrity'. British Telecommunications Engineering, 13:296–303.

[7] In information security literature the term 'integrity' usually refers to the property that data or communications cannot be altered or tampered with.

Figure 1: Scope of Art. 13a national implementation (security measures)

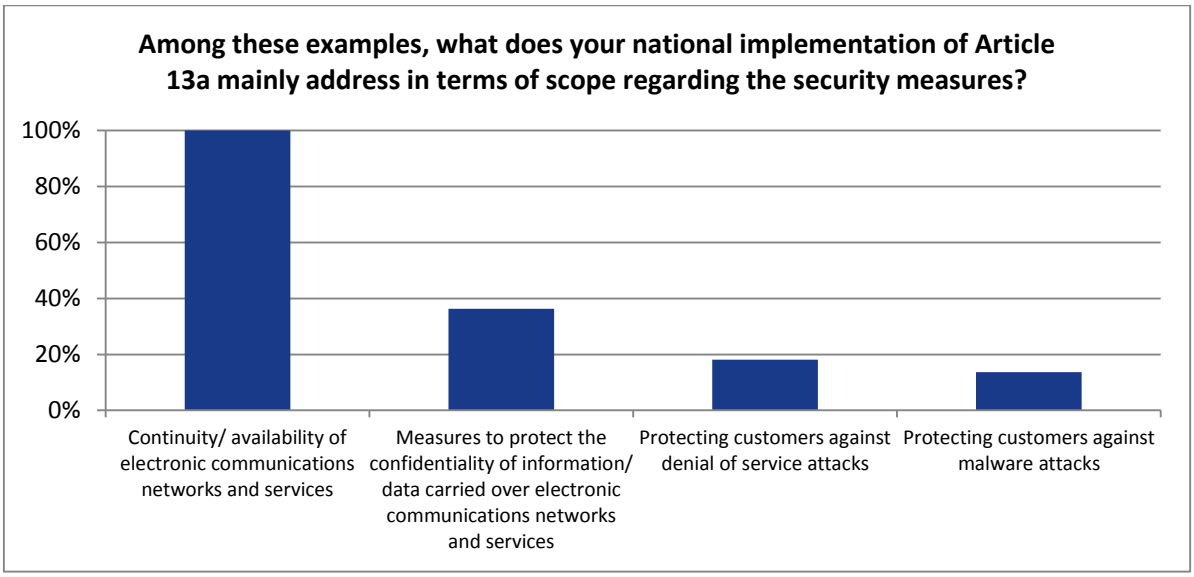
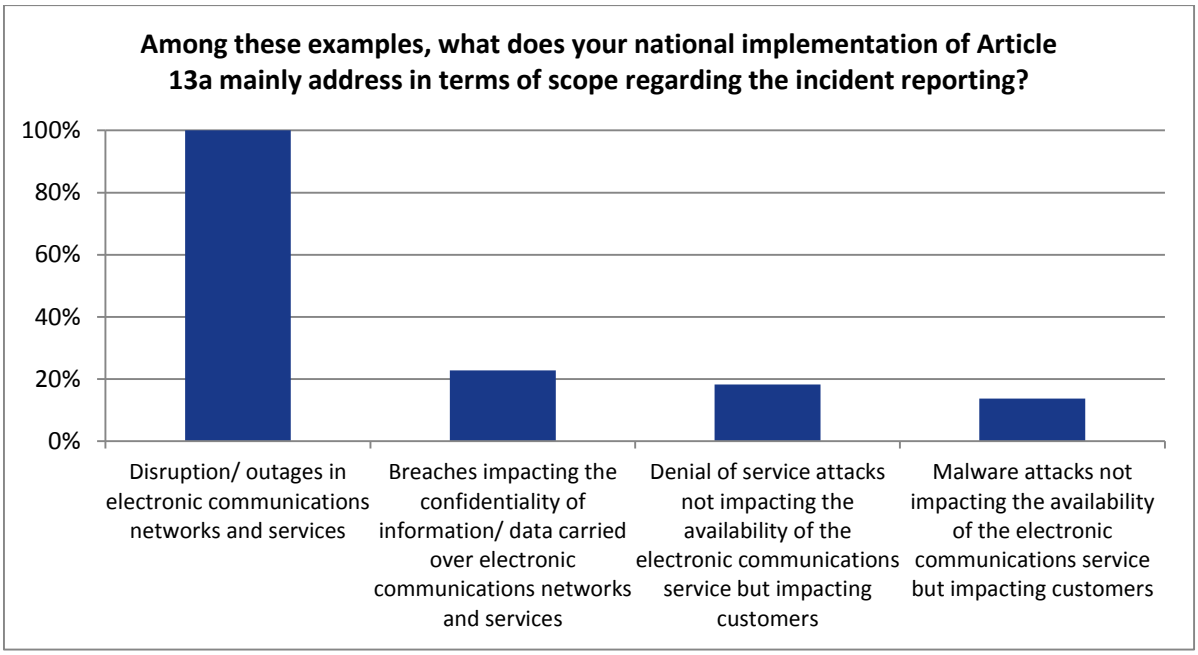


Figure 2: Scope of Art. 13a national implementation (mandatory incident reporting)

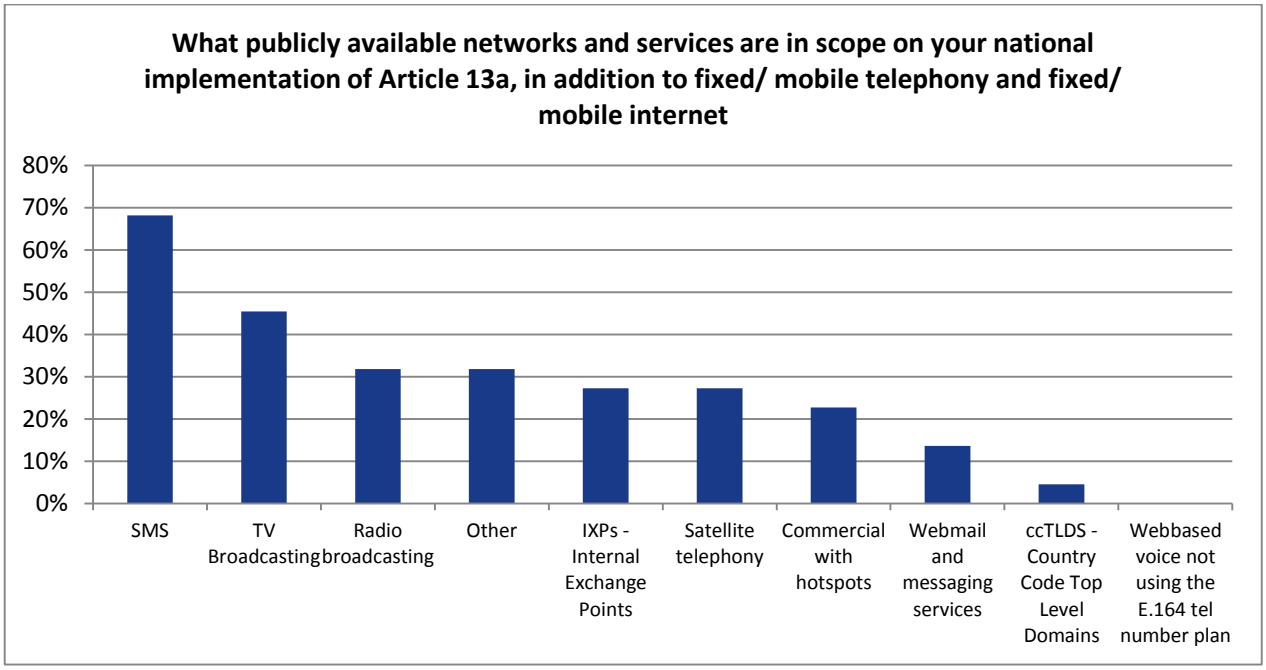


After receiving reports/notifications at a national level, NRAs shall report to ENISA any incident that had a significant impact on the operation of networks or services***. As the term "significant incident" has not been defined by the directive***, neither has been defined within the national implementations of Art. 13a in most of the countries, ENISA, in collaboration with the Art. 13a Expert Group has defined "significance" by adopting certain thresholds through a set of informal guidelines, adopted/referred to by all member states, as shown in Chapter 1 - Introduction.

2.1.2. Networks and services in scope of Art. 13a

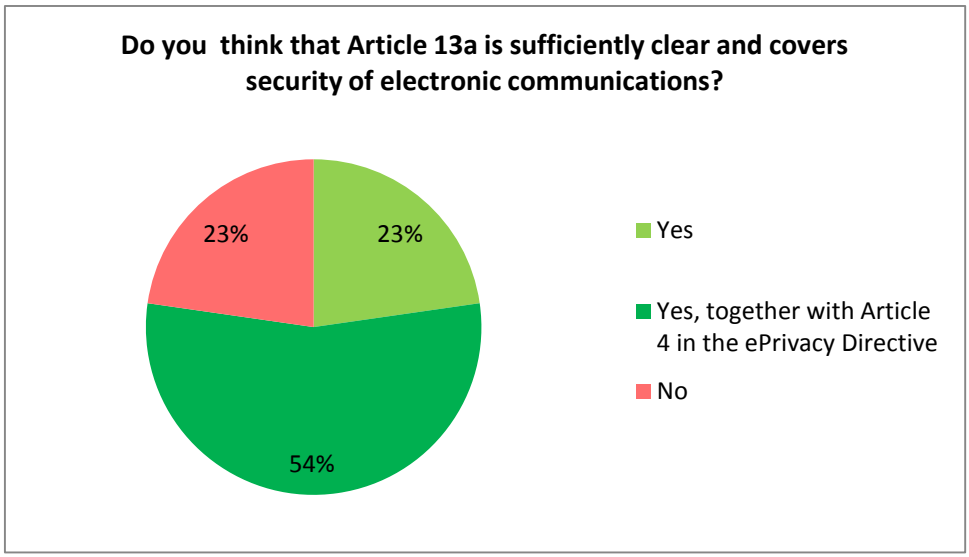
Art. 13a aims at safeguarding network availability through minimizing the impact of security incidents and ensuring the continuity of service supplying provided over those networks. The article applies for several types of networks and services, depending on the national implementation of the directive by each member state. Services such as ***mobile and fixed telephony but also to mobile and fixed internet are covered by all member states***. In addition to these networks and services, NRAs included in Art. 13a several other services such as SMS (almost 70%), TV and radio broadcasting (45% and 31% respectively), according to their national implementations of the framework directive. For a full set of networks and services covered by national implementations of Art. 13a please see Annex I.

Figure 3: Services in scope of national implementation of Art. 13a



As telecommunication networks and services can also be affected by other types of incidents that may or may not have an impact on the availability of the service, we have also tried to understand if stakeholders (meaning only NRAs) are satisfied with the current types of incidents covered by Art. 13a as regards to the overall security of electronic communications within a member state. ***54% of the surveyed NRAs consider that appropriate level of security within the telecom sector is achievable together with Article 4 of e-Privacy Directive, so that more types of incidents could be covered***.

Figure 4: Coverage of telecom security by Art. 13a



2.2. Situation of the countries before the implementation of Art. 13a

Before the implementation of Art. 13a, the telecom security landscape was fragmented and very specific to each country, with no pan European regulation. In other words, the legal maturity, practices and governance of the network resilience of each country were very heterogeneous which impacted the transposition and implementation process according to the level of maturity.

Although the 2002 Telecom Package tended to obliterate the legal differences among the countries at EU level by providing harmonized guidelines, countries kept their national prerogative and transposed the requirements into national law according to their countries specificities, market and maturity. However, the differences observed during the implementation process of the 2002 Telecom Package resurfaced in the approach taken by each country when implementing Art. 13a requirements from 2009. As you may see from Fig. 3 (or the Annex 1) ***although all countries have implemented mandatory incident reporting for service disruptions on telecom providers, they do cover differently the types of networks and services in scope of Art. 13a, meaning that incidents affecting different types of services are reported by each state***.

2.2.1. Approach of the NRAs and providers

Art. 13a has been received in many different ways by the consulted stakeholders, ranging from reluctance to enthusiasm but most commonly by skepticism. NRAs and providers were challenged to have a clear understanding of the scope and how to assess the criteria defining the impact of an incident or the appropriate level of security measures as per Art. 13a requirements, although the provisions of the European regulations were quite unclear.

NRAs

When Art. 13a was initially published, many NRAs were uncertain about the level of details and precision of the Directive, because several aspects of it were left – on purpose – open for the NRAs' interpretation. For example, Art. 13a states that member states shall ensure that providers take all appropriate steps to guarantee the integrity of their networks, but does not specify what is meant by "appropriate steps" or how "integrity" is defined. In this situation, NRAs referred in their replies to the Technical Guideline on Incident

Reporting[8] for further clarity in aligning as much as possible the domestic practices with the expectations at European level. Following the consultation of these guidelines, some NRAs issued second level regulations and/or some specific guidelines to support their national providers in their national implementation process.

In addition, NRAs were invited on a regular basis to participate in the Art. 13a Expert Group, an information exchange group especially created in this context by ENISA. This group had a critical role in federating NRAs during and after the implementation process. During these meetings, NRAs shared their point of view, experiences and thoughts about Art. 13a requirements.

Providers

As far as providers are concerned, the reaction of those consulted varied significantly and it can be directly correlated with their level of maturity in terms of country legislation and practices as well as to the level and maturity of collaboration with the NRA. Therefore, in the cases where providers were very mature, they were for most indifferent to Art. 13a, as such requirements were already included in their day-to-day practices and obligations.

As far as was shown from the qualitative approach of interviewing providers, those with a good level of maturity were either eager to improve their process and security measures, or reluctant due to the additional cost and due to stricter rules. Small providers or immature ones were either welcoming Art. 13a, identified as a strong opportunity to improve or reluctant to these new requirements, due to the additional effort to be provided while they face limited resources.

As a conclusion regarding the providers, whatever their maturity and development was, had whether a reluctant or embracing attitude towards adopting the new requirements, depending more on other causes (like business processes) than their maturity. Unfortunately, the survey could not capture more insights on this area, future work needing to be done.

[8] https://resilience.enisa.europa.eu/article-13/guideline-for-incident-reporting

3. Appropriate security measures for providers

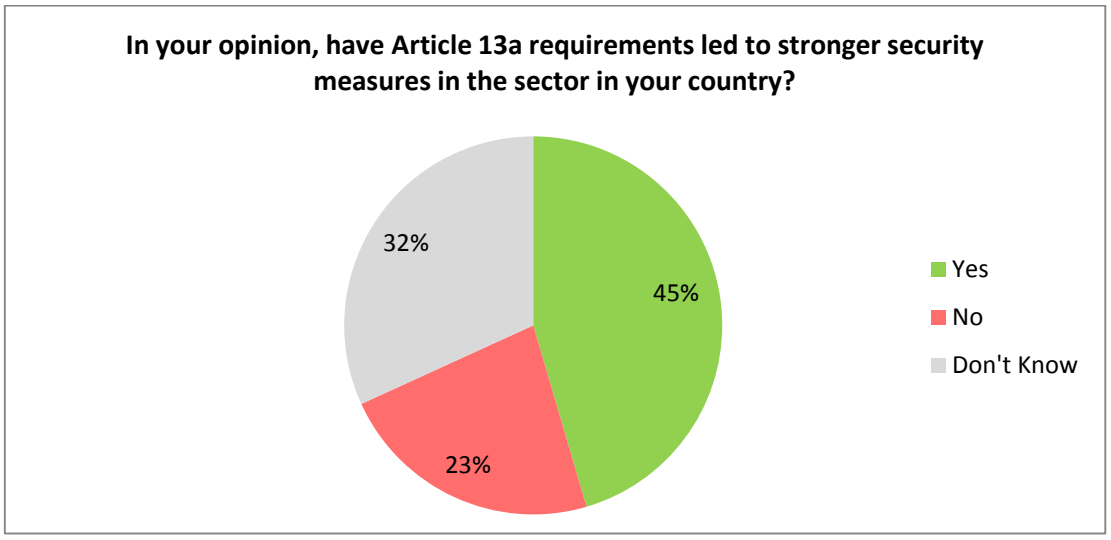
3.1. Specific objective context

Art. 13a requires NRAs to ensure that providers take the appropriate security measures to protect and guarantee the integrity and service continuity of their networks. In that regard, ENISA collected feedbacks regarding the level of satisfaction with the security measures implemented and assessed the resulting outcomes for providers and NRAs.

