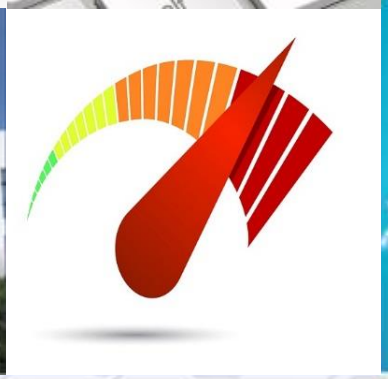




Security incidents indicators- measuring the impact of incidents affecting electronic communications

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 (Alexandre Minarelli, Brice Lecoustey, George Tountas, Cedrine Herbin, and Swathi Selvaraj) and based on the input of the following experts: Vassilios Stathopoulos (ADAE), Manuel Barros (ANACOM), Costin Masiliev (ANCOM), Heidi Kivekäs (FICORA), Vasiliki Mylona and Antonis Antoniades (OCECPR), Karin Lodin (PTS), Ulrich Latzenhofer (RTR), Pedro Gomes Silva and Pedro Gaspar Moreira (NOS).

ISBN: 978-92-9204-156-4; DOI: 10.2824/887699

Table of Contents

Executive Summary

Telecommunication is an industry that can be considered as the backbone of modern economies. Economic development is strongly related to the existence and well-functioning of the telecommunication networks. Telecommunications demands advanced technologies and processes, playing a vital yet growing role in the European Union (EU). Current developments have determined some changes within customer preferences over the years, changes that have made it crucial for telecommunications operators to illustrate transparency, customer innovation and bring new services to the market. At the same time, operators have to maintain high security and availability standards. Security incidents affecting this sector can have detrimental effects that can manifest themselves in a number of ways.

Measuring the impact of incidents has become one of the toughest challenges nowadays, given the multitude of factors/indicators that must be taken into consideration. To address this issue, indicators are used, accompanied by thresholds, to assess the impact of incidents. This approach allows evaluation of incidents from various perspectives, such as business perspective, compliance with regulations, root causes, impact on customers etc. Incidents can vary in nature, and this report tries to include as many indicators as possible, so that as many types of incidents as possible are covered.

The overall purpose of the document is to provide guidelines to national regulatory authorities (NRAs) and telecommunications providers (providers) within EU member states, to assist them in the process of measuring the impact of security incidents affecting electronic communication services.

This report comes as a practical approach, and contains the view of both NRAs and providers within EU, on real indicators used for measuring significance of incidents affecting telecommunication networks and services. Therefore, interested stakeholders have at their disposal a catalogue of indicators to be used to tailor impact assessment and design the corresponding solutions.

As the survey performed had also the objective of analysing the approached taken by NRAs and providers in defining indicators and significance, the results indicated that while there are some discrepancies between NRAs and providers in terms of why they measure security incidents, and for what purpose they use certain indicators over others, it is still plausible to state that the ***approaches taken and indicators used by both parties are more similar than they are different***, as more than half of the respondents have stated this. Further developments regarding harmonisations of the approaches taken are still needed but overall the situation is running smoothly, the processes are in place, and the reporting of significant incidents is being done at national and EU level. From the study, it was realized that ***approaches taken by NRAs and providers varied depending on certain country-level factors***. Some were much more mature than others. Due to several advantageous circumstances, some NRAs experienced strong cooperation with their providers when it came to implementing the necessary changes.

Having said this, it is advised that making use of a standardized approach among NRAs and providers can help derive more precise results in the incident reporting process. So, along with the list of indicators to use, the key recommendation from the study is that NRAs and providers should further increase the level of harmonisations in the approach taken to measure the impact of security incidents. Studying the approaches taken, including the benefits and challenges of each measurement method led to gaining an insight of the most common approaches used to assess security incidents. The list below summarises the main classes of indicators, as identified during the study:

- User/connection related indicators

- Time/duration related indicators
- Geographic area related indicators
- Indicators related to infrastructure and services affected
- Root cause dependent indicators
- Economic impact related indicators
- Indicators related to cyberattacks
- Impact on confidentiality, availability and integrity

ENISA recommends the extensive use of this list of indicators, in related activities carried out by both NRAs and telecommunications providers within EU and abroad. Measuring the impact of security incidents, is a rather difficult process and the use of the current study can bring additional clarity.

1. Introduction

1.1 Background

Advances in electronic communication services have resulted in many changes, altering, reshaping and even modernizing the way in which people communicate with each other. Some industries are strongly revolutionized, especially those that deal with human senses, including entertainment, healthcare, education and advertising. Electronic communications services warrant a smooth transmission of data in this strongly interconnected world by providing the infrastructure for other business services to run. Electronic communication services also play a significant role in national security, emergency response and even in the economic well-being of a country. As a result, an outage in any one of these areas can result in severe consequences. For example, impact could range from strong customer dissatisfaction to impairing security and public safety and leading to economic repercussions.

In that context, measuring the impact of security incidents affecting telecommunications providers has become a necessity in nowadays interconnected digital market. The European Commission (EC) has made significant steps in this direction, with the 2009 Telecom Package, that included Art. 13a, a regulation enforcing mandatory incident reporting for security incidents in the telecommunication networks. The purpose of Article 13a of the Directive 2009/140 EC is to ensure the security and integrity of electronic communication networks and services in the European Union, mostly by preventing disruption of networks and services among others. As only significant incidents had to be reported, meaning the ones with greater impact, member states have struggled for some time to define “significant”.

To be able to identify significant incidents, providers and NRAS need to know how to measure their impact. Measuring the impact of security incidents is not always easy as there are several different variables which play a role. Furthermore, the impact of an incident can be evaluated from different perspectives, making the process rather complicated.

By studying the indicators used to measure the impact of security incidents, especially the ones affecting the availability of the service (disruptions), this report aims at collecting good practices and expertise in order to share it across, encourage the exchange of these practices between member states and improve harmonisation of the existing approaches. Evaluating the direct and indirect impact of security related incidents can be crucial as a basis for investment in recovery strategies as well as investment in prevention and mitigation strategies.

1.2 Scope of the document

This report aims to provide guidelines to NRAs and providers, to assist them in the process of measuring the impact of security incidents affecting the availability of electronic communication services. Therefore, interested stakeholders, especially telecommunications providers, will have at their disposal a catalogue of indicators to be used to tailor impact assessment and design the corresponding solutions.

The goal of this study is to help policy makers at EU and member states level, along with the European Commission and ENISA, develop better policies in order to further increase the security and resilience of the electronic communications sector.

1.3 Target audience

Electronic communications providers (named providers as for the rest of the document), professionals in the telecommunications industry, along with national regulatory agencies (NRAs) within the EU are the main targets of this report. The report is also addressed to experts within the policy making area, such as European Commission.

1.4 Methodology

The study was carried out in 3 phases. Firstly, a desktop research was performed to review approaches taken by different member states and non-EU countries.

Next, a range of NRAs and service providers were identified and selected in order to complete an online survey. A questionnaire was designed and communicated with those who agreed to take part.

Finally, telephone interviews were scheduled and conducted. Interview guides were sent to the selected participants prior to the interview in order to foster meaningful conversations and gather useful insights.

Conclusions in this report are driven from the desktop research, interviews and the results of the online survey. A total of 9 NRAs and 4 providers were reached for the interviews, whereas 13 NRAs and 23 providers responded to the online survey.

2. Varying approaches on measuring the impact of incidents

A milestone in measuring the significance of incidents within the telecommunications sector in the EU was set up along with the adoption of the Framework Directive (Directive 2009/140 EC) within the 2009 Telecom Package, which included Art. 13a.

Art. 13a aims at ensuring the security and integrity of electronic communication networks and services in the EU. 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.

When article 13a was initially published, NRAs and providers were required to make some changes to their internal procedures so as to comply with its requirements. This was especially true with regards to how security incidents were measured and reported.

To have a well-established incident reporting method, NRAs and providers need to know how to effectively measure the impact of a security incident. However, measuring the impact of a security incident can often be a lengthy and complex process. In addition to this, there are some differences in the approach taken between member states as well as the approach taken among NRAs and service providers.

2.1 Approaches taken by member states (NRAs)

The approaches taken by NRAs can be classified into two main categories.