3.2. Level of satisfaction with the security measures implementation

It is noted that 45% of the interviewed NRAs are satisfied with the level of security achieved by implementing new security measures in their respective countries. Telecom service providers share the same opinion, although some of them adopted an approach that goes beyond the current legal requirements, with continuous improvement process and more demanding security measures.

Figure 5: NRA satisfaction regarding stronger security measures in the sector



For 45% of the respondents, Art. 13a requirements led to stronger security measures in the sector and the country. But, the majority of interviewed NRAs think that it is not possible to attribute this improvement only to the new security regulations. This is reflected by the heterogeneity of the answers, which can be attributed mostly to the fact that:

- *The level of implementation differs from one country to another*. Art. 13a requirements had an important impact on harmonizing the level of security measures among countries, as the general approach was highly different in some cases before the enforcement of the regulation. Although harmonizing has been achieved at the higher level, the situation still remains fragmented at lower levels of detail from one country to another.
- *NRAs do not have sufficient information from the providers to assess the impact of Art. 13a on the security measures already in place*.
- *Providers' maturity and the level of security measures vary from one country to another*. Thus Art. 13a requirements will impact the level of security measures in a heterogeneous manner, with more improvement and stronger impact in countries where the providers are less mature and where the legal framework is weak.

- *The variety in size between providers lead to a difference in impact*. For instance, Art. 13a requirements had a much stronger impact on small providers than on large providers. Small providers experienced an increase in security severity and overhead, while large providers did not face any particular issue or strong benefits.

Based on opinions expressed, providers, on the other hand, expressed two different. Either (a) they were already experiencing such level of security measures and did not see any particular changes, resulting in indifference or neutral opinion, or (b) they were quite satisfied with the level of security measures included in Art. 13a. ***The responses of the providers only underlined linear development in the industry, as more mature operators already had similar measures implemented, whereas the more immature ones had to invest some resources in adopting the new measures***.

3.3. Challenges encountered during the implementation

On average, most of the NRAs faced relatively small challenges with regards to the implementation of the security measures. The most common were:

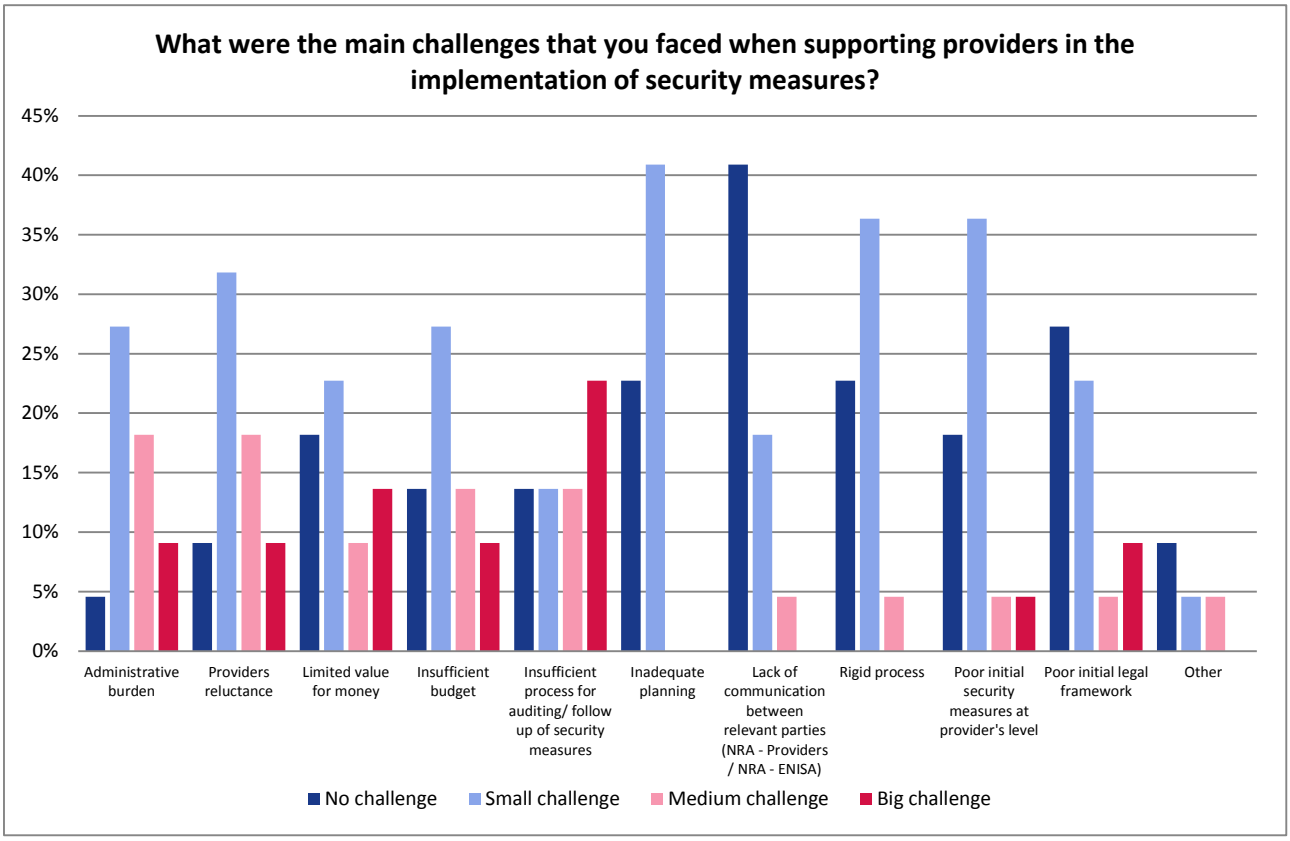
- 37% of the NRA respondents indicated challenges within the process of auditing and following-up on the security measures, meaning that ***after implementation of the regulations and the subsequent security measures, authorities found it difficult to check whether those measures/requirements were properly implemented***.
- 27% of the NRAs indicated as a medium to big challenge the reluctance of some of the providers in implementing the new regulations;
- over 25% of the respondents mentioned as a medium to big challenge the available budget and the administrative burdens;
- 21% indicated as a medium to big challenge the limited value for money as an outcome for the overall process, meaning that the expected benefits were not as consistent as expected.

It has been mentioned in the interviews that in most cases smaller providers were lacking the appropriate internal processes and methodology to implement these requirements. On top of that, most of them faced some operational challenges as they did not have sufficient resources and knowledge about the security measures to implement them without struggling at some point.

As revealed from the interview, another challenge in the implementation process of the security measures has to do with the lack of precision in the definition of “critical assets” and other key concepts such as “appropriate level of security”. Indeed, Art. 13a does not specify or define what is to be considered as a critical asset leaving the interpretation to NRAs. In order to overcome this challenge, providers and NRAs consulted the ENISA’s technical guidelines (see Introduction). Based on those some NRAs issued a second level of legislation as well as other guidelines.

As indicated within the interviews, the ***activities developed by ENISA within the area of Art. 13a, including hosting and coordination of the Art. 13a expert group, was perceived as an essential support in easing the implementation process and supporting NRAs and providers during their transition phase***.

Figure 6: Main NRA challenges during the implementation process



3.4. Outcome/benefit analysis of stronger security measures

The implementation of the Art. 13a requirements affected both NRAs and providers, in terms of resources needed. Even though policy making and implementation is the day-to-day business of most NRAs, they faced additional costs such as: educational costs (for training the providers on the new regulations), costs for developing secondary legislation or other guidelines, follow-up and audit on the progress of the implementation.

Providers faced implementation, maintenance and management costs. In their case, the size of the costs is largely depending on:

- the average level of security measures already implemented in the providers in the country
- the flexibility / ability of the providers to comply with the requirements within a short time frame
- the complexity of the process for security measures implementation
- the level of involvement of the NRA
- the availability and allocation of resources (FTEs[9]) necessary for the implementation process.

Some providers have been advertising security measures and resilience, as a competitive advantage. Especially in the countries where the level of the security measures was weak, providers emphasized the quality of their infrastructures, network and connections.

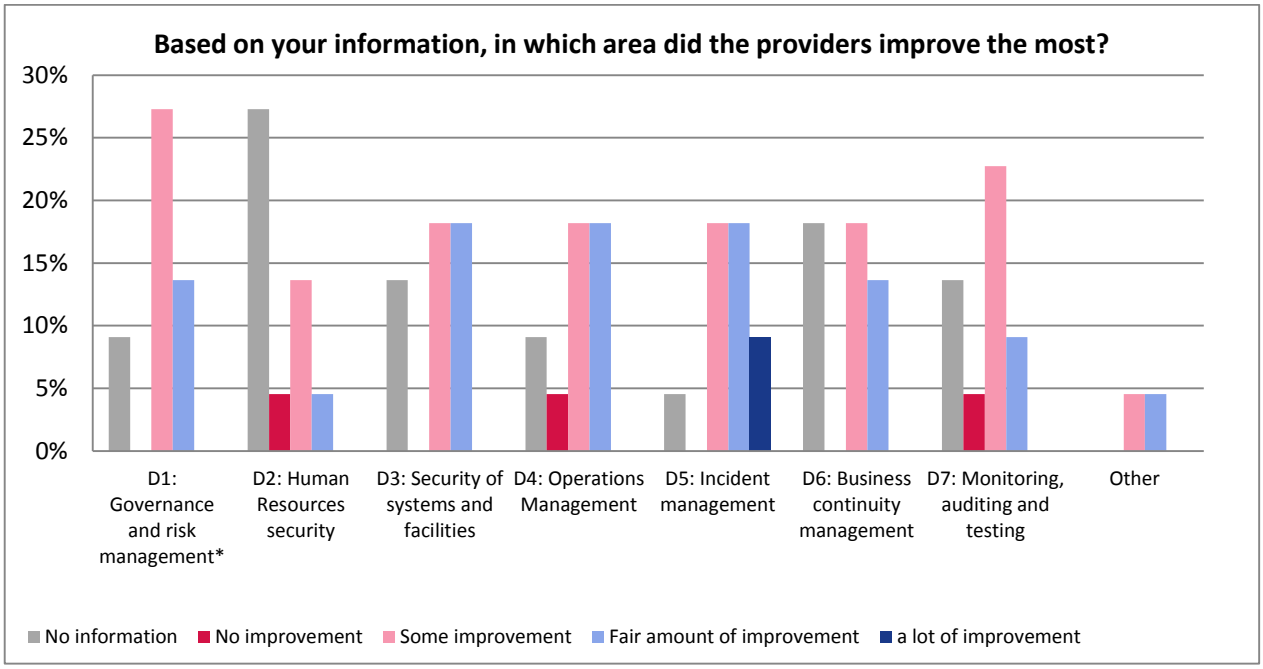
It is difficult to link the improvement of security measures with the evolution of the number of incidents experienced. Implementing better monitoring mechanisms may mean more incidents reported, which does

[9] FTE = Full time employee

not necessarily mean that the security measures have worsened. Providers deal with some external risks that cannot be controlled nor prevented by an increase of the security measures. Such risks mainly include environmental risks and malicious actions. As such it becomes difficult to measure direct benefits attributed to Art. 13a.

Nevertheless, ***according to the consulted parties, Article13a has definitely helped in reducing the risks related to infrastructure resilience through reporting and learning***. That is especially true for the smaller or less advanced operators, where technical assistance and know-how were needed. For larger operators, especially in more developed countries, the security measures where already implemented as part of their corporate strategy.

Figure 7: Areas in which providers improved the most



*based on Art. 13a Technical Guideline on Security Measures

The numbers from the Figure 7 discount the fact that in many areas, NRAs do not have sufficient information to assess whether Art. 13a brought improvements. For instance, 28% of the surveyed NRAs do not have information on the improvement level regarding human resources security and 18% don't know if Art. 13a positively impacted business continuity management.

Moreover, NRAs estimate that in general, stronger security measures have indeed improved the overall security in their countries. As shown in Fig. 7, NRAs consider that most of the improvements were done in the following areas:

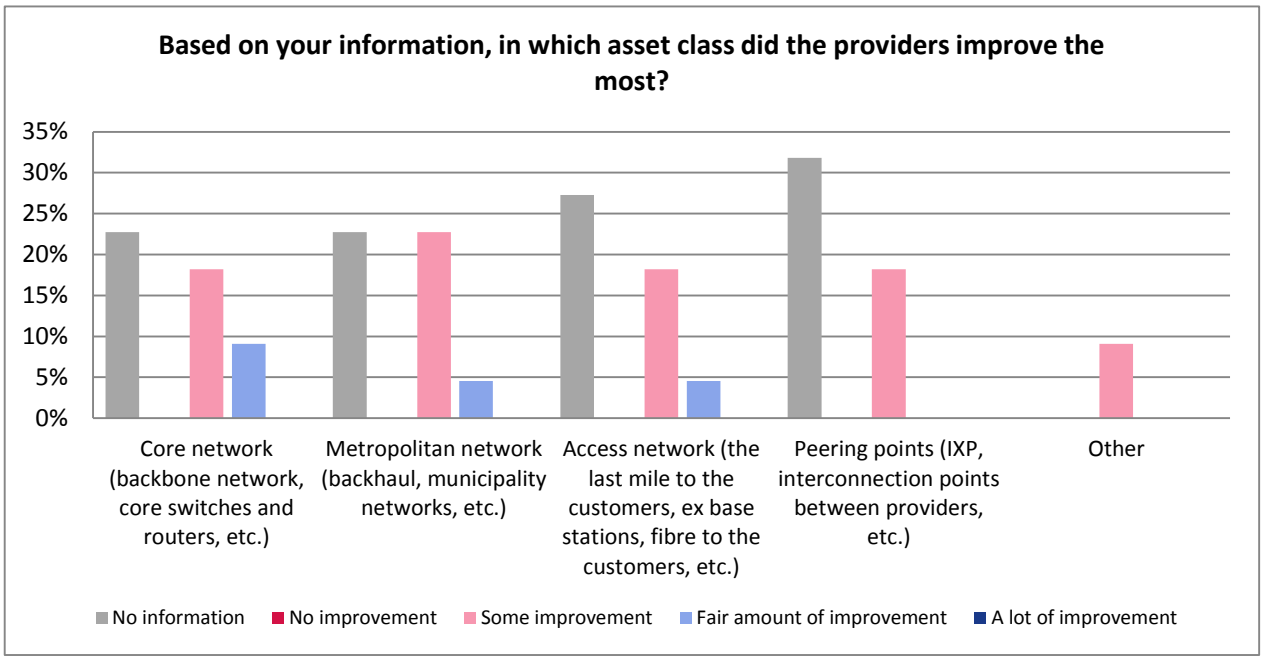
- incident management (27% fair amount or a lot of improvement)
- operations management (18% fair amount or a lot of improvement)
- security of systems and facilities (18% fair amount or a lot of improvement)
- business continuity management (14% fair amount or a lot of improvement)
- governance and risk management (14% fair amount or a lot of improvement)

It is reported that for front-runner providers, when Art. 13a came out, it did not bring strong benefits compared to the practices already in place. In other words, as the security measures and practices were

already strong and well implemented, front-runners did not gain strong benefits from Art. 13a security measures. Security measures positively impacted the quality of the infrastructures and thus of the services provided, which is the core business of telecom providers.

Regarding the improvements on the assets operated by providers, Fig. 8 expresses the opinion of NRAs on this matter.

Figure 8: Asset classes most improved by providers



3.5. Areas of further improvement

Suppliers of telecom components have a key role in the resilience of the infrastructures, but are not included in Art. 13a requirements. In case of a security incident, only the telecom service provider is responsible while the telecom components suppliers are not part of the legal action/ incident action. Further assessments in this area are needed, with the involvement of responsible stakeholders, in order to develop an optimal approach to addressing this issue.

As more than half of the respondents (55%) haven't indicated that Art. 13a has led to stronger security measures in the sector, and 60% of the respondents are not aware of areas where providers have improved the most, further analyses must be carried out in this area in order to determine next steps to be taken. ***Adoption of common baseline security requirements for all EU telecommunication providers has been indicated as a possible further development***. ENISA has already done some work in this area, please check the Technical Guideline on Security Measures.

4. Transparency in incident reporting

4.1. Specific objective context

Transparency is achieved through the reporting obligation that falls on providers experiencing incidents and is driven by the quality of information provided. Transparency is fundamental for the NRAs as they need correct and relevant information in order to take adequate and proper supervision measures. NRAs also have a reporting obligation towards ENISA and the European Commission, as information collected at national level is sent at European level for aggregated analysis. Therefore the more the information is detailed and transparent, the more the reporting flow is straight forward and the less NRAs request complementary information, which is time and resource consuming. All in all, transparency is an asset for providers, NRAs and ENISA as it enables the stakeholders to understand the issues faced in order to take appropriate actions (by the providers themselves, but also by the NRAs who can assist the providers or amend the national regulations in place).

In order to promote transparency, NRAs usually issue templates for incident reporting with a list of the mandatory information and the level of details required. Besides, providers have a specific point of contact at the responsible NRA to enhance communication and anticipate any need for further information.

4.2. Level of satisfaction regarding the transparency in the incident reporting

On average, NRAs are satisfied with the level of transparency reflected in the incident reports filled by the providers, meaning that the information quality of the incident reports is satisfying. This part assesses in more detail the level of satisfaction regarding the level of transparency, based on 3 perspectives:

- the provider's compliance with the expected level of information transparency,
- the information quality,
- the number of incident reports collected.

4.2.1. Providers' level of collaboration

Providers' attitude towards Art. 13a mandatory incident reporting regulations was mostly collaborative, as 68% of the respondent NRAs attest that providers were overall collaborative with the incident reporting compliance requirements (Fig. 9). Nevertheless NRAs also faced two other distinct behaviors. On the one hand, most of the providers were neutral or even indifferent (up to 40% of the responses) regarding the new incident reporting requirements and provided the reports as required as per the defined thresholds. This is due to the fact that some providers were already using such process at internal level and that Art. 13a did not bring major changes, constraints or benefits on this point. On the other hand, a minority of providers (21% of the responses) were reluctant towards the changes imposed by the new incident reporting process. These providers are mainly from countries were the practices are not as mature as in the most advanced countries and are, in most cases, small providers. This attitude can be explained by the investments that providers were asked to do in order to complete the requirements. Such investments can prove to be a real challenge for smaller providers with limited resources (financial or otherwise).

As an incentive to promoting a more collaborative and transparent approach for providers, 86% of NRA respondents stated they have issued several guidelines or country level legislation to fill in the lack of precision in the directive and mitigate the level of reluctance due to the lack of information. As shown by Fig. 10 below other measures adopted by NRAs to promote transparency are: provide online tools for incident reporting (59%), issue second level regulation on top of the standard requirements (inform customers (59%), inform general public on major disruptions (41%)), inform other member states, ENISA or the public for major disruptions.

Figure 9: Provider's attitude towards mandatory incident reporting

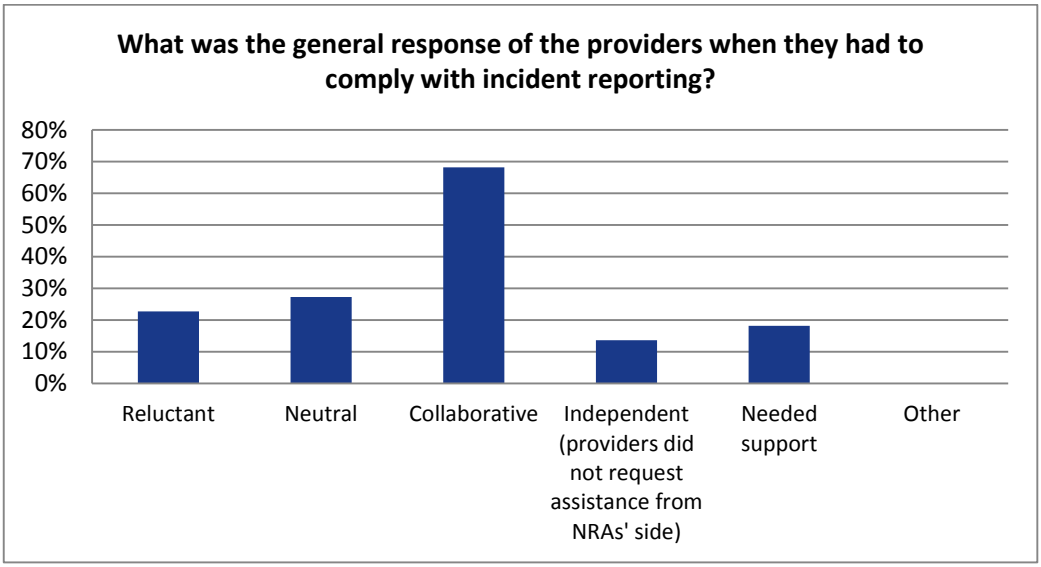


Figure 10: Measures for promoting transparency by NRAs

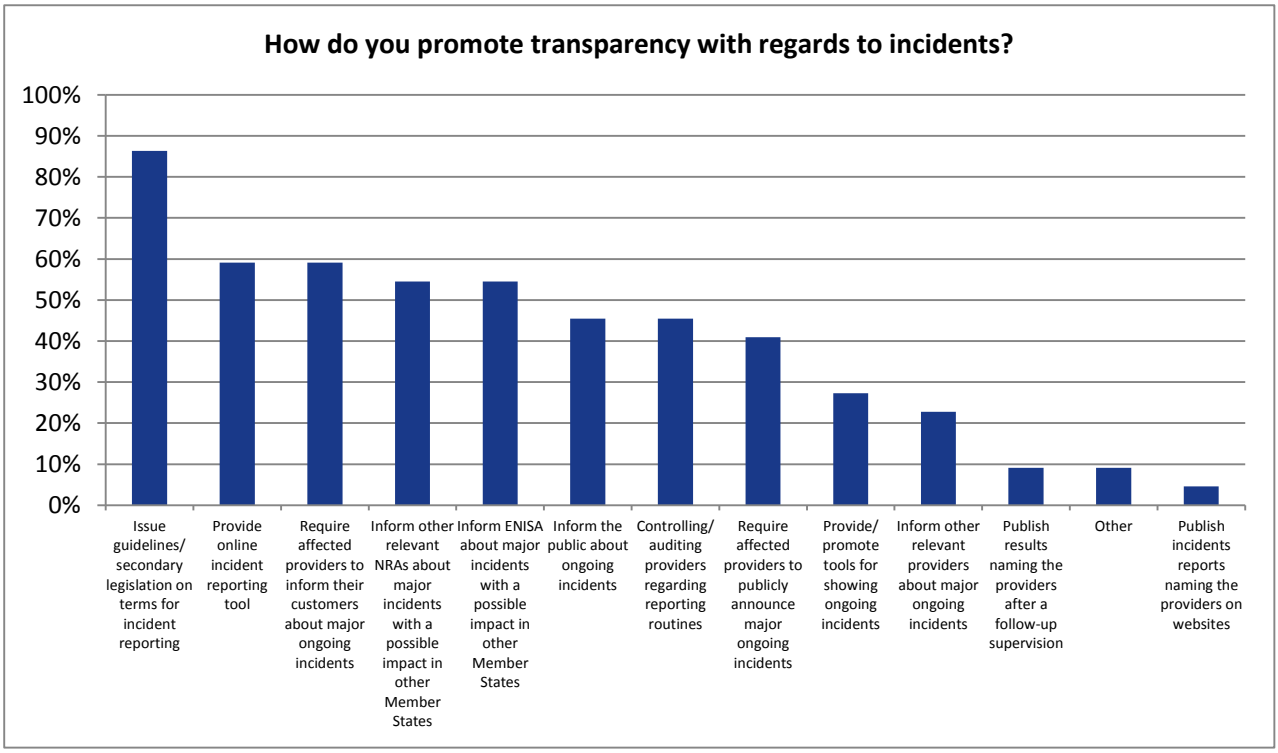
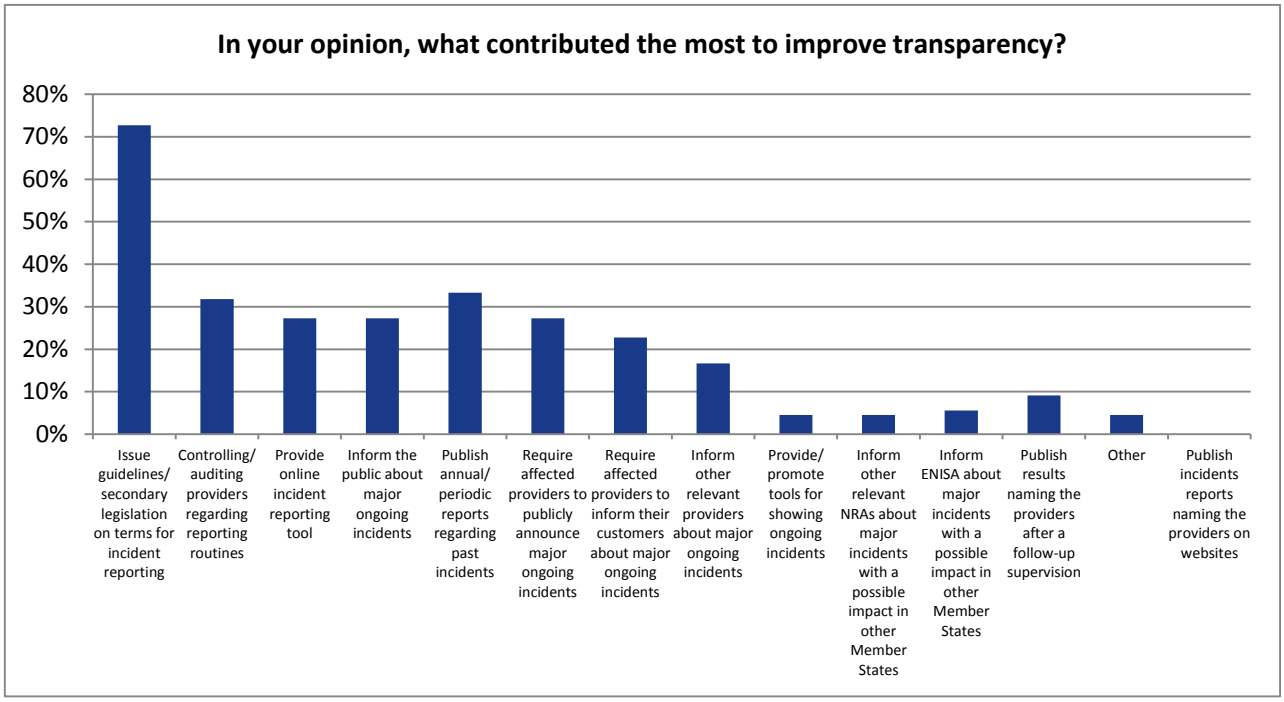


Fig. 11 reveals that, in NRAs opinion, ***bringing more clarity to the process (by issuing guidelines and additional legislation – 73%), was by far the most effective method of improving transparency***.

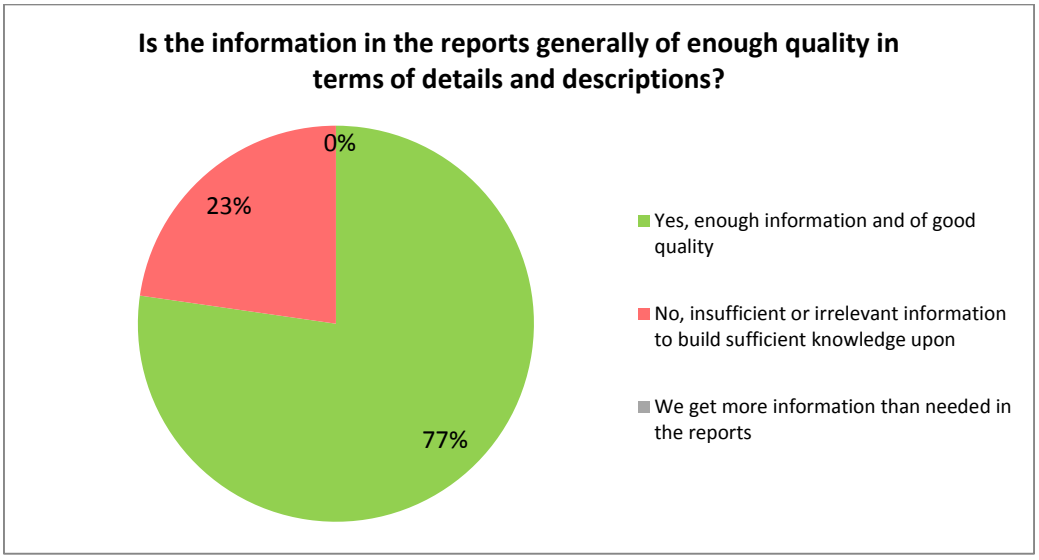
Figure 11: Measures that contributed most to transparency



4.2.2. Regarding the information quality

77% of the respondent NRAs are satisfied with the quality of the information provided by the operators in their incident reports. Information collected by NRAs mainly follows the ENISA guidelines on incident reporting. Most relevant pieces of information reported are: numbers of users/connections affected, duration of the incidents, services affected, assets affected, measures taken etc.

Figure 12: Opinion regarding the information quality



In cases where the information provided is insufficient, usually NRAs contacted the providers to obtain the complementary information. Some common issues which were reported, include situations such as the incident description being too short, or the vocabulary used being too technical or too specific at the internal

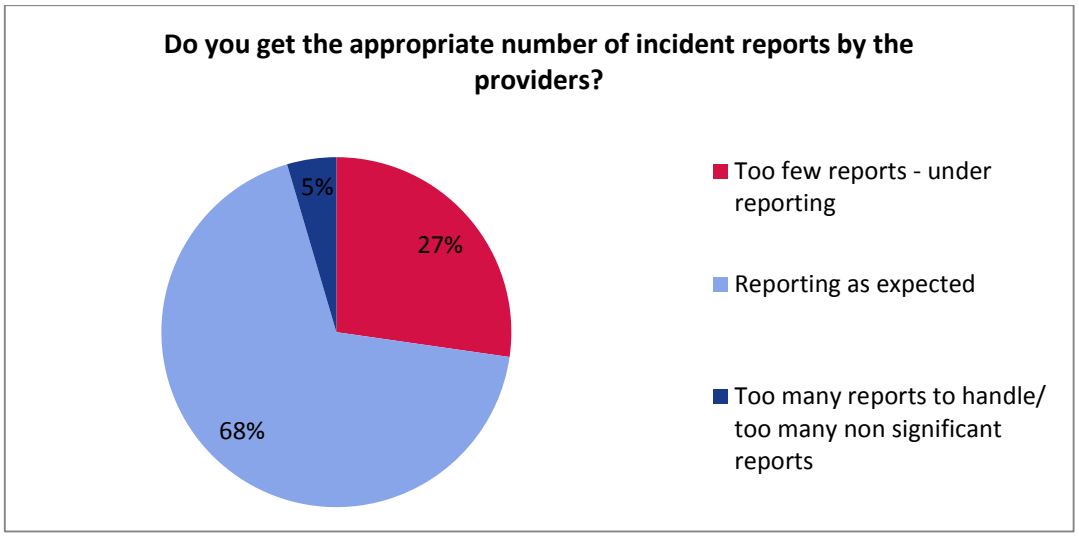
lingo of the provider's organization. Due to this feedback process, the level of the quality of the information self-maintains itself.