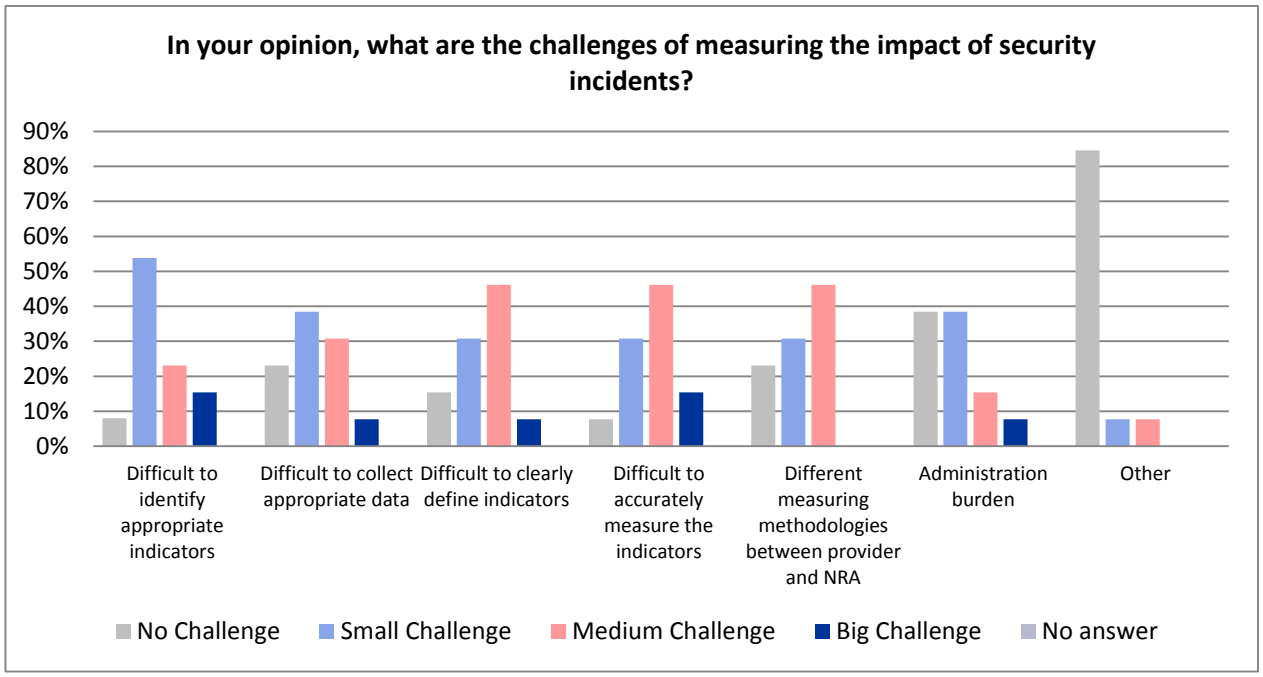
The first category is one wherein NRAs have taken a reasonably collaborative approach with the providers in adopting indicators to measure security incidents. In these cases, there has been a lot of communication between the various groups involved. Furthermore, the indicators were defined and agreed upon through consultation between the NRAs and providers.

The second approach however, is somewhat that of directly implementing the provisions of the directive. Providers did not have much to say in the incident reporting process and instead had to comply with the requirements of their NRAs. Differences in the approach taken can primarily be attributed to country particularities. Regardless of whether the approach was more or less collaborative, NRAs and providers were encouraged to use an additional second-level regulations along with ENISA's technical guidelines. However, this was not the approach taken by all member states. The reason for which additional measures exists in some cases (but not in all), is related to the fact that the Telecom Package, does not explicitly mention the indicators or reporting procedures that member states must follow.

2.1.1 Challenges

Since providers can vary in size, popularity but also in terms of their maturity levels, NRAs can find it difficult to agree on a measurement method, which is applicable to all. Although mentioned as a medium challenge, ***providers and NRAs are using different measurement methodologies*** (stated by 45% of the respondents from the survey). A difference in the approach taken to measure security incidents can potentially impact the results of the incident reporting process, and may not always represent a true and fair view of the current situation in the country.

Figure 1: Challenges of measuring security incidents - NRAs



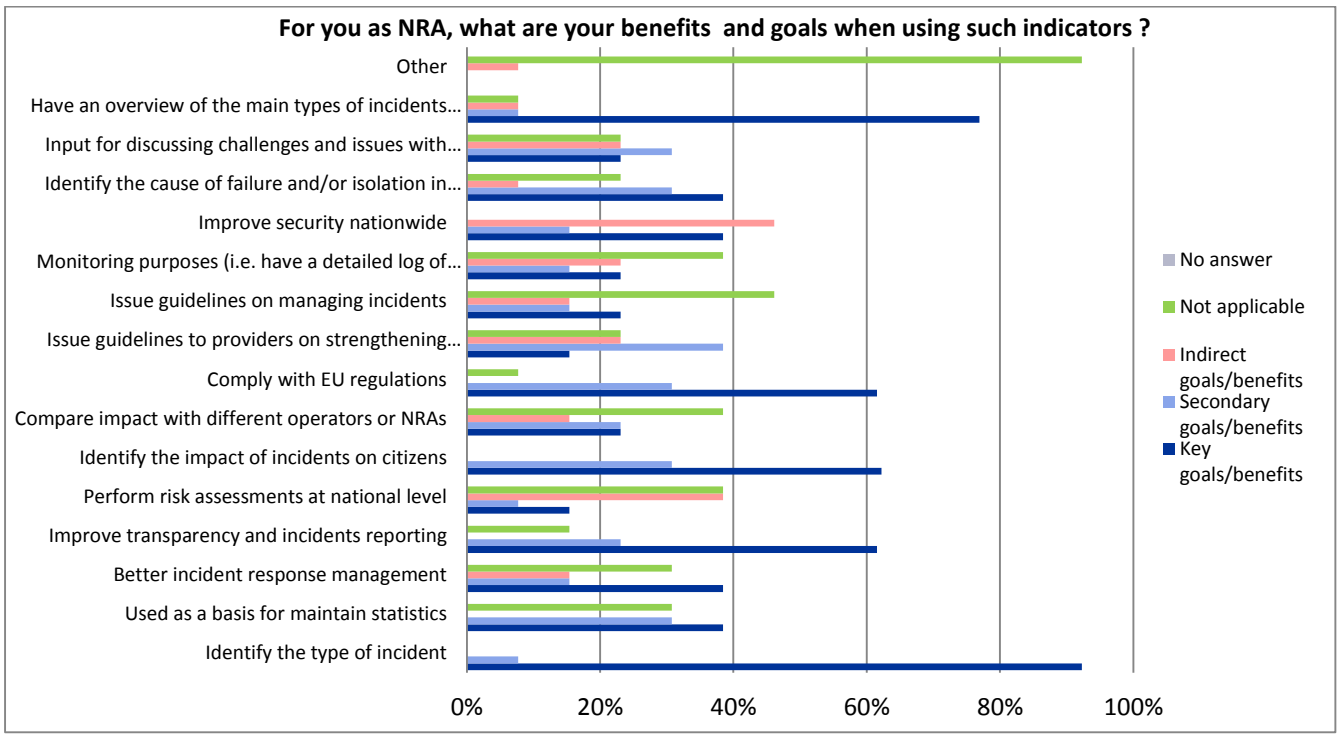
That being said, ***identifying appropriate indicators and accurately measuring them,*** is in fact most problematic (38% of the NRAs expressed this to be their medium to big challenge). Although only listed as a medium challenge, NRAs also experienced difficulty in clearly ***defining an indicator*** (46% responded that this was the case). The fact that NRAs experienced confusion in defining, identifying and accurately measuring security incident indicators, can, for the most part, be attributed to Article 13a's relative ambiguity. Article 13a asks NRAs and providers to take appropriate steps to guarantee the integrity of networks, but does not specify what is meant by "appropriate steps" nor does it specify on what basis "integrity" is defined. The directive also lacks necessary details needed for defining "significance" of incidents. To provide more clarity, the Art. 13a Expert Group, coordinated by ENISA, has been established in order to help by issuing good practices on these matters. ***Accurately measuring the indicators*** has been mentioned as big to medium challenge by half of the NRA respondents.

2.1.2 Goals and benefits

Identifying the type of incident including the reason behind it (i.e. if the incident was accidental or deliberate) and identifying the target of the incident, such as whether the incident affected customers or networks etc. is seen as a key goal and benefit among NRAs (92% of respondents replied this to be the case). This is in line with expectations as NRAs ultimately aim to protect citizens. Therefore, measuring the impact an incident has on the population is necessary. Furthermore, accurately measuring security incidents enables NRAs to have a better overview of the "as-is" situation in their country. By identifying the types of incidents that can occur at a national level, NRAs are also more likely to put in place the right kind of risk assessment and security measures (77% agreed). NRAs were also keen on ***understanding how security incidents impacted their citizens***, with 62% replying that this was another one of their main goals/benefits. 62% of survey respondents also stated that they were measuring the impact of security incidents so as to ***comply with EU regulations*** (which was seen as a key goal/benefit).