In the special case of emergency services incident or outage, providers are requested to provide more details and information in their incident reports, increasing transparency requirements for the providers.

4.2.3. Regarding the number of incident reports collected

The number of reports collected by the NRAs is linked to several factors. First and most important is the level of thresholds that determines whether an incident report is triggered or not. As the directive does not specify details regarding thresholds or how "significance" should be detailed, the Art. 13a expert group, has issued a non-binding document to help member states define significant incidents. The ENISA's Technical Guideline on Incident Reporting establishes absolute and relative thresholds, so that countries in different sizes in terms of population or providers in different sizes in terms of customers can be covered.

Figure 13: Appropriate numbers of incidents collected



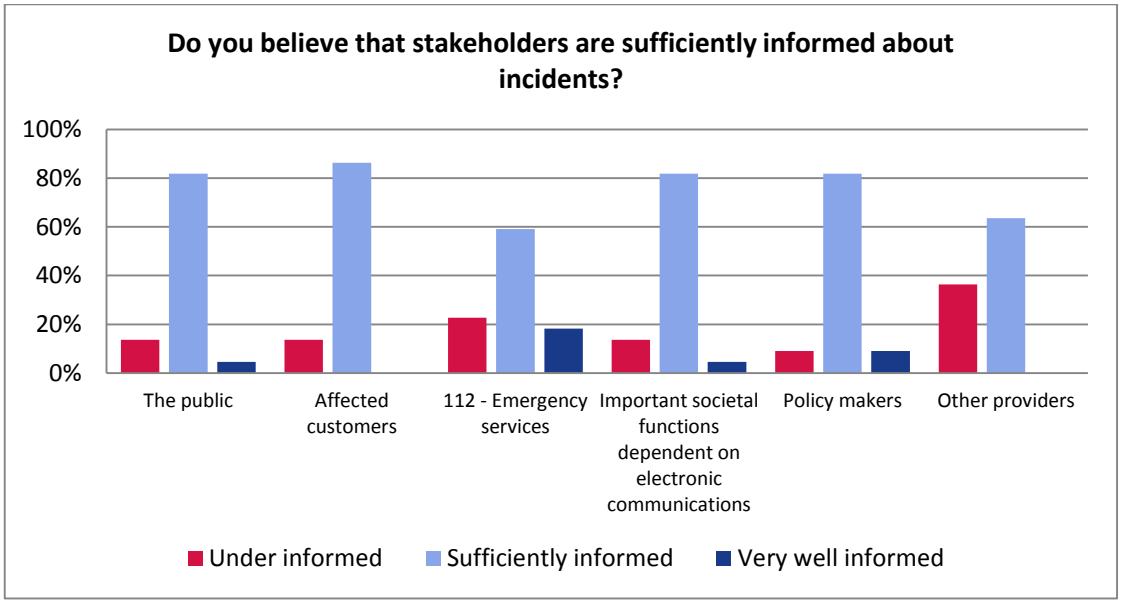
68% of the surveyed NRAs reported that they are receiving reports as per the expected levels, however one third of the surveyed NRAs do not receive as many reports as expected. One of the reasons could be that the thresholds are not fine-tuned to the number of incidents, market or provider size; therefore the reports do not capture as many incidents as expected in the first place. The second reason has to do with the size of the provider. Outages from small providers do not impact as many users as the larger ones, and as such thresholds do not trigger incident reporting in their cases. As no additional information was obtained in this area, this remains still to be further analyzed.

Another challenge addressed by the majority of the interviewed NRAs, is that 90% of the telecom services providers are SMEs, which represent only 10% of the incident reports received by the NRAs. Given that smaller providers (SMEs) – usually – do not have enough customers to breach the reporting thresholds, the vast majority of incident reports come from the large operators (the 10%). Consequently, ***the number of incidents reported could represent a distorted view of the status of each country***.

4.3. Level of communication

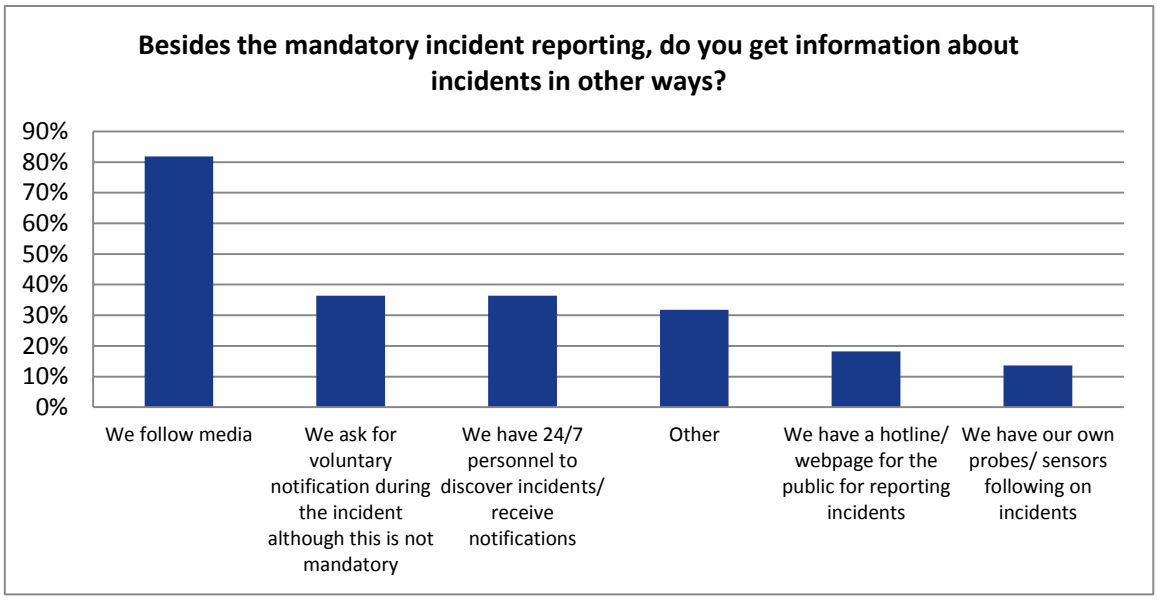
Although according to the surveyed NRAs, all stakeholders are sufficiently informed about the incidents (at least 50% of all stakeholders are sufficiently informed), some nuances are to be mentioned. After a deeper look, it appears that if sufficient communication takes place, it is often upon affected users request that information is disclosed and exclusively to this specific user. Instead of receiving information from providers, affected users often have to inquire themselves on the experienced incident. In some cases, it also happens that incident notifications are not published in the media or on the provider's website, whereas the thresholds have been reached.

Figure 14: Informing the stakeholders



Communication with affected users is not an obligation triggered by Art. 13a requirements, but can be requested by the NRA if the disclosure of the breach is in public's interest. Many NRAs took the opportunity to introduce a transparent communication with the population.

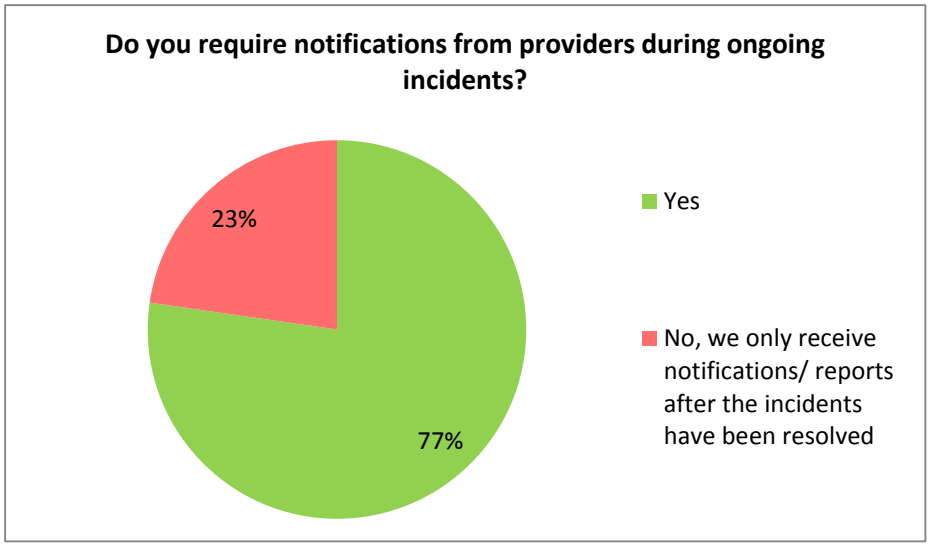
Figure 15: Additional sources of information



4.4. Challenges

From the interviews conducted, it appeared that the main challenge for providers, in terms of incident reporting and transparency is to compile a report while the incident handling process is in progress (77% of the NRAs answered that they require notifications from providers during ongoing incidents). In this case resources are allocated to the reporting process whereas they could be affected to the resolution of the incident. The full use of the resources for reaching other providers practices, level and maturity can be detrimental for the providers which are still in the maturation process. The incident may last longer and impact the providers' reputation and finances.

Figure 16: Incident notifications for ongoing incidents

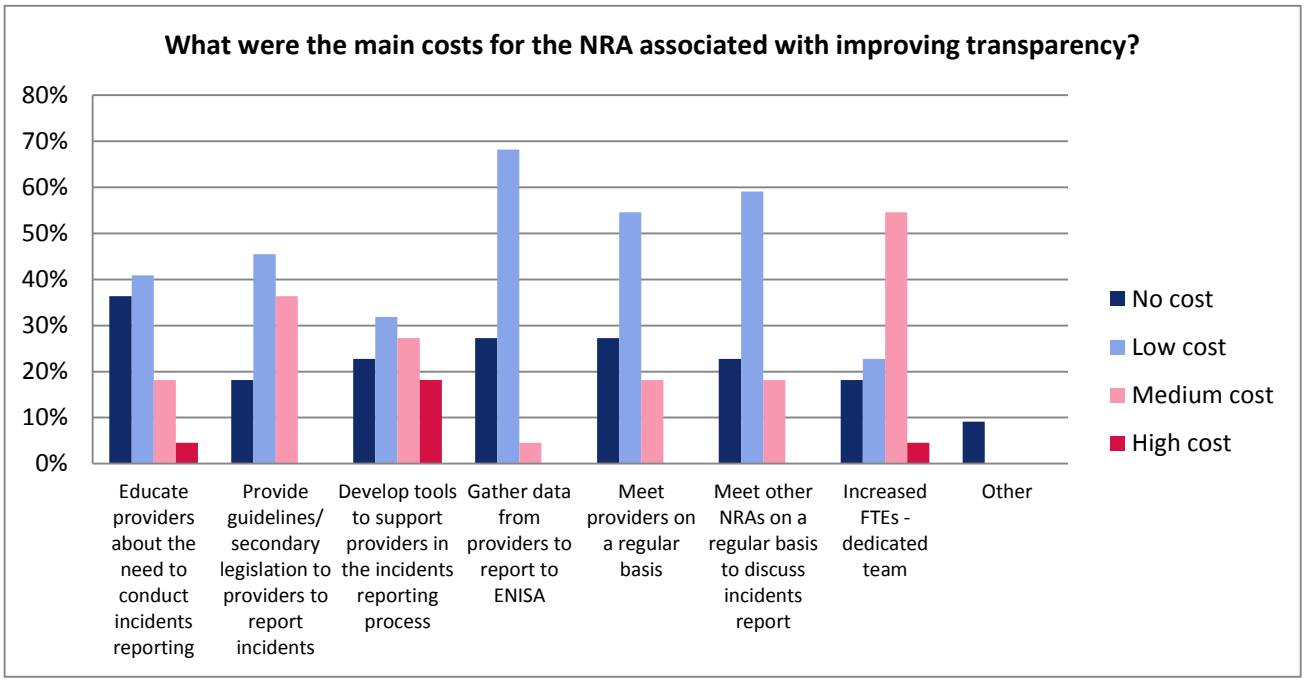


4.5. Outcome/Benefits analysis regarding transparency

4.5.1. Costs for the incident reporting from transparency requirements

Based on the graph below, for the majority of the NRAs, transparency requirements as per Art. 13a had a relatively low cost. The main costs regarding the improvement of transparency are the development of a new tool to support the providers in their incident reporting process and the creation (in some cases) of a dedicated team. Indeed 60% of the NRAs had to increase their workforce and faced this issue with a medium or high cost.

Figure 17: Main costs associated with improving transparency

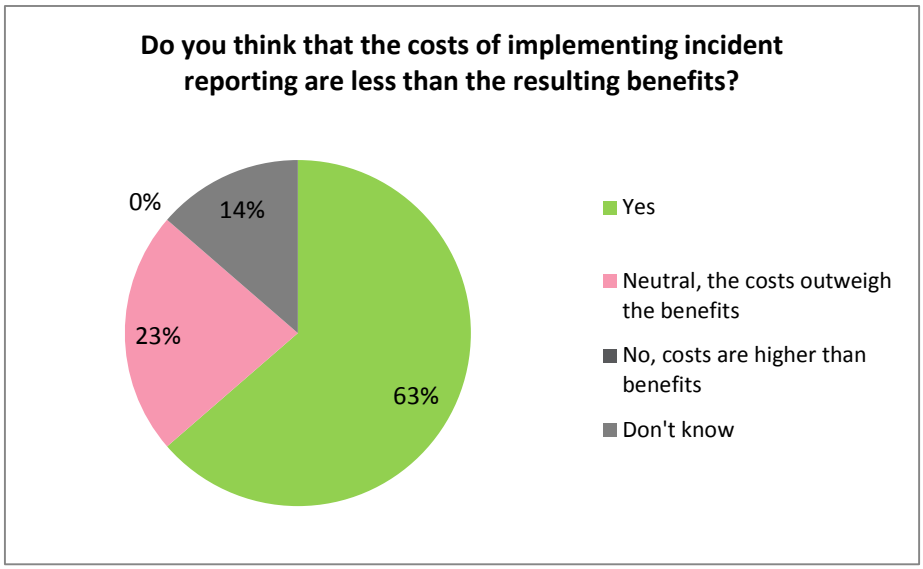


The burden supported by the providers with regards to the transparency highly depends on whether the indicators used by the providers are the same as the indicators used by the NRAs to assess the impact of the incident. When the indicators used are not the same between providers and NRAs, providers have to generate two reports with different indicators to assess, which is time and resources consuming. As a consequence, the quality of the report differs from one provider to another.

4.5.2. Benefits of the incident reporting from transparency requirements

Although ***for more than 60% of the surveyed NRAs, the implementation of an incident reporting process had greater benefits than costs***, the rest (40%) remains quite neutral on the question. It is certain that such process has been beneficial for the providers and NRAs, but 40% of neutral opinions show that there is still some space for further improvement.

Figure 18: Costs vs. benefits on implementing Art. 13a incident reporting



Incident reporting and transparency requirements, as requested by NRAs in their incident report templates, do contribute to the improvement of the information quality and quantity. Such transparency requirements benefit the NRAs because they have uniform and detailed information about the incidents in order to generate reports and country level analyses.

4.6. End – user feedback regarding Art. 13a

As part of this survey NRAs were inquired on whether the end-users have expressed any opinion on Art. 13a and whether there's any type of communication regarding improvements. The general consensus is that ***NRAs do not have feedback from end-users regarding these effects***. ***Most of the public remains unaware of the initiative***, and even if some improvement in the communications has been noticed, it would be difficult for the NRAs to gather the sentiment, and even more so, to attribute it to Art. 13a – related procedures (rather than advances of technology for example). Consequently, no feedback has been collected from the end – user (citizen) perspective.

4.7. Area of further improvement

Providers only officially report incidents to the NRAs but end-users do not have access to such information. Being business-impact orientated, in opposition to NRAs and ENISA which are more end-users orientated, some providers do not proactively communicate directly to their customers on the on-going faced incident. End-users have to either request the information or wait for the yearly report from the NRAs and ENISA to obtain information on the past incidents. Further developments in this area are needed ***to add more transparency to customers and the general public***, by periodically informing them about outages, measures taken etc.

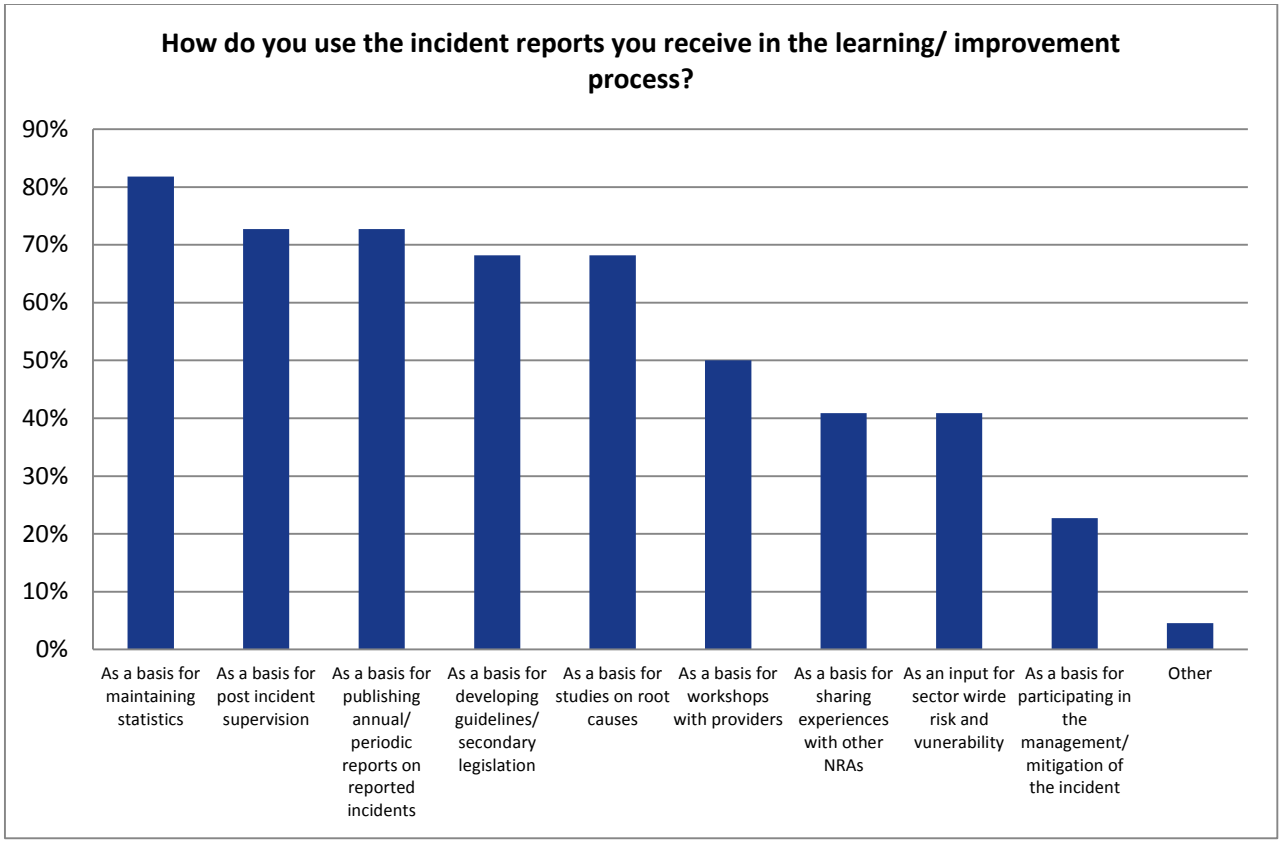
Current thresholds are more likely to trigger an incident report from large providers than from the small providers, resulting in NRAs receiving more incident reports from large providers than from the small providers. Consequently, NRAs have an overview only of the incidents that impact large providers. Thus NRAs should adapt the thresholds to capture incidents experienced also by small providers. However this option is difficult to implement because it assumes a ***very delicate fine-tuning of the thresholds in order to cover incidents affecting smaller providers***.

5. Learning and improving based on reported incidents

5.1. Incident reporting as a tool for learning

The incident reporting process is a tool itself to learn from incidents and to sustain a continuous and dynamic internal learning process for both providers and NRAs. According to the surveyed NRAs, incident reporting is used as a tool for learning in many areas, as shown in Fig. 19. Statistical purposes, post incident supervision, periodic reports, developing guidelines and root causes studies are areas where incident reporting is mostly used for learning, confirmed by 70% or more of the NRA respondents.

Figure 19: Areas where incident reporting is used for learning

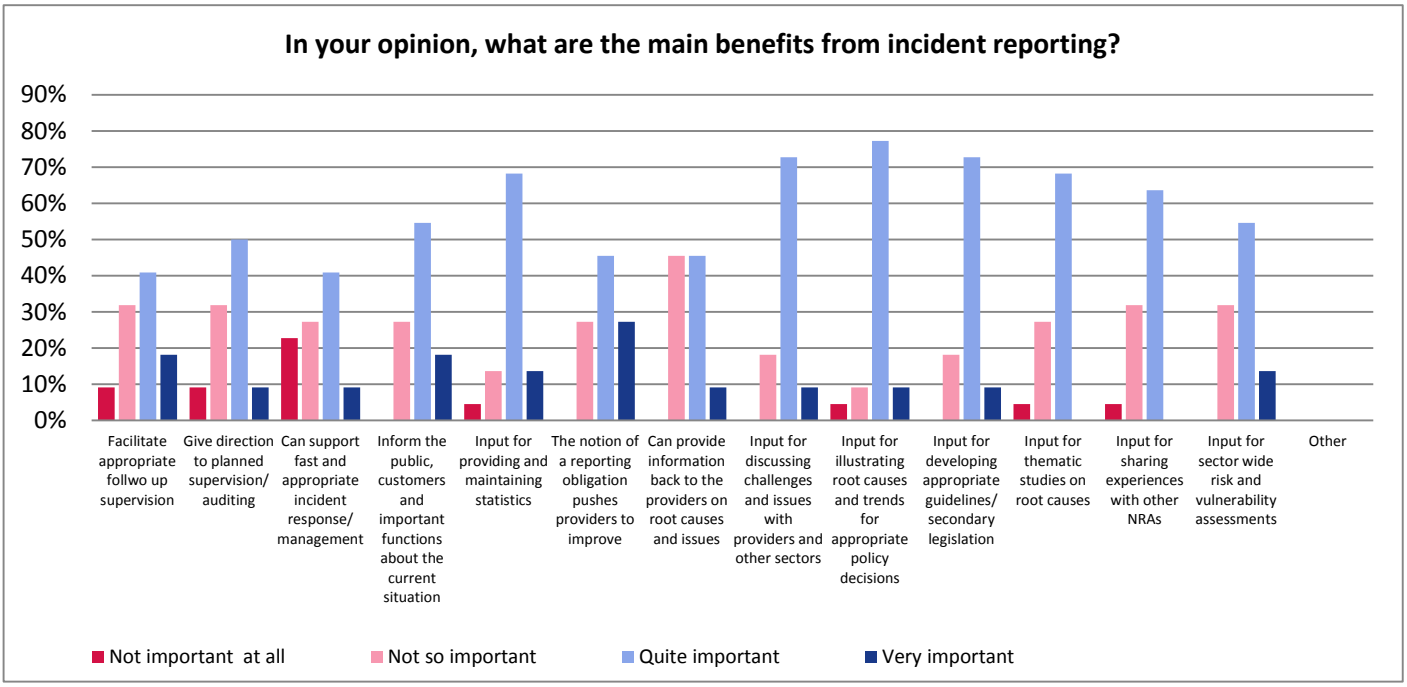


5.2. Outcomes/benefits of the learning process

Incident reporting and the resulting learning process contribute to continuously strengthening and maintaining providers' infrastructures. As reflected in the graph below, the notion of the reporting obligation pushes providers to improve (identified as an important benefit by 77% of the surveyed NRAs), and is an input for sector wide risk and vulnerability assessment (qualified as "quite important benefit" by 69% of the surveyed NRAs).

87% of the respondents also stated that the incident reporting process is used as an input for appropriate policy decision, meaning improving regulations within the sector.

Figure 20: Benefits of incident reporting



However incident reporting and a learning process cannot guarantee a drop in the number of incidents, especially in case of incidents that are due to environmental causes, although they surely contributed to improving the overall process of addressing different types of incidents.

5.3. Areas of further improvement

In this part, the suggestions made in order to further improve the learning process, as communicated by the surveyed NRAs and providers, are conflicting. Some NRAs and providers think that sharing more information regarding the learning and preventive actions taken could help other providers in their own incident solution process and would bring stronger knowledge to small providers. In addition, cross country collaboration on incidents and supervision matters for NRAs could be reinforced by more information sharing.

However, this suggestion raises the issue related to confidential information disclosure and a concern from providers regarding the risk of being penalized for the incident that they have experienced. In addition, such information sharing may not bring as many benefits as expected to the other providers as the impact and the corresponding solution may be specific to the infrastructures of the providers. Therefore driven solutions and lesson learnt may not be compatible from one situation to another or from one provider to the other.

As you may notice NRAs mostly use the incident reporting process as a tool in learning/improvement but mostly for compliance, internal statistics and improve regulations (Fig. 19). The percentage of those who use the results of the process also as an input for sector wide or nationwide risk assessment is rather low. ***Considering widening the usage of the results to other areas, related to national security or industry related risk analysis, could be a further improvement in this area***.

6. Collaboration between the actors

6.1. Specific objective context

Collaboration is at the very heart of the implementation process, especially when the telecommunications' market landscape is quite different from one country to another.

A successful implementation at national level is possible only if the NRA and the national providers work together, helping each other to overcome the challenges. NRAs involvement is all the more important given that small providers do not have as much experience as the front-runners and may face more difficulties in the implementation process.

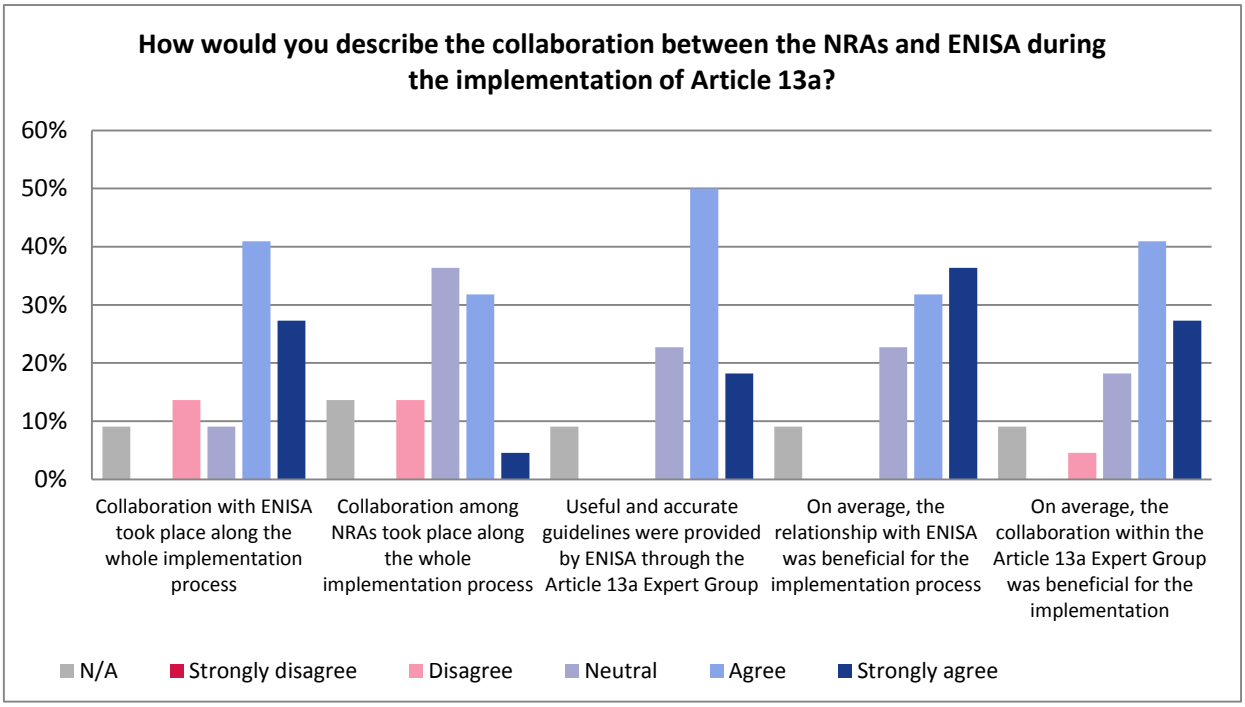
However, such collaboration faces some limits when brought at EU level. Indeed, providers and NRAs are hesitant in sharing confidential and sensitive data to other stakeholders, even in the context of Art. 13a and for collaboration and improvement purposes.

6.2. Collaboration during the implementation of Art. 13a requirements

6.2.1. Collaboration between ENISA and NRAs

ENISA's role has been to support NRAs along the implementation process of the requirements mandated in Art. 13a, to provide expertise, advice and to promote the exchange of good practices among the member states. In order to do so, ENISA built a strong relationship and collaborative working environment. As a matter of fact, ***68% of the surveyed NRAs agreed/strongly agreed that ENISA's role was beneficial for the implementation process***.

Figure 21: Collaboration between NRAs and ENISA



ENISA worked closely with the NRAs to provide more detailed information to them as well as the providers and has issued several guidelines. These guidelines have been helpful for the NRAs to better understand the requirements of Art. 13a, especially the scope and definitions, and to have a concrete perception of the threshold levels to set up. Indeed, ***ENISA's guidelines provide definition and advice to NRAs and providers on how to consider the interpretation of the requirements, and were very well received and appreciated by the community (as stated by 68% by the respondents)***.

Exchange of information between NRAs is facilitated by the Art. 13a Expert Group meetings, which are organized on a regular basis, and aim at involving all the EU member states in an open discussion about Art. 13a. This observation includes discussing implementation in detail, sharing knowledge and exchanging views, in order to achieve a harmonized approach of implementing Art. 13a.