An additional benefit to measuring the impact of a security incident, from the perspective of the NRAs is that the information can be used as a ***basis for maintaining statistics*** (as expressed by 38% of the respondents).

Figure 2: Goals and benefits of measuring security incidents – NRAs



Issuing guidelines to providers on strengthening infrastructures and using the measurement methodologies as an input for discussing challenges can be of benefit. Furthermore, it can also aid in discussing issues with other providers and other sectors. However, both these indicators were seen as more of a secondary objective rather than a primary one (38% for strengthening infrastructures and 31% for discussing challenges).

In terms of the indirect goals, analysing indicators, resulted in the NRAs' ability to perform ***better risk assessment procedures at a national level***, and to ***increase the level of security nationwide*** (38% said that it helped perform risk assessments at national level and 46% agreed that it improved security nationwide).

2.2 Approaches taken by e-communications providers

The approaches taken by providers can be directly correlated with their level of maturity in terms of country legislations and practices (which can be seen when benchmarking one member state with another). Approaches also vary among providers in terms of the providers' business maturity, as well as their level of maturity as regards the relationship and collaboration with their respective NRAs.

For providers who were very mature, the reporting process, including the indicators used to measure security incidents were incorporated to a relatively good standard in their day-to-day practices.

Providers with an average level of maturity, including smaller providers were either eager to improve their internal processes and security measures, identifying it as an opportunity to improve or were reluctant to do so due to additional effort and resources needed. These providers were either using

fewer or different indicators than the ones defined in the guidelines. In order to comply with the regulations, small providers had to implement these security measures from scratch.

2.2.1 Advantages

Benefits in the approach taken by providers were quite similar to the benefits experienced by the NRAs. Having a more transparent affiliation with the NRA, wherein there existed good communication and transfer of information and knowledge between the two, meant that the transition process to the new requirements of Article 13a, was a lot more easy than when compared to provider's whose relationship was not so strong. Furthermore, providers were able to better understand the importance of Article 13a and how the former could positively benefit them. Effectively using the guidelines meant that providers experienced less implementation costs and efforts taken to comply with the regulations. This was especially true for the bigger telecommunications providers, as well as those who had greater investment capacities.

As for the smaller players in the industry, although they may not have had the right capital to invest in, or the relevant expertise and skills to do so, the advantage for them is that they have had the opportunity to learn from the methods used by their counterparts, and based on this, adopt some of the leading practices which would be most applicable to them. By doing so, they can also gain a competitive advantage which is core to the nature of their business.

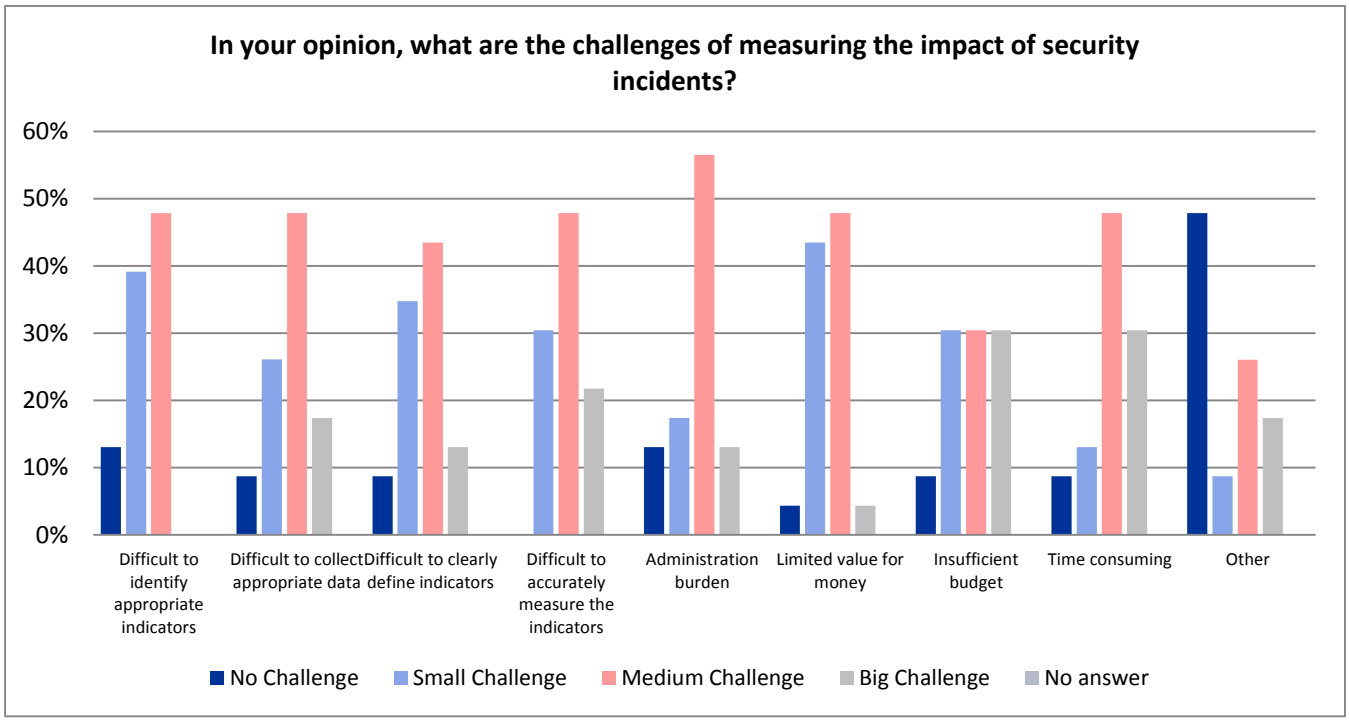
2.2.2 Challenges

Unsurprisingly, providers felt that measuring the impact of a security incident was a process that was not only ***time consuming*** but also, ***expensive*** (30% said that it was time consuming and 30% mentioned that they had insufficient budget). Providers expressed more in detail, their concerns during the interviews. For example in situations where the NRA had implemented a second level of regulation, providers were asked to issue two incident reports, instead of just one. They were asked to issue the first report within 24 hours following the identification of an incident. The second report was requested to be issued within two weeks following the incident fix. Therefore, this situation led to some ***administrative burdens*** and delay in resolving the incident (13% stated that this was a big challenge and 57% agreed that it was a medium one). Similarly, it was sometimes the case that the same incident was measured twice. The incident was measured once by the provider for internal purposes and was later measured again for the purpose of reporting to the NRA. Given that there are usually limited resources which are usually supposed to be dedicated to resolving the issue; providers felt in such situations that they are "wasting" time in writing reports, and measuring the impact. The former could denote that more transparency and cooperation within the indicators area is required between providers and NRAs.

57%

Of providers felt that measuring security incidents was an Administrative burden

Figure 3: Challenges of measuring security incidents - Providers



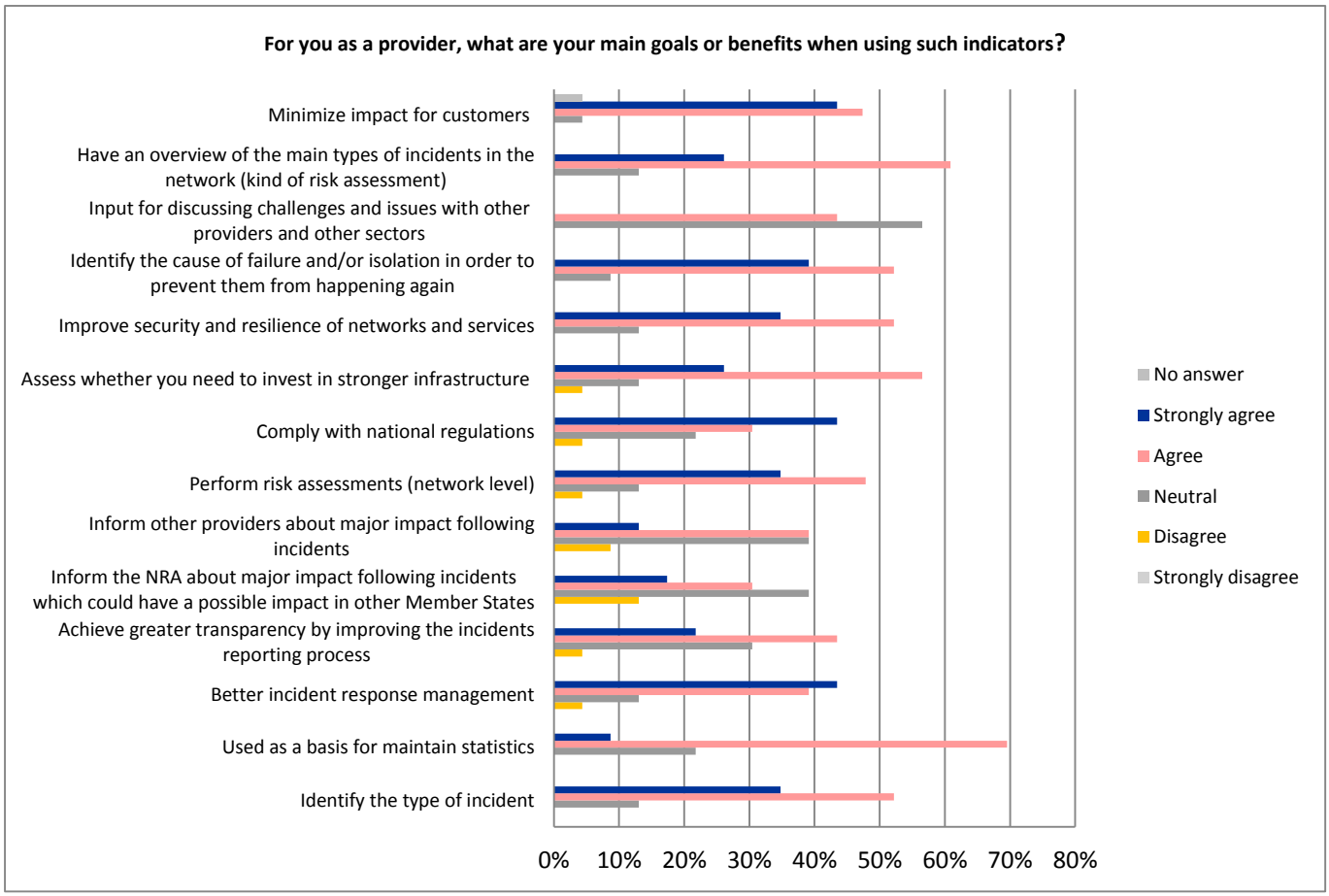
Furthermore, ***measuring security incident indicators also resulted in limited value for money*** (48% of the providers responded that this was a big challenge whereas 43% stated that the challenge was a small one).

Regardless of maturity levels however, and similar to the NRAs***, all providers experienced some level of difficulty when it came to identifying, collecting the relevant data, and accurately measuring security incident indicators***.

2.2.3 Goals and benefits

Complying with national regulations is one of the main objectives of measuring security indicators (43% of the respondents agreed). Additionally, goals and benefits in the assessment approach means that providers can in consequence also be able to ***better identify incidents*** and to establish a more rigorous incident response mechanism (35% strongly felt that this improved identification of security incidents, and 43% replied that this meant ensuring a more rigorous incident response system)

Figure 4: Goals and benefits for measuring security indicators - Providers



Another benefit from the viewpoint of the provider is that measuring security incident indicators can enable them to use the information collected, as a ***basis for maintaining statistics*** (70% agreed). Using the indicators also means that providers can identify repeated incidents and thus, put in place certain measures so as to reduce the impact on their customers (52% believed this to be the case).

What is interesting to note is ***that informing other providers of the major impacts following an incident was neither a benefit nor a goal*** (39% felt this way). At the same time, input for discussing challenges and issues with other providers and other sectors also appeared to be neutral as well. From this information, it can be assumed that providers were not so willing to share or discuss of the security incidents among each other or within different sectors.

In addition to this, although complying with national regulations is one of the main aims, many providers expressed that their goals were not always in line with that of their NRAs. Unlike the NRAs, whose ultimate purpose is to protect citizens, providers are much more business oriented. Providers are constantly seeking new ways to grow their business and increase revenue and are also trying to position themselves strategically in the market. Their objective is to deliver a positive experience for their customers. Having said this, being customer centric meant that providers were using security indicators (i.e. root cause of an incident, number of users affected, time duration etc.) to design effective security mechanisms to not lose reputation among the public. The measures were also being used to assess damage of the incidents and to also identify revenue for their business.

2.3 Approaches taken by non EU states

Researching the methodologies used to assess security incident indicators outside of the EU, can help assist NRAs and providers in refining their existing procedures to a further extent. The former can provide useful insights which can eventually be applied, and also leveraged upon among the different members states. A lot of information is available on threats and security issues associated with "information security" in particular. This is especially true for countries such as the United States and India. As a principle, it was noted that three aspects of information security are considered: "availability", "integrity" and "confidentiality" of information. While availability is the main area of focus for Article 13a, other sectors have directed their attention towards "confidentiality" instead.

For example, the Federal Communications Commission (FCC) in the United States measures the impact of security incidents using several key indicators. Furthermore, they have also established an incident reporting process which provides guidelines to telecom operators in the United States on what to report and when to notify of incidents. To facilitate the incident reporting process, the FCC has also set threshold values. Telecommunications operators are requested to report on the following; the date and time of onset of the outage; a brief description of the problem; service effects and the geographic area affected by the outage. A distinction is also made on "initial" and "final" reports meaning that similar to Article 13a, providers report the same incident more than once (once initially and after it is resolved). Outage reporting requirements are categorized based on the service that is affected. Services include cable services, IXC[1] tandem facilities, outages to satellite communications, signaling system, wireless services and interconnected VOIP service providers. For more information, readers can refer to the ecfr.gov website.

To achieve efficiency and encourage the public to communicate the incidents, the FCC has issued key information via their online website. They have also established a page which is dedicated to providing information to users including the FCC phone directory, organizational charts, the FCC's offices and emergency contact information.

In India, the Department of Information Technology (DIT) has defined Service Level Indicators for their SWAN operation (State Wide Area Network). Indicators for SWAN are requested to be considered by the respective states within India for incorporation in their Service Level Agreements with operators. Thresholds values are defined which help in measuring the impact of an incident. In addition to this, emphasis is also placed on the time duration of an incident (initial response time and issue resolution time). To assess severity of an impact, the DIT also recommends operators to measure the availability and extent of outage experienced for the following: internet availability, firewall outage, IDS outage and Denial of Service. This is different to the existing indicators used at EU level and assessing the impact of incidents through this viewpoint can allow member states to obtain technical insight on the cause of an incident or vulnerabilities surrounding existing infrastructures and services. For more information on the thresholds including how they are used among different states in India and on the specificities of the technical information, such as bandwidth and availability etc., readers can access this website.

The indicators used to measure security incidents in both these situations, can be related to the ones transposed in the European Union, linked to Article 13a.

[1] Interexchange Carrier or long-distance telephone company.

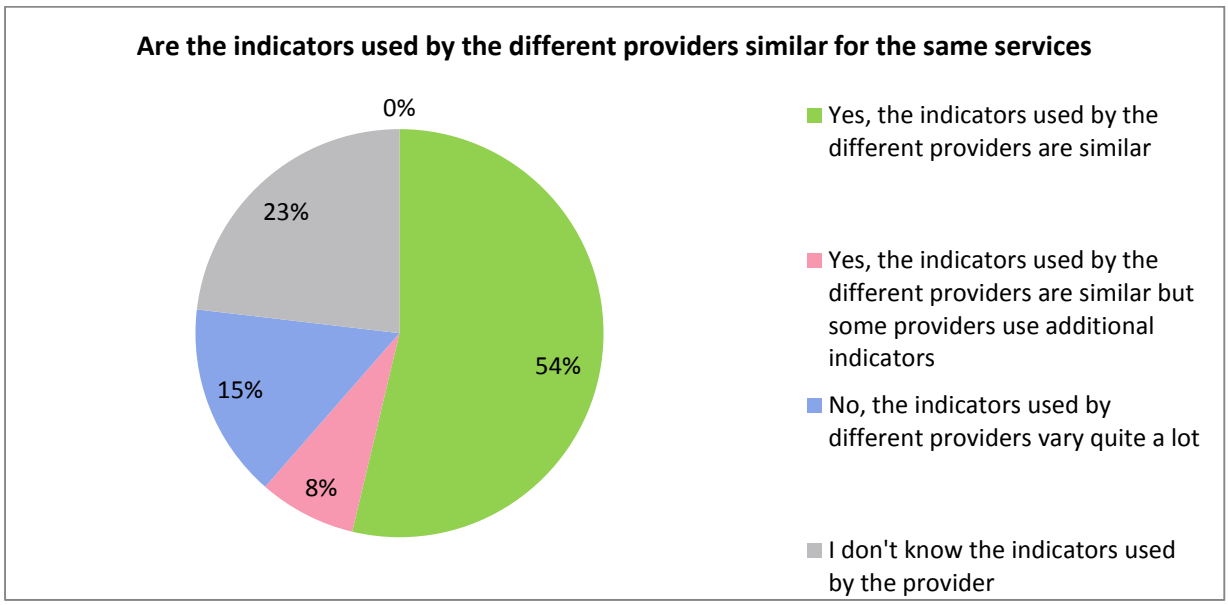
2.4 Harmonizing NRAs & Providers

To remain a key player in the market, providers should know how to attract and retain customers. For this, they need to be able to provide the best services to their customers. One way of achieving this, is to continuously monitor the functionality of infrastructures and services. In contrast, the approach taken by the NRAs is not necessarily going to be the same (NRAs do not have the same commercial objective as that of a provider). NRAs are concerned with protecting their citizens and on improving security within the country.