6.2.2. Collaboration between NRAs and providers

As shown by Fig. 22 ***most of the NRAs indicated some overloading as regards to the implementation process of Art. 13a, but most of them rarely indicated overloads of more than 25% of the total time of the responsible personnel involved (FTE)***. In order to support their domestic telecom service providers, dedicated personnel within 20% of the NRAs spent half or more than half of their time to issue second level regulations, guidelines and educate providers. Developing reporting tools for providers was also indicated as time consuming by less than 20% of the respondent NRAs.

Regarding the collaboration between NRAs and providers, as described in Fig. 23, the majority (77%) stated that the collaboration lasted for the whole implementation period, and 64% of them declared that the providers requested additional supporting documentation, as guidelines or advice. Given the level of detail provided within the directive, we can certainly ***say that collaboration was more than necessary at this level, both at European level and at national level***.

Figure 22: FTE spend by NRAs during implementation phase

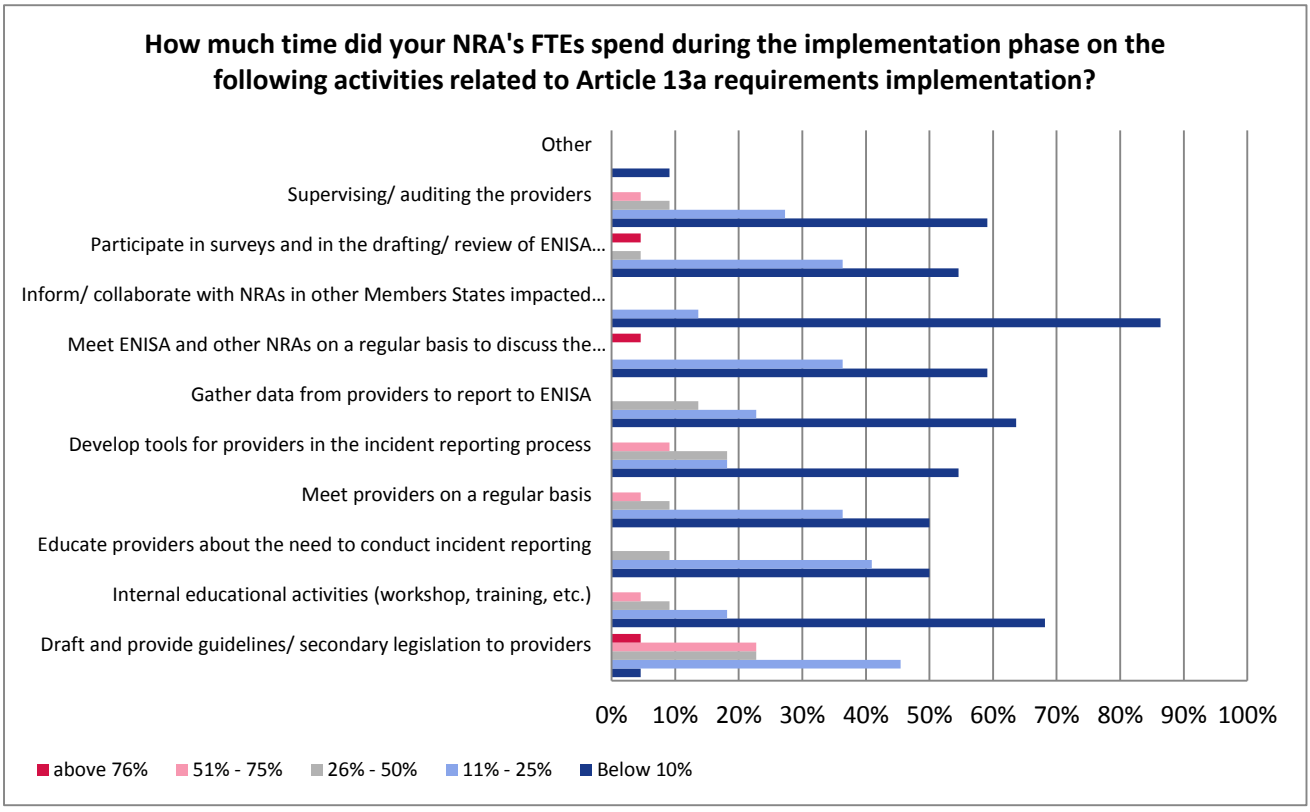
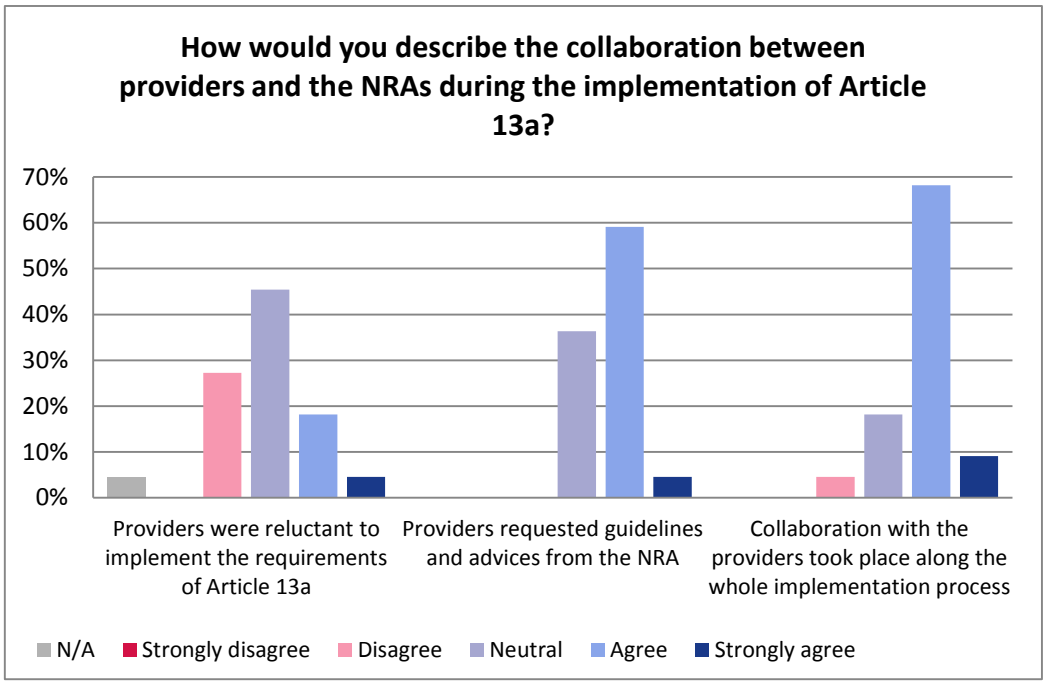


Figure 23: Collaboration between providers and NRAs during the implementation of Art. 13

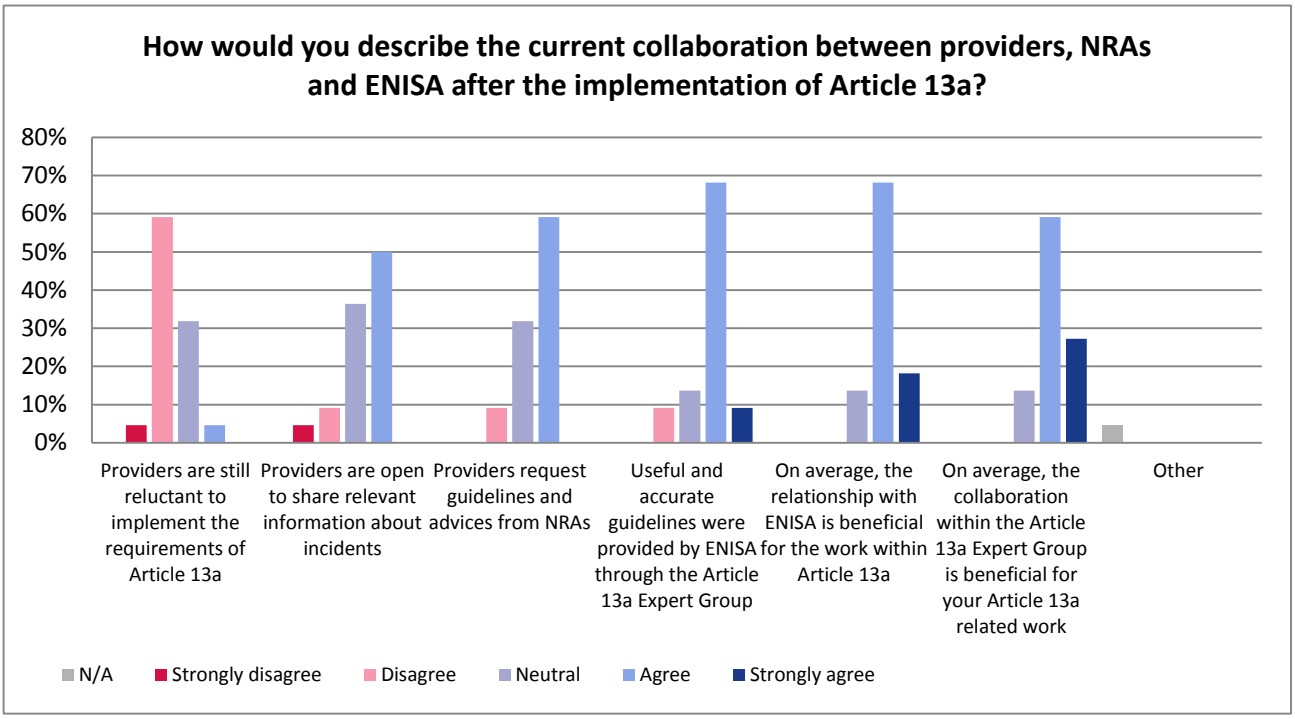


6.3. Collaboration after the implementation of Art. 13a requirements

As regards to the situation after the implementation period of Art. 13a, we can notice from Fig. 24 that collaboration between NRAs and ENISA was still needed, as by the majority of the respondents. More specifically ***guidelines on particular areas were still needed, and the overall activities carried out by ENISA alone or within the Art. 13 Expert Group are considered beneficial by more than 80% of the respondents***. ENISA continues to hold the Art. 13a Expert Group Meetings with the intent to keep a high level of collaboration and information exchange between the member states. The Expert Group is also a way for ENISA to measure the level of harmonization in regards to the member states practices.

The estimated time spent by the NRAs' FTE dedicated personnel during the implementation phase of Art. 13a (Fig. 22), with the time spent after the implementation (Fig. 25), is more or less the same, highlighting that Art. 13a has developed to a continuous process within NRAs. Although the implementation process is complete, providers still need the support of the NRAs, as further improvements to the incident reporting process are developed periodically and, as statistics show, the number of incidents is increasing. The only activity that sees its allocated time decreasing is the supplying of guidelines/secondary legislation to providers, as the market has reached a certain level of maturity within this area.

Figure 24: Current collaboration NRAs – ENISA after the implementation of Art. 13a

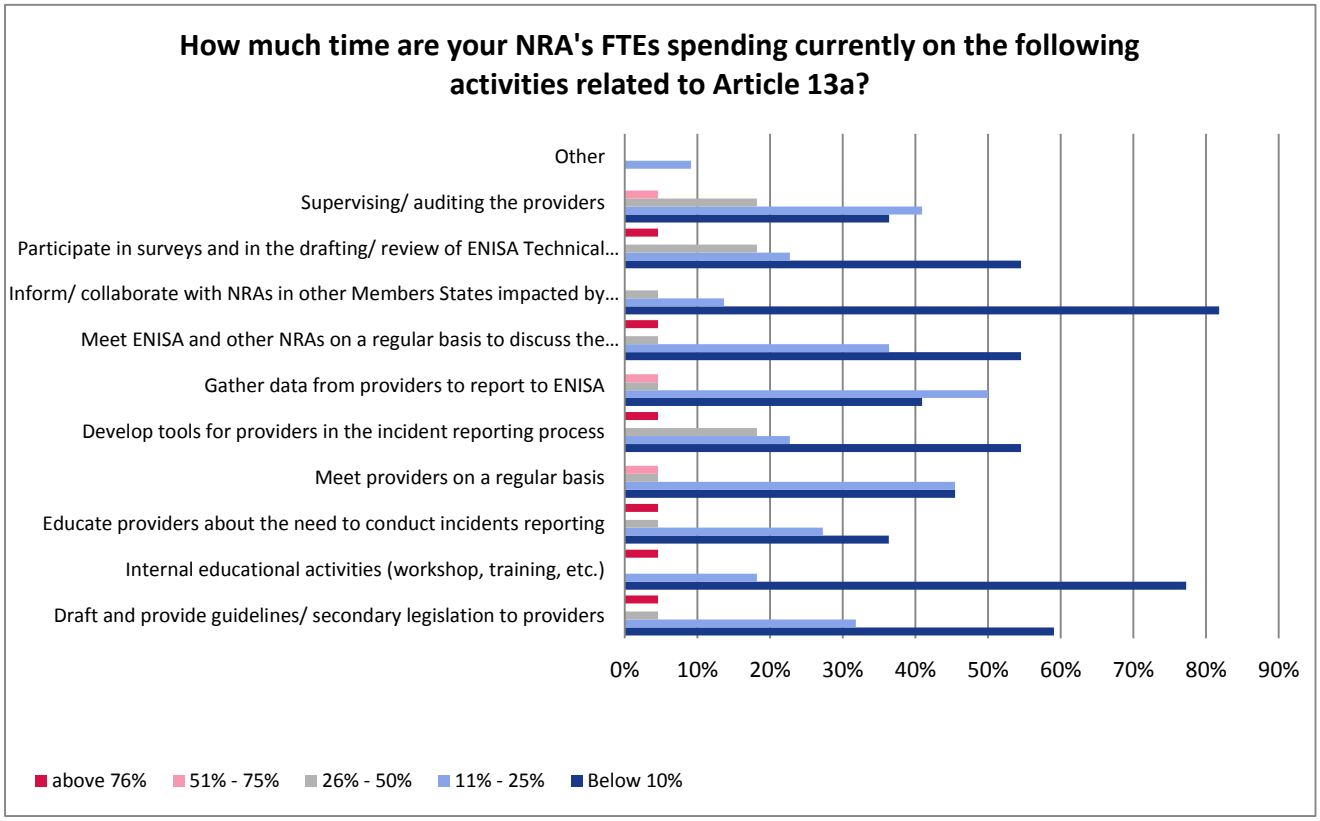


However the need for developed tools and supervision/audit of the providers remains almost the same as during the implementation process. This is the consequence of a need for a continuous effort in monitoring the measures implemented for compliance with Art. 13a.

This graph (Fig. 25) confirms that the ***cross border collaboration between NRAs remains quite limited as 82% of the surveyed NRAs estimate spending less than 10% in exchanging information with NRAs in other member states impacted by the same type of incident***. In addition interviewed NRAs confirmed that they did not often collaborate or exchange information with other NRAs on a regular basis.

Regarding the supervision and audit of the providers, 63% of the dedicated personnel within NRAs spent up to 50% of their total time doing this activity. Other time consuming activities are gathering data for reporting to ENISA, develop tools and meet with providers on a regular basis etc.

Figure 25: FTE spend by NRAs after implementation phase



6.4. Areas of further improvement

The opinions on the possibility and benefits of improving the current level of collaboration differ among different types of stakeholders.

On the one hand, for some NRAs, it would be useful to collect incident reporting and information from national providers, which will be anonymized, in order to share this information with the other NRAs, so their domestic providers have access to other providers' incident reports, experiences and practices. On the other hand, some NRAs do not agree with this proposition for several reasons. First, if the incident is a major incident and has been related in the media, it is always easy to find the identity of the provider. Secondly, some NRAs state that each incident is specific to a provider, a market structure, the providers' infrastructures, etc. and that it is not possible to adapt preventive measures from one country to another where the culture, infrastructures and market structure is not the same. Meanwhile ENISA is trying to develop, along with the Art. 13a expert group, a provider to provider sharing capability in order to facilitate this kind of cooperation and, of course, satisfy the majority of requests by member states.