Regardless of the role and purpose of the NRA and provider, the bottom line is the same. Both need to take appropriate measures to guarantee security, but the main purpose of why they offer security differs from one to the other.

Sometimes it appears to be difficult to know of the internal regulations used by operators. Furthermore, it is difficult to say if these regulations are in place in an attempt to comply with country level regulations or if they already existed beforehand.
Other than the incidents that are reported to the NRA (as part of the reporting process), several NRAs did not know of the additional indicators that providers were using (23% stated this to be the case).

Figure 5: Similarity of indicators among NRAs and providers – NRAs perspective



The same was also conveyed more in detail during the interviews, wherein NRAs described that even if they had a good overview of the security measures taken by the big operators within the country, access to relevant information on the smaller players was very much limited.

In situations where the NRA did have an indication of the measurement methods however, it was found that providers were using similar indicators for the same kind of services (54% of the NRAs agreed). Nevertheless, there were some notes by providers, stating that although the indicators used may be the same, in some cases the measurement method is not the same. For instance, when measuring affected users on a fixed voice service, the value of the indicator will differ if the NRA uses provisioned customers and the provider uses statistic usage curves.

In one example though, the NRA argued the opposite. It explained how 5 of the largest providers in the country represented 90% of the market in terms of customers, while 500 small providers represented only 10%. Indicators were calculated based on affected customers, geographic area and loss of capacity etc. The smaller providers found it difficult to meet the standards of the reporting process, and felt more comfortable with reporting on loss of capacity only.

54%

Of providers felt that there was a good level of collaboration between them and their NRAs

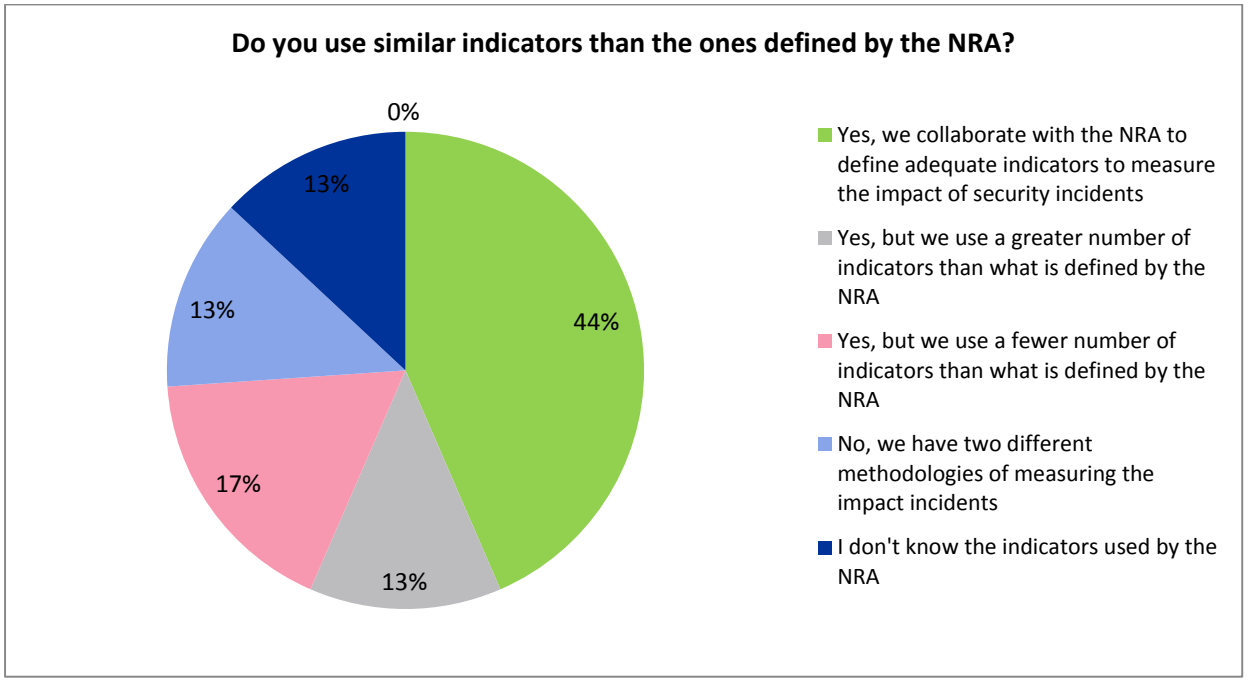
In addition to this, if for example an incident affects a large provider, it would be more likely that the incident is published in the news and/or media. When the incident affects a smaller provider instead, the visibility of that incident is not so apparent, therefore making it much more difficult for the NRAs to come to know of it.

15% of survey respondents mentioned that the indicators used by different providers, varied quite a lot from one provider to another and 8% expressed that the indicators used were similar, but that some providers were using additional indicators. From this, it is reasonable to say that NRAs had differing opinions on the level of harmonization between them and their providers. Some felt that the harmonization levels were good and that there existed a good alignment between the two, whereas others expressed that this level of harmonization could be further improved.

Differing opinions in harmonization levels was also perceived among providers as well. 54% of the respondents from the survey felt that there was a good level of collaboration between them and their NRAs.

That being said, 13% described that they were in fact using a greater number of indicators than what had been defined by their NRAs. As resulted from the response, it's quite normal that a large provider uses more indicators that those requested by the NRA. While the NRA is interested in "major" indicators of impacts on citizens, the provider needs a lot more indicators to help manage the day-to-day operations. Nevertheless, it cannot be assumed that the indicators that the NRA requests are within the indicators already used by the provider.

Figure 6: Similarity of the indicators among NRAs and providers –Provider's perspective



Using fewer indicators as opposed to using more is what essentially can lead to some issues (17% of the providers mentioned that they were using a fewer number of indicators than their NRAs). This often resulted in additional costs and extra effort. For example, providers already had in place certain indicators to fulfil their own objectives and goals (i.e. build good relationships with customers, establish a good reputation in the marketplace, become the leading provider in the industry etc.). However, complying with the requirements of the NRA meant that they had to make some changes to the way in which they measured security incidents. This also included measuring the same type of incident based on a new set of thresholds. A misalignment in the way in each of the indicators were measured sometimes resulted in a difference in opinion between the NRA and the provider and in some cases also had an impact on the relationship between the NRA and the provider.

Furthermore, the "misalignment" most often manifested itself in the incident reporting process. For example, according to the guidelines of 8 of the NRAs interviewed, an incident report should be sent by the provider to the NRA with one hour after identifying an incident. However, the incident is not necessarily resolved within that hour. The time taken to report an incident actually results in a delay in time to resolve the incident. That being said, in the majority of the cases the team who is responsible for reporting the incident to the NRA is also the same team involved in resolving the incident. A lot of effort is required in terms of reporting the incident and additional work is also performed when reporting the same incident for the second time (incident is reported within 1 hour of being identified and then reported again once resolved). While this demands quite a lot of effort from the side of the providers, measuring incidents in this way, actually adds value to the incident reporting process from the viewpoint of the NRAs (NRAs are able to gather more insight on the nature of the incident).

To summarize, irrespective of the differing opinions among NRAs and providers and irrespective of if internal procedures differed based on the type of incident in scope, it was found that NRAs and providers mainly use similar indicators to measure security incidents. There are although slight differences regarding the measurement methods, as reported by some providers.

To reinforce this point, when asked if objectives of the NRA were aligned with the providers objectives, 54% of NRAs from the survey, felt that objectives were "somewhat aligned". In other words, even if protecting end users vs building a good reputation, differed to some extent, the means of achieving the objectives are in actual fact similar (Fig. 7). Only 23% of the survey respondents replied that both NRAs and providers had exactly the same objectives when defining indicators to measure the security incidents, whereas only 8% replied that the objectives were different.

Figure 7: Alignment of the objectives between NRAs and providers– NRA's perspective

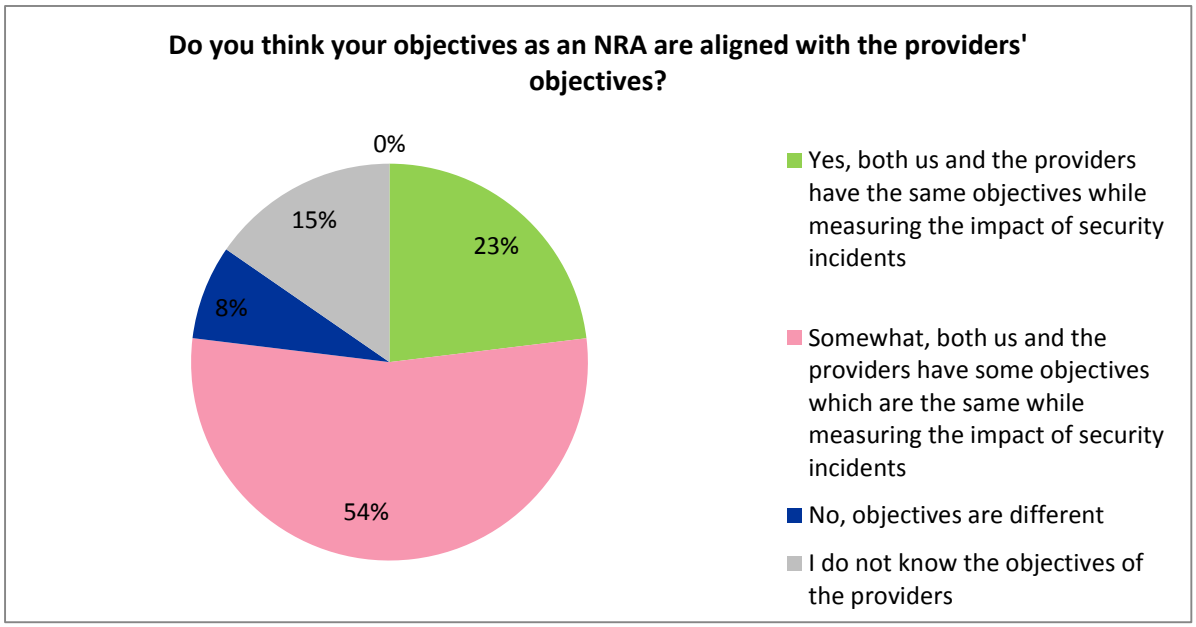
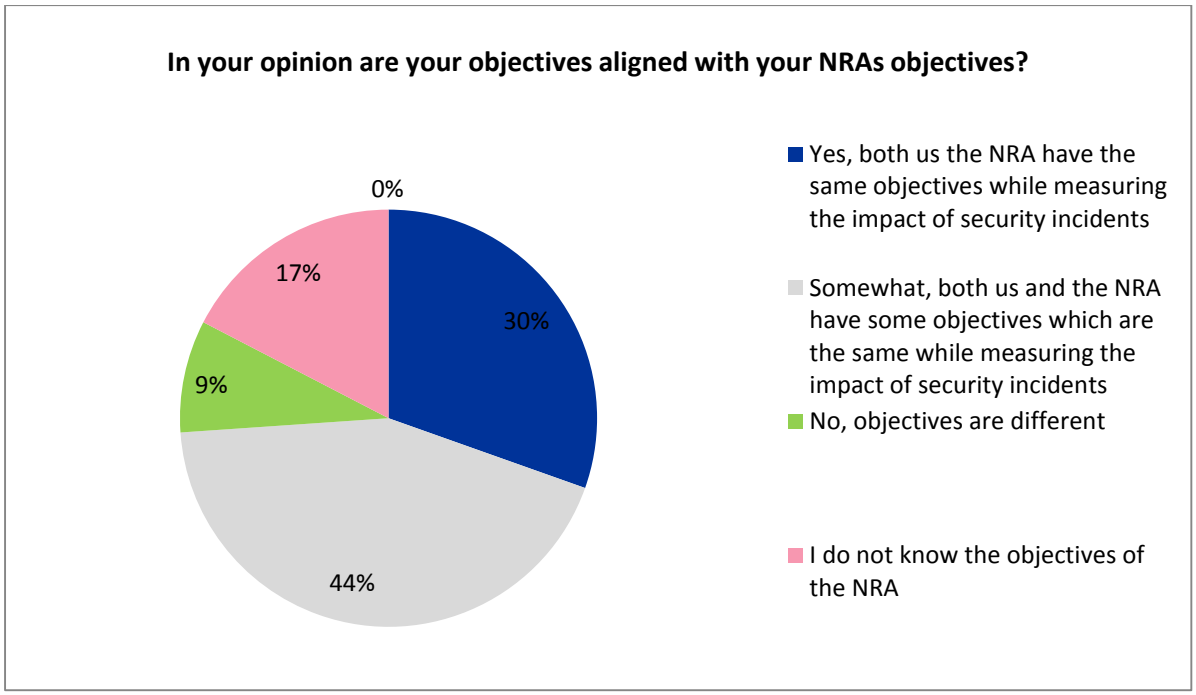


Figure 8: Alignment of the objectives between NRAs and providers – Provider's perspective



The question was also asked to providers, where 44% replied that according to them, their objectives, where somewhat aligned with that of the NRA. To add to this, 30% replied that both they and their NRA had the same objectives. 17% claimed that they did not know of the objectives of their NRA and another 9% stated that the objectives were different. The key message here is that providers share the same objectives as NRAs.

17%

Of providers claimed that they did not know the objectives of the NRA

In the same way, to gain an insight on the satisfaction levels, NRAs and providers were asked to also give their opinion as regards to the indicators used by providers as well as the guidelines provided by the NRA. From what can be noted, ***the majority of NRAs were satisfied with the indicators used by providers***. 62% of NRAs replied that they were somewhat satisfied whereas only 15% stated that they were missing details on the impact of incidents. Another 23% replied that security incidents were measured in an accurate and timely manner by the providers.

According to ***44% of the providers, NRAs facilitated them in their process of defining appropriate indicators***. However, 13% answered that these guidelines could be somewhat improved. Another 13% answered that they did not need help any from the NRA when measuring security incidents at all. This could because they were already using a good set of indicators, which happened to also be the ones purported by the NRA. There could have also been a certain degree of reluctance on the part of the provider to complying with the recommendations as mentioned in the guidelines. Finally not all providers may have seen the value, or return on investment in complying with regulations.