However, providers do share their need for more information exchange on the incidents experienced by other providers. This information sharing is already in place in some countries, under the NRA's supervision and in project in some others. Providers also underline their continuous need for feedback and support from their NRAs on incident reporting quality and assessment, and a true bi-directional beneficial communication.

Last but not least, collaboration could be improved further, as the different indicators used by NRAs and providers to measure the impact of an incident are not aligned. If this situation is persistent, it shows that communication and collaboration are not optimum between NRAs and providers.

7. Harmonization of practices within the EU

7.1. Paradox: harmonization at EU level vs fragmentation at country level

7.1.1. Harmonization vs differentiation

In the European Union, directives prevail on national law and bind upon the EU member states as to the implementation of the requirements, regardless the specificities of the national law. EU member states have an obligation of transposition into domestic legislation, although they are free to choose the means and the ways to reach this objective within the given time frame. Lastly, countries are always free to adapt the requirements on the national level. Differences between countries can include: difference of maturity, different practices and cultures, etc. For example, some countries issue one or two incident reports annually, while other countries can issue hundreds.

If the directive sets up minimum standards to be implemented within national legal framework, member states are free to apply more demanding national measures, as long as they do not conflict with the requirements of the directive and with the free movement and free market rules. Although this principle wants to respect countries' sovereignty, this is a source of differentiation among countries. If the legal framework is by definition harmonized at EU level, the content of the domestic law is impacted by the countries specificities and needs. For instance, thresholds that trigger the incident reporting process are different from one country to another, although the NRAs referred to the *ENISA's Technical Guideline on Incident Reporting*. This guideline and the others aim at providing more details and indications to the NRAs in order to facilitate the implementation of Art. 13a requirements.

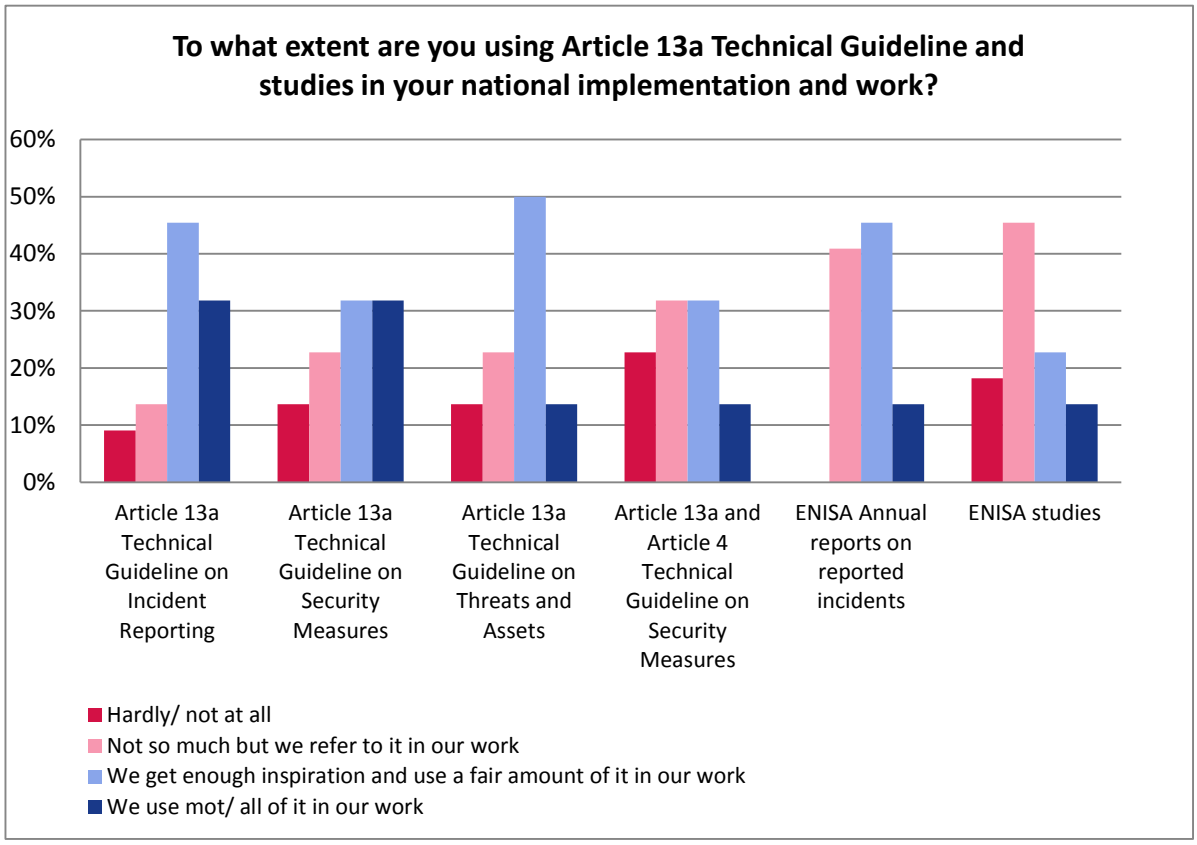
As per the Directive 2009/140/EC, member states were required to conduct a national public consultation to "give interested parties the opportunity to comment on the draft measure within a reasonable period[10]" but remain free to take the results more or less into consideration.

In the context of Art. 13a, the transposition of the directive into domestic law has been successfully achieved by all the member states but one, which is still under progress. Furthermore, the implementation process has not been completed within the same timeline. For example, some countries implemented Art. 13a requirements by 2011, while some countries needed an additional time period to complete the process by 2012, 2013 and 2014.

If countries kept their specificities and regulation prerogatives, Art. 13a definitively helped to harmonize the provider and member states general approach regarding incident reporting.

[10] Directive 2009/140/EC, Article 6

Figure 26: The use of ENISA's technical guidelines by NRAs



However, if the NRAs do refer to the ENISA technical guidelines, reports and studies, most of them use those documents as an inspiration or guidance when the European regulations or domestic laws are not clear enough (on average **30% of the surveyed NRAs use most or all of ENISA's technical guidelines on incident reporting and on security measures in their work, and *40% of the NRAs use ENISA's technical guidelines on incident reporting and on threats and assets as a source of inspiration in their work***). Nevertheless, ***ENISA's technical guidelines are the most important source of harmonization***, given the fact that the Directive does not provide sufficient level of details regarding the scope and thresholds for the incident reporting process, and also lack of definition of what to consider as an asset.

On the other hand, the frequent meeting groups held by ENISA enabled NRAs to share good practices, experiences and advices among themselves, resulting in a trend for harmonization of the practices within the member states. This harmonization is driven indirectly but does not reach every country.

7.1.2. Different approaches in implementing Art. 13a requirements

Most of the countries held a public consultation, according to Article 6 of the Directive 2009/140/EC, before adopting the new regulations; the NRAs as regulatory authorities are free to take the results of the consultation into consideration or to follow their own prerogatives. Therefore, the levels of input from the providers are different from one country to another and impact more or less the domestic legislation.

Furthermore, if the majority of the countries benefit from a second level legislation, some countries do not have such legal framework and are keener in interpreting the Directive and refer to the guidelines than countries which have such level of regulation. ENISA's technical guidelines remain in each situation the main point of information, although countries did not implement Art. 13a through the same level of regulation and legal means.

In most cases, countries with a second level legislation are the most advanced countries with regards to their legal framework and good practices, resulting in different level of efforts required in comparison with countries that have a very young or immature legal framework. Given that some countries had already a more mature legal framework in place and a NRA issuing supportive guidelines, there were only limited efforts to be provided for the implementation of Art. 13a requirements.

Consequently, as the ways and means used to implement Art. 13a requirements differ from one country to another, the thresholds for incidents reporting defined and implemented in the countries differ. First some NRAs set up their thresholds based only on ENISA's Technical Guideline on Incident Reporting, while some other countries took in consideration the comments collected during the public consultation to adapt the level of thresholds proposed in the guidelines. Last but not the least, some countries implemented the thresholds based on the guideline but updated them later to better fit the market specificities, sector practices and the need to collect more information.

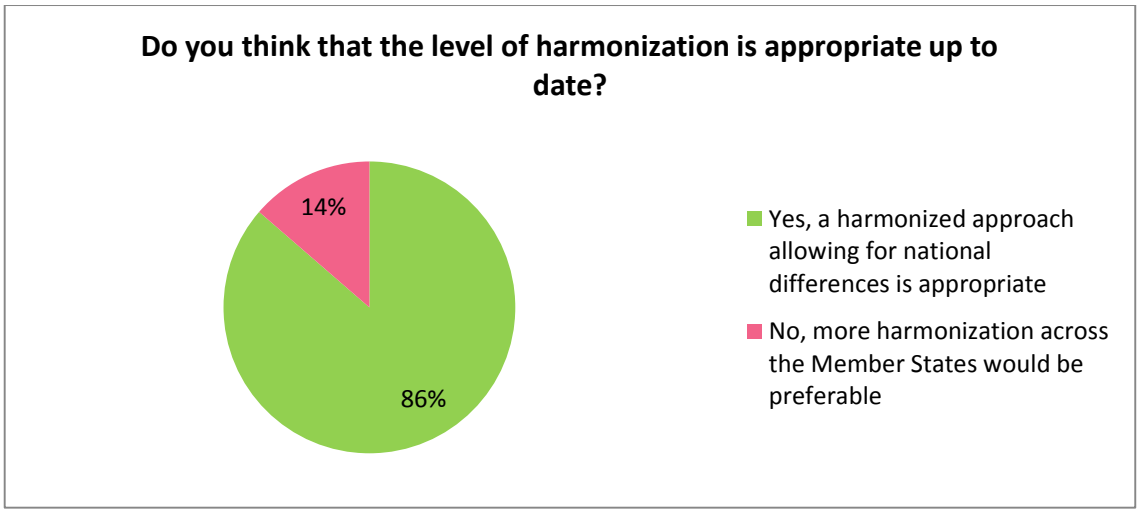
Harmonization of the regulation within the European Union will facilitate the continuous development of a single EU market. Furthermore, diverging regulatory requirements across EU member states may deter and hinder effective competition and thus limit the benefits for some customers in specific countries. Harmonized procedures in terms of incident reporting will also guarantee customers getting access to information related to interruption of service or other types of incidents. On the other hand, harmonized security measures and incident reporting processes will enable cross-border providers to realize economies of scale, as they are already familiar with the incident reporting process, the requirements and then benefit from synergies in the training materials, tool usage, incident management, lessons learnt on passed incident in other countries, etc.

For ENISA, a harmonized approach in the incident reporting is necessary to compare, benchmark and assess the situation within the European Union. Without a common template, indicators and process, the assessment and benchmark of the incidents would be complicated.

7.2. NRAs level of satisfaction regarding harmonization

Taking into account the mandatory level or harmonization imposed by the directive, the necessary level of harmonization induced by ENISA's guidelines and the common specificities noticed at member states level, ***90% of the surveyed NRAs declare that they are satisfied with the level of harmonization within the EU, which sustains also national specificities*** (as shown in Fig. 27).

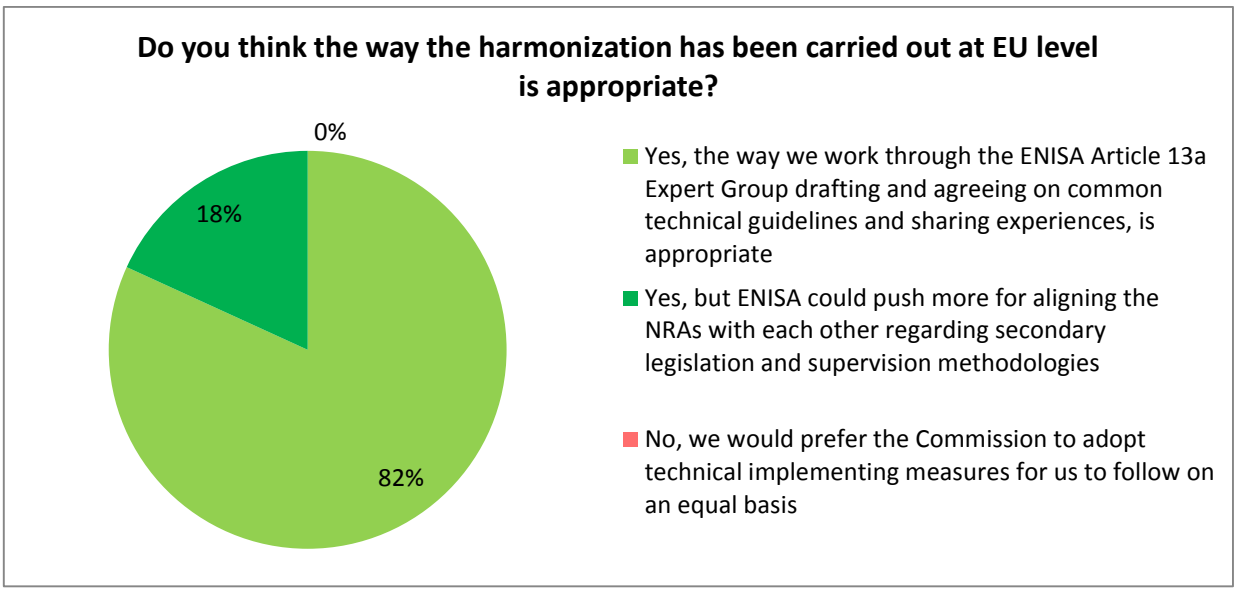
Figure 27: Appropriate level of harmonization



7.3. Areas of further improvement

The interviews and the online survey revealed that the ***82% of the NRAs are currently satisfied with the level of harmonization, and do not think that an improvement is needed for the member states and the telecom market***.

Figure 28: Ways of carrying harmonization



However, 18% of the surveyed NRAs do think that ENISA could improve the current level of alignment among the NRAs regarding the secondary level of legislation and supervision methodology. Also, an enhanced level of alignment would reduce the differences between the countries and enable cross-border service providers to reduce the current faced costs and barriers.

Nonetheless, improving the level of harmonization might be a challenge as the current achieved result is already quite satisfying for ENISA also. Besides the more the harmonization level is raised, the more countries tend to lose their particularities, as created by their internal markets. The risk is that countries start to be reluctant to the implementation of new and stricter regulations.

On the other hand, it may be more difficult for cross border operators to continue to expand and to grow with these differences among the countries, regarding the security measures, the security incident reporting triggering thresholds and the security incident indicators. Complying with all the different legislations requires considerable much effort and could impact the decision to enter the market and compete with the already established national providers.