Figure 9: Satisfaction of security measurement methods – NRA's perspective

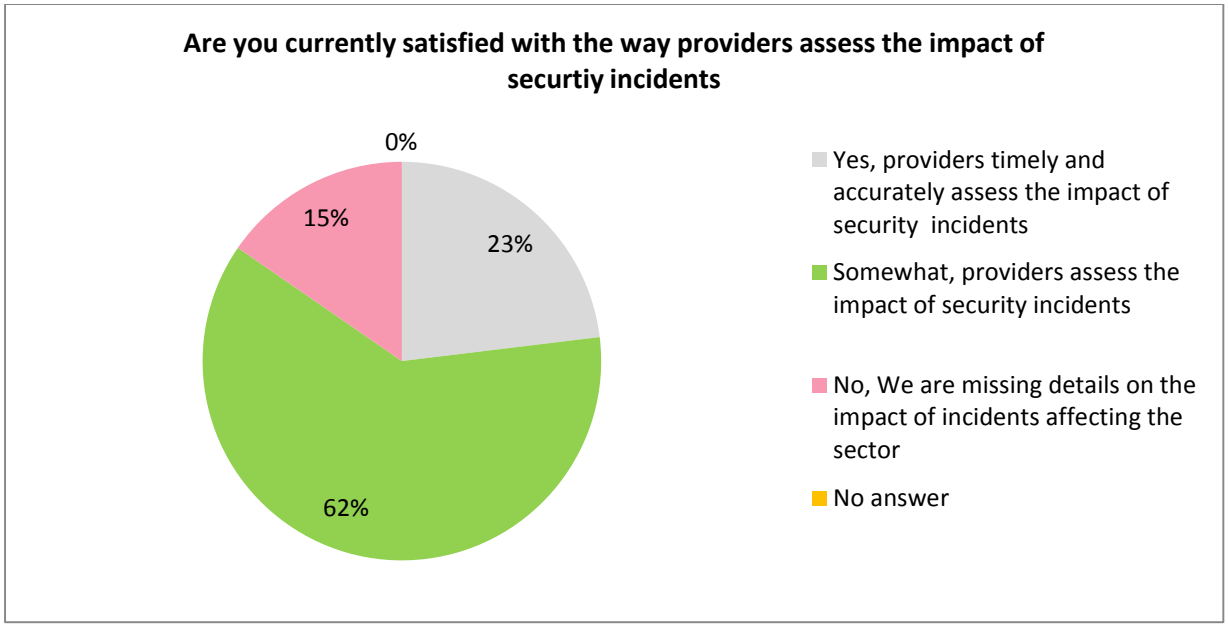
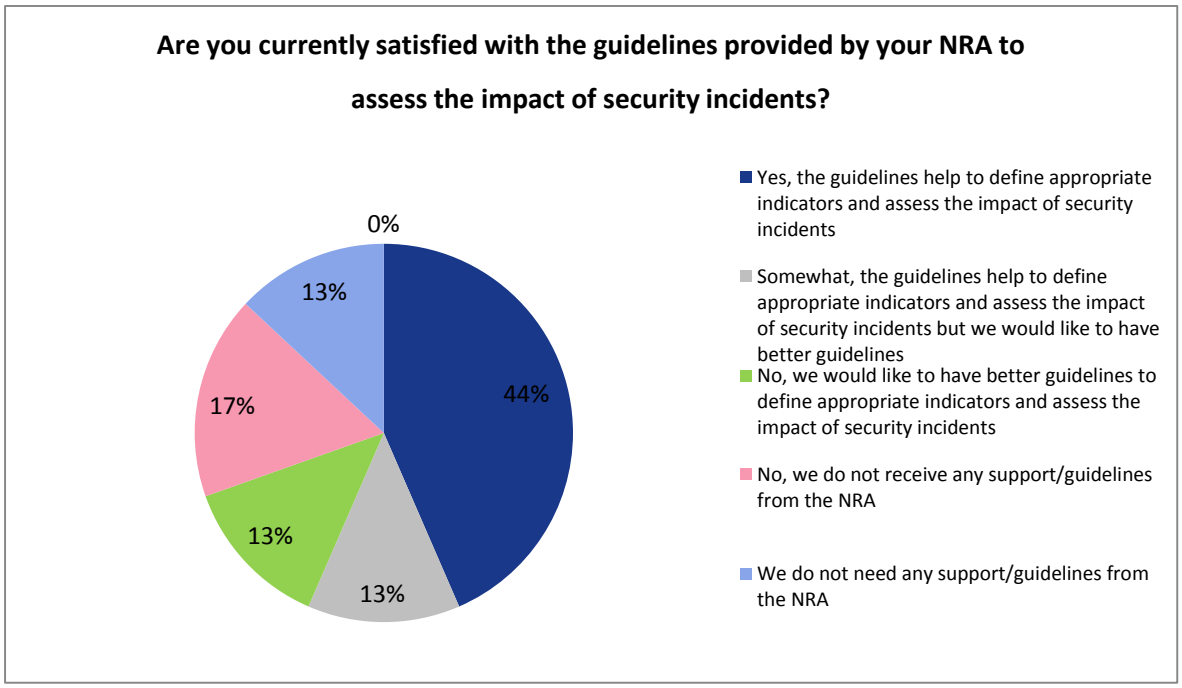


Figure 10: Satisfaction of security measurement methods – Provider's perspective



As mentioned above and to conclude on this part, while there exists some discrepancy between NRAs and providers in terms of why they measure security incidents, and for what purpose they use certain indicators over others, it is still plausible to state that the indicators used by NRAs and providers are more similar than they are different

At the same time, ***while both NRAs and providers may each have their own set of goals which would be unique to their specific situation, the overall and ultimate goal by both parties involved is on minimizing and effectively recovering from any security related incident that affects the electronic communications sector***.

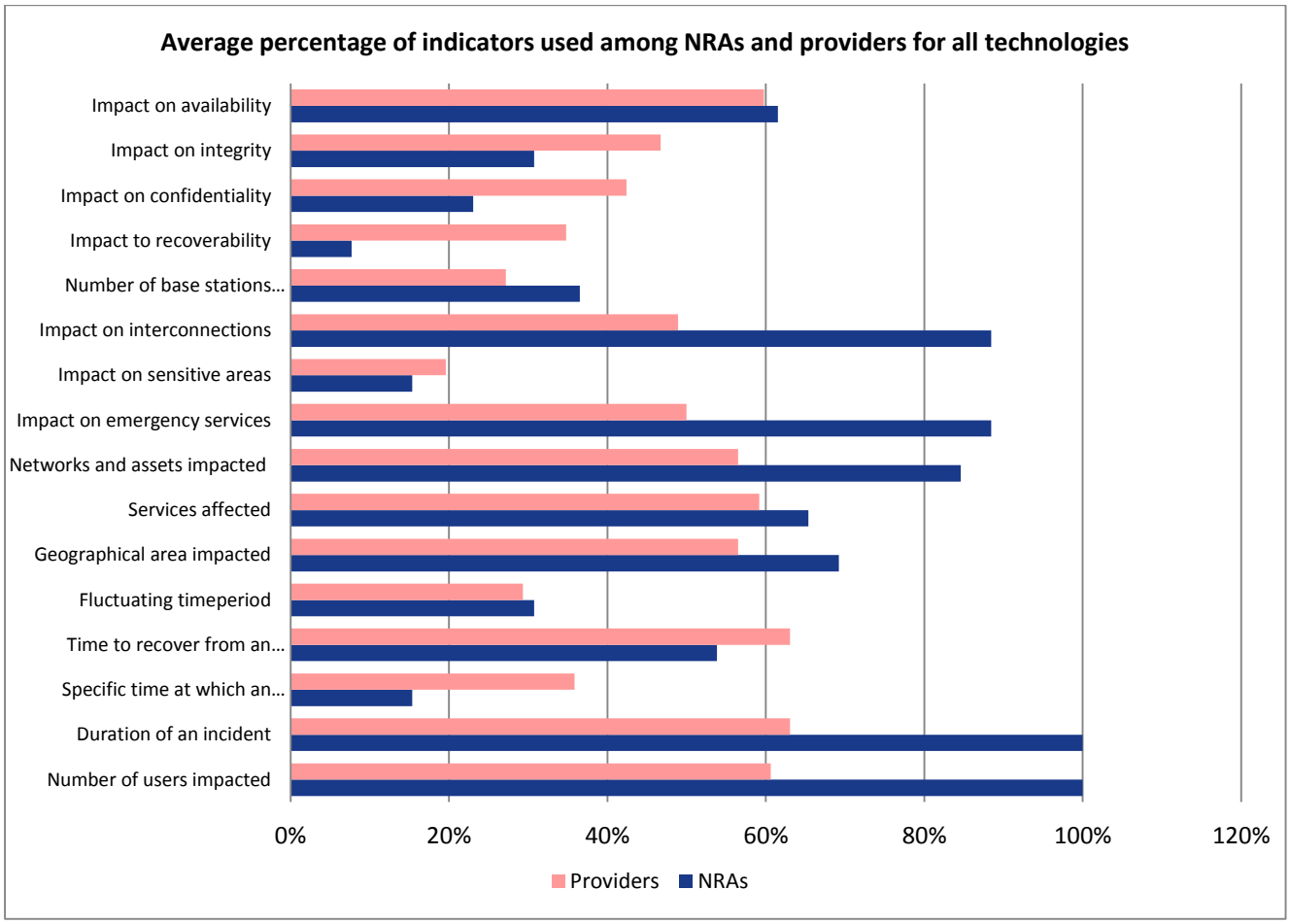
Figure 11: Similarity of goals and objectives between the NRA and provider

SIMILARITY OF GOALS AND OBJECTIVES	NRA VIEWPOINT	PROIVDER VIEWPOINT
Objectives of the NRA and provider are somewhat aligned	(54%)	(44%)
Objectives of the NRA and providers are exactly the same	(23%)	(30%)
I don't know of the indicators used by the NRA/Provider	(15%)	(17%)
Objectives of the NRA and providers are different	(8%)	(9%)

3. Analysis of identified incident indicators

The indicators presented within this chapter have been obtained and were compiled as the most commonly used indicators from the views of both NRAs and providers. The results from the graph below represent the average percentage of users that replied as using the indicators for measuring security incidents for all technologies. In cases where the user did not answer or the indicator was not used, these percentages were omitted from the calculation.

Figure 12: Commonly used indicators among NRAs and providers



From the graph, it can be noted that “number of users impacted” and “duration of an incident” were the most common indicators which were used by 100% of NRAs, whereas providers used these indicators on average 61% for “number of users impacted” and 63% for “time duration” of an incident. Furthermore, “impact on emergency services”, “networks and assets impacted” as well as “geographical area impacted”, was also used quite frequently. This is especially true among NRAs in particular. To obtain more information on the indicators used by both NRAs and providers for each individual technology however, readers can refer to the following sections of the report.

Keeping this in mind, it is important to note that the above does not represent the exhaustive list of indicators. Referring to the summary below, it is possible to also get more information on the measurement methodologies of each indicator including the indicators benefits and challenges.