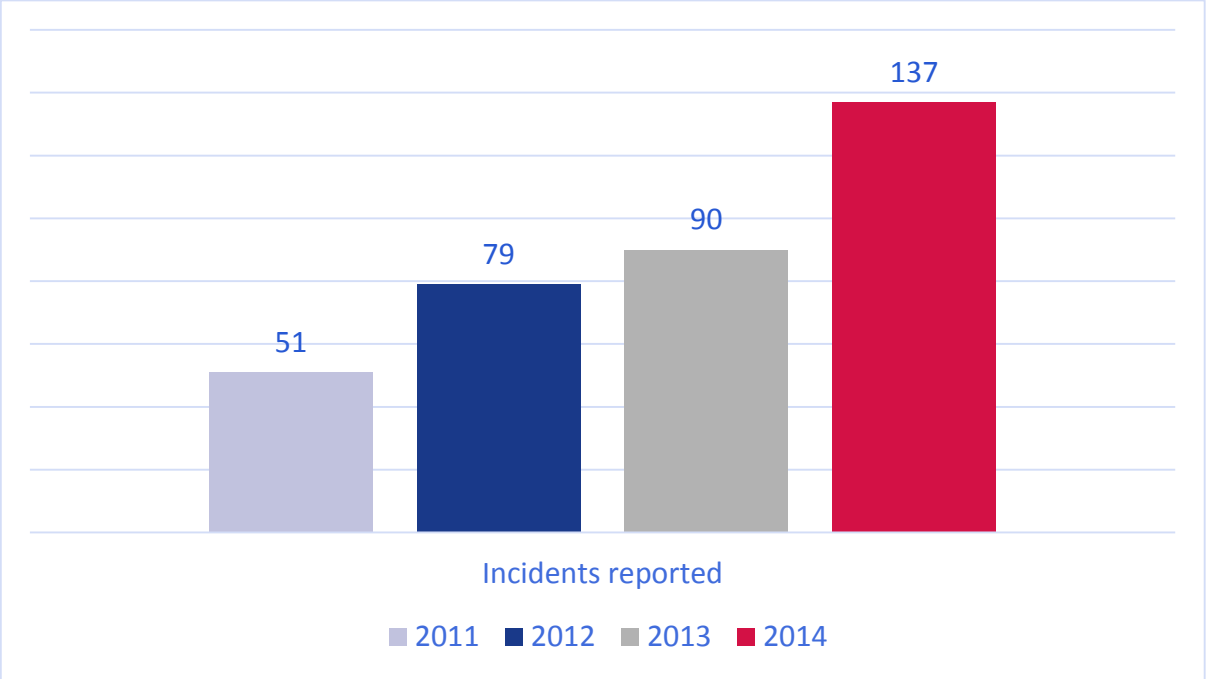
8. Impact evaluation based on reported incidents

8.1. ENISA's annual incident reports

For four years now, ENISA publishes the annual report about significant disruption/outage incidents in the EU electronic communications sector, which are reported to ENISA and the European Commission under Art. 13a of the Framework Directive (2009/140/EC)[11], by the National Regulatory Authorities (NRAs) from all member states. This annual report covers the incidents that occurred in a year and it gives an aggregated analysis about severe outages across the EU, keeping details about individual countries or providers confidential.

As you may notice from the chart below (Fig. 29), the number of incidents reported every year is continuously increasing, showing year by year, the stakeholder's maturity in identifying, collecting and processing more and more incidents. The number of reported incidents has grown along with the number of reporting countries. Only 51 significant incidents in 2011 reported by 11 countries, and 137 incidents reported by 25 countries in 2014.

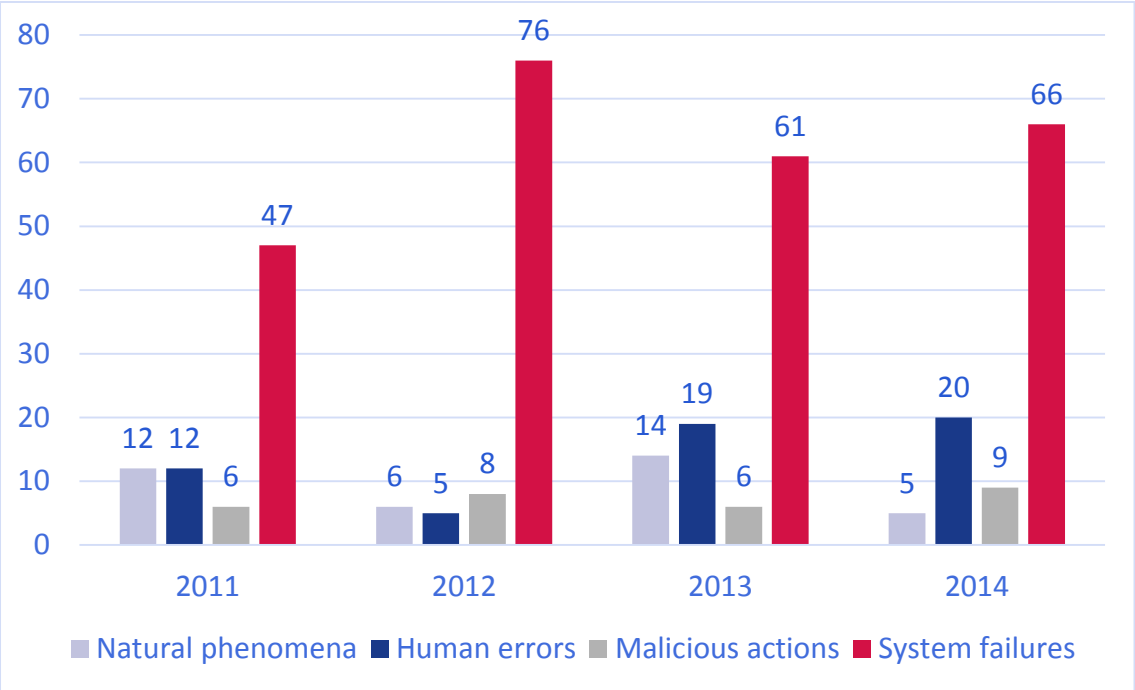
Figure 29: Total incidents reported 2011 - 2014



Looking at the root causes, as shown in the figure below, system failures is one of the main causes that triggers disruptions in Europe. On a closer look, we will notice that a part of the system failures were actually third party failures (16% from all incidents in 2014, 11% in 2013), meaning failures caused by other parties along the supply chain and not the providers that suffered the actual incident. These findings raise other issues regarding causes of disruption incidents around Europe, and how to address them.

[11] Directive 2009/140/EC of the European Parliament and of the Council of 25 November 2009 amending Directives 2002/21/EC on a common regulatory framework for electronic communications networks and services, 2002/19/EC on access to, and interconnection of, electronic communications networks and associated facilities, and 2002/20/EC on the authorisation of electronic communications networks and services

Figure 30: Root causes for reported 2011 - 2014



Supply chain security and responsibility is one of the issues to be taken into consideration in future developments within the area.

8.2. Areas of further improvement

In agreement with the NRAs in the Art. 13a expert group, at the moment incidents affecting only 4 types of services are expected to be reported to ENISA:

- Fixed telephony
- Fixed internet
- Mobile telephony
- Mobile internet

However, the types of services offered by modern telecommunications providers have developed over the years (e.g. messaging services, software based voice services). ***Consequently the range of covered services within ENISA's annual report needs to be updated, by adopting the modern services offered by providers***.

As third party failures represent an important part of reported incidents, signaling different issues within this area, further actions need to be considered in the near future. ***Developing requirements regarding the supply chain security and responsibility could be a further action to be considered by responsible stakeholders.***

9. Key findings and conclusions

Art. 13a gave a new momentum in the telecom industry at European level. By amending the 2002 regulations, the Art. 13a within the Framework Directive of the 2009 Telecom Package, addresses security and resilience issues for the first time in the EU.

As several years have passed since the publication and implementation of the new regulations, an impact evaluation of the new provisions was the proper thing to do. The evaluation has the purpose of assessing the changes in outcome that can directly be attributed to the provision of Art. 13a, and the effects caused by this particular regulation within the Telecom Package.

The compendious evaluation we have done within this project has brought to light some important outcomes that have definitely contributed to increasing the resilience and security of the telecommunications infrastructures in Europe. In a European Union which was highly diversified in terms of security measures, Art. 13a brought a certain amount of uniformity in the approach taken regarding security of telecommunication services, but more importantly contributed to strengthening the European telecom infrastructure's resilience and services availability across the EU. The role of ENISA, especially in the coordination of Art. 13a expert group, was most beneficial as it helped considerably in bringing more harmonization within the implementation process and collaboration among stakeholders (NRAs and providers).

Despite the obvious positive outcomes that have been expressed by the majority of the respondents, there are also some areas of further improvement. Clarifying the scope of art. 13a in order to provide clear information on the types of networks and services that should be covered is one of them, along with reinforcing cross-border collaboration and also other areas that can contribute to a higher degree of resilience of European networks and services.

Overall, Art. 13a has contributed to improving the level of security in the telecommunication sector but in a balanced way as some counties were already in line or even ahead of the requirements and were already experiencing the expected benefits. By opposition, the less advanced countries and providers experimented strong benefits and improvement in their security measures and infrastructures resilience in spite of the costs and efforts provided.

It has been also noted throughout this project that further analyses are needed in order to draw some strong conclusions on next steps that are needed in this area. The short period of time allocated to this project along with the complexity of the area, prevented the project team to further analyze additional details and areas that could also have influenced the result of this evaluation. In this respect, this report will only cover a set of findings that must be further analyzed in order to propose concrete recommendations and next steps to be considered by different types of stakeholders. Main findings of the study are the following, grouped into categories:

The scope of Art. 13a

1. Current lack of precise information within Art. 13a and Telecom Directive, as regards the types of networks and services that should be covered, has led to some differences among national implementations within member states. Although, the level of harmonization seem to be satisfactory, the differences within services covered by member states could represent obstacles in achieving the overall or specific objectives stated within the Telecom Package. Further assessments in this area are needed (more details in section 2.1.2. and Annex I) in order to establish possible next steps.

2. More than half of the respondents (54%) considered that Art. 13a cannot sufficiently and clearly cover by itself security of electronic communications, but together with Art. 4 in the e-Privacy Directive.

Appropriate security measures for providers:

1. The majority (45%) of the respondents (NRAs) considered that Art. 13a has led to stronger security measures within the sector, but further analyses are needed as more than half of them (55%) do not share this opinion, 23% stating "no" and 32% "don't know".
2. Almost 60% of the respondent NRAs are not aware of the areas where the providers have improved the most, in terms of security measures.

Transparency in incident reporting

1. The approach of the providers towards NRAs as regards the implementation of Art. 13a mandatory incident reporting regulations was mostly collaborative. Withal the majority of the respondent NRAs are satisfied with the quality of the information provided by the operators in their incident reports and declared that they are receiving reports as expected.
2. Bringing more clarity to the incident reporting process, by issuing guidelines and additional legislation – 73%, was by far the most effective method of improving transparency.

Learning and improving based on reported incidents

1. NRAs mostly use the incident reporting process as a tool in learning/improvement, but mostly for internal purposes such as compliance, internal statistics and improve regulations. The use of annual incident statistics as an input for evaluating risk at national or sectorial level is not a common approach among NRAs (more details in section 5.1. and 5.3).

Collaboration between the actors

1. The establishment and development of Art. 13a expert group, under ENISA coordination, turned out to be a successful and helpful experience (more details in section 6.3.), as appreciated by 80% of the respondents. The operation and development of the group should definitely be continued, under ENISA's coordination.
2. Bi-directional communication with the population in the incident reporting process is poorly addressed by both NRAs and providers. Further analyses should be carried in order to determine the necessity of developing such processes (more details in section 4.3.).
3. The amount of resource employed by NRAs in the cross-border collaboration area appears to be low (more details in section 6.3.).

Harmonization of practices within the EU

1. Over 80% of the surveyed NRAs declare that they are satisfied with the current level of harmonization within the EU, which sustains also national specificities, and do not think that an improvement is needed in present.
2. ENISA's work, together with Art. 13a expert group, in the area of guidelines and good practices, was considered useful by up to 70% of the respondent NRAs, as it supported the achievement of a mature level of harmonization.

Impact evaluation based on reported incidents

1. More and more reported incidents (at ENISA level) are caused by third party failures (more details in section 8.2.), meaning they are caused by parties out of provider's direct control, but within the provider's supply chain.

2. The main root cause for incidents at EU level in 2014 and years before, is “system failures”. Further assessment needs to be done in this area, in order to identify more detailed causes and security measures that can be adopted.

Annex A: Network and services covered by national implementations of Art. 13a

Nr.	Flag	Country	NETWORKS						SERVICES												INTERNET RELATED									CI
			Cable terrestrial	Cable aerial	Submarine cable	Fiber-optics	Radio (terrestrial)	Satellite	Fixed Telephony	Fixed internet	Electricity cable systems	Mobile internet	Mobile telephony	SMS	MMS	Satellite services	International roaming	Voice mail	RADIO broadcasting	TV broadcasting	Cable television networks	IXPs	ccTLDs	IPTV	VoD	Public WIFI	Web based voice services	Web-messaging services	VoIP	Public email services	Critical Infrastructure
1		Finland	♦	♦	♦	♦	♦	♦	♦	♦	♦	♦	♦	♦	♦	♦	♦	♦	♦	♦	♦	♦		♦		♦		♦	♦	♦	
2		Slovak republic	♦	♦		♦	♦	♦	♦	♦	♦	♦	♦	♦	♦	♦	♦	♦			♦	♦	♦	♦	♦			♦	♦	♦		
3		Estonia	♦	♦	♦	♦	♦	♦	♦	♦	♦	♦	♦	♦	♦	♦	♦	♦	♦	♦	♦	♦									♦
4		Hungary	♦	♦		♦	♦	♦	♦	♦	♦	♦	♦	♦	♦	♦	♦	♦			♦			♦		♦			♦	♦		
5		Lithuania	♦	♦	♦	♦	♦	♦	♦	♦		♦	♦	♦	♦		♦	♦		♦	♦		♦	♦			♦			♦		
6		Portugal	♦	♦	♦	♦	♦	♦	♦	♦	♦	♦	♦	♦	♦	♦	♦	♦	♦	♦	♦										♦
7		Czech Republic	♦	♦		♦	♦	♦	♦	♦	♦	♦	♦	♦	♦	♦	♦	♦	♦	♦	♦								♦		♦
8		Sweden	♦	♦	♦	♦	♦	♦	♦	♦		♦	♦	♦	♦		♦					♦				♦			♦	♦	♦
9		UK	♦	♦	♦	♦	♦	♦	♦	♦	♦	♦	♦	♦	♦	♦	♦	♦		♦	♦										
10		Romania	♦	♦	♦	♦	♦	♦	♦	♦	♦	♦	♦	♦	♦	♦					♦			♦							
11		Belgium	♦	♦	♦	♦	♦	♦	♦	♦		♦	♦	♦	♦		♦	♦											♦		
12		Croatia	♦	♦	♦	♦	♦	♦	♦	♦	♦	♦	♦	♦	♦							♦		♦							
13		Cyprus	♦	♦	♦	♦	♦	♦	♦	♦		♦	♦	♦	♦			♦				♦							♦		
14		Germany	♦	♦	♦	♦	♦	♦	♦	♦	♦	♦	♦	♦	♦	♦	♦														
15		Slovenia	♦	♦		♦			♦	♦		♦	♦	♦	♦						♦			♦	♦				♦		
16		Norway	♦	♦	♦	♦			♦	♦		♦	♦	♦		♦						♦	♦								
17		Switzerland	♦	♦	♦	♦		♦	♦	♦		♦	♦						♦	♦	♦										
18		Ireland	♦	♦	♦	♦	♦		♦	♦		♦	♦	♦			♦														
19		Poland	♦	♦		♦	♦		♦	♦		♦	♦	♦	♦						♦										
20		Greece	♦	♦	♦	♦	♦	♦	♦	♦		♦	♦																		
21		Malta	♦	♦	♦	♦			♦	♦		♦	♦	♦			♦														
22		Austria	♦	♦		♦	♦	♦	♦	♦		♦	♦																		
23		Luxembourg	♦	♦		♦	♦	♦	♦	♦		♦	♦																		
24		Bulgaria	♦	♦		♦	♦		♦	♦		♦	♦																		

* Countries that have responded within the given time period.

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 Vass. Sofias & Meg. Alexandrou
Marousi 151 24, Athens, Greece

Catalogue Number TP-04-15-873-EN-N

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

ISBN: 978-92-9204-149-6
DOI: 10.2824/491369