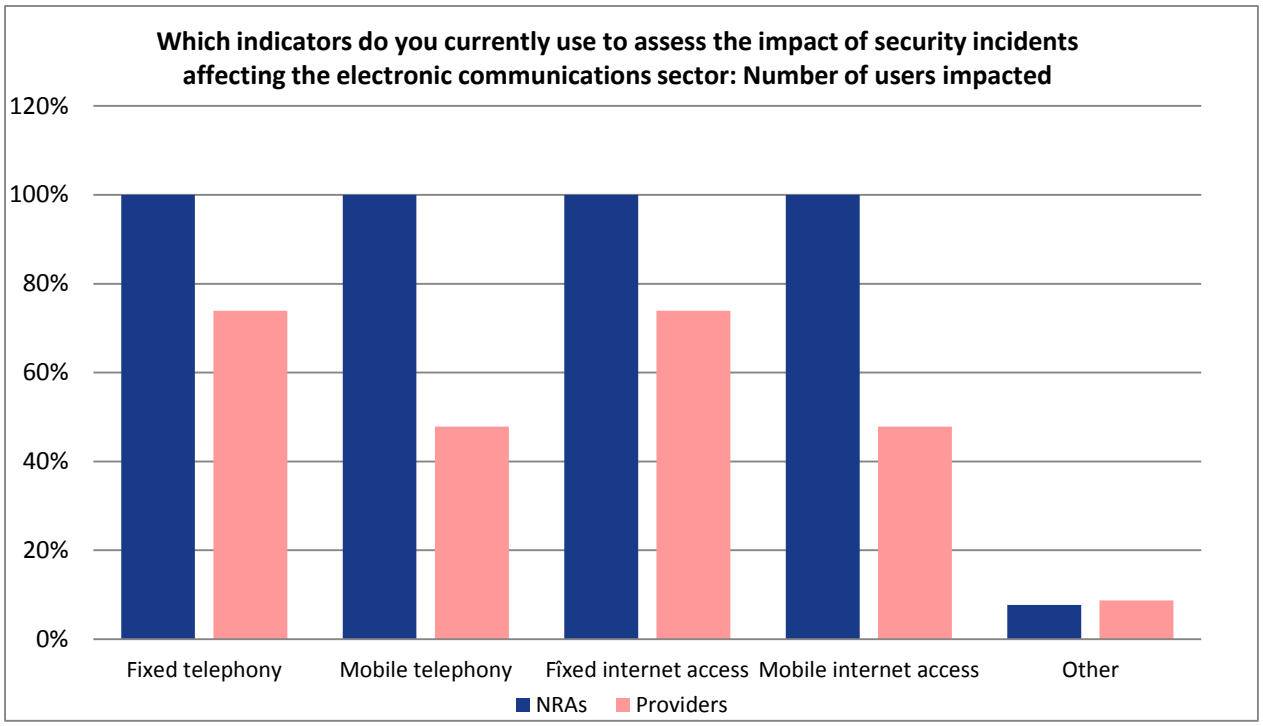
- User/connection related indicators
- Number of users affected (fixed telephony)
- Number of users affected (mobile telephony)
- Time/duration related indicators
- Time duration of an incident
- Specific time at which an incident occurred
- Time to recover
- Fluctuating time period of an incident
- Geographic area related indicators
- Impact based on location
- Geographic area based on infrastructure coverage
- Geographic area based on number of customers affected
- Geographic area based on number of services affected
- Indicators related to infrastructure and services affected
- Network infrastructures and assets
- Impact on emergency services
- Root cause dependent indicators
- Human error
- System failures
- Natural phenomena
- Internal vs. Third party failure
- Economic impact related indicators
- Indicators related to cyberattacks
- Sources/destination of “attacks” related indicators
- Vulnerabilities related to networks and services
- Impact on confidentiality, availability and integrity

3.1 User/connection related indicators

Calculating the number of users or connections affected was identified as a key indicator among NRAs and providers. This indicator was being used by all respondents of the surveys, to measure the impact of any given security incident.

During the interviews, it came to light however that the measurement method for assessing this particular indicator was in fact, the most challenging one. To add to the difficulty, there are different technologies that are offered to customers, such as fixed telephony and mobile telephony etc. which complicate the measurement even further. A common measurement method for each service cannot be applied. For this reason the measurements are grouped per technology.

Figure 13: Measuring incidents based on number of users affected



3.1.1 Number of users affected (fixed telephony)

Identifying the number of users impacted for fixed line telephony is relatively easy to measure when compared with mobile telephony. Fixed telephony service providers can use the number of customers connected to a Switch to estimate the number of affected customers (usually 1 line = 1 subscriber). Furthermore, as providers know the number of users connected to specific equipment, they are in a position to better determine the impact of an incident. However, not all providers are able to apply this method as sometimes 1 line can have many users and this is not always easy to know. The former is often the case when the user is a company (not an individual customer) and unless the providers are able to have access to information about the number of connections/subscribers in the company, the measurement method is not so accurate.

When considering the number of users impacted by a security incident, providers can also approach this by measuring both the provisioned number of customers impacted, as well as the actual usage. This allows for a differentiation between the two because the number of users affected by an incident will not be the same at 4PM than at 4AM. This information can be useful for a number of reasons including for example, maintenance purposes. In addition to the former, the provider can also have in place a detailed process for measuring “service usage”. By using a service usage curve, it is possible to examine the number of users using a given service at a specific point in time as opposed to the number of provisioned users for that particular service.

3.1.2 Number of users affected (mobile telephony)

For mobile services the guidelines are much more flexible. Therefore, providers can chose in which way they want to perform the analysis to determine the impact on their customers. For example, providers can chose to look at the number of people who are living in the affected area or to look at the market share in the specific area and on how the network is dimensioned in this particular area, to find out how many possible affected subscribers are included.

As opposed to fixed telephony, mobile telephony is the provision of telephone services to phones which may move around freely rather than stay fixed in one location, thus making it difficult to measure. An approach taken by some NRAs to overcome the challenge in measuring the number of users affected for mobile services, is to request providers to assess the traffic use of the previous week of the incident or to compare the traffic of the previous week day with the traffic of the current day on the affected equipment and multiply this number with the total number of SIMs they had before the incident took place.

(Traffic last Thursday - Traffic this Thursday) x number of SIM cards = number of SIM cards affected

While calculating the number of SIM cards can be one way of determining the number of users affected in a geographic area, not all the providers have the ability to obtain the exact number. Therefore most of the operators have a rule that considers the average number of users per base station.

In the case of moving disturbances such as a storm, the NRA can request to receive a map from the providers showing the area where the outage occurs at a particular point and the number of affected based stations.

74%

Of providers measure incidents for fixed technologies

48%

Of providers measure incidents for mobile technologies

To summarize, even if NRAs have equipped their providers with guidelines on measuring the number of users or lines that have been affected following an incident, the choice of methodology has been left to the providers.

According to the study, 100% of the NRAs are asking for the number of users affected for fixed and mobile telephony and internet services. When making the same comparison at the provider level, the majority of providers were measuring the number of users affected for fixed telephony and internet technologies, than they were for mobile telephony and mobile internet technologies (74% for fixed telephony and internet and 48% for mobile telephony and internet technologies).

It can be assumed that the reason for which there exists a difference in the figures at the provider level is because some providers are not so sure on how to effectively measure mobile telephony and internet access services than when compared to fixed lines. As mentioned above, this is because it is easier to detect how many users are connected to fixed line services and also to calculate how many users are impacted following an incident than when calculating the number of mobile users as mobile services can be used for many purposes (not only for phone calls). Furthermore, mobile users are constantly “on the move”. Therefore if for example one were to measure the number of mobile users impacted based on geographical area, this would be different based on individual factors (the user may work in a different area to where he lives). There are many other individual factors as such, making the process complicated. Similarly it is difficult to make correlations between users who use fixed and mobile services simultaneously.

3.2 Time/duration related indicators

The gravity of the incident and the type of resources it affects will determine the amount of time and resources needed to recover from that incident. An incident may require far more resources to recover from than what the organization can handle. Those resolving an incident should consider the effort necessary to actually recover from an incident and carefully weigh that against the value of the recovery effort. As with number of users affected, this indicator can be measured in different ways. The commonly identified methods for NRAs and providers were to assess the impact of the former based on the time duration of an incident but also the time to recover from an incident.

For example, “time duration” and “time to recovery” were used as indicators by 100% of NRAs who took part in the survey. Indicators such as “fluctuating time period”, was used on average by 31% and “specific time” at which an incident occurred was only used by 15% of the NRAs.

Figure 14: Measuring incidents based on time – NRAs perspective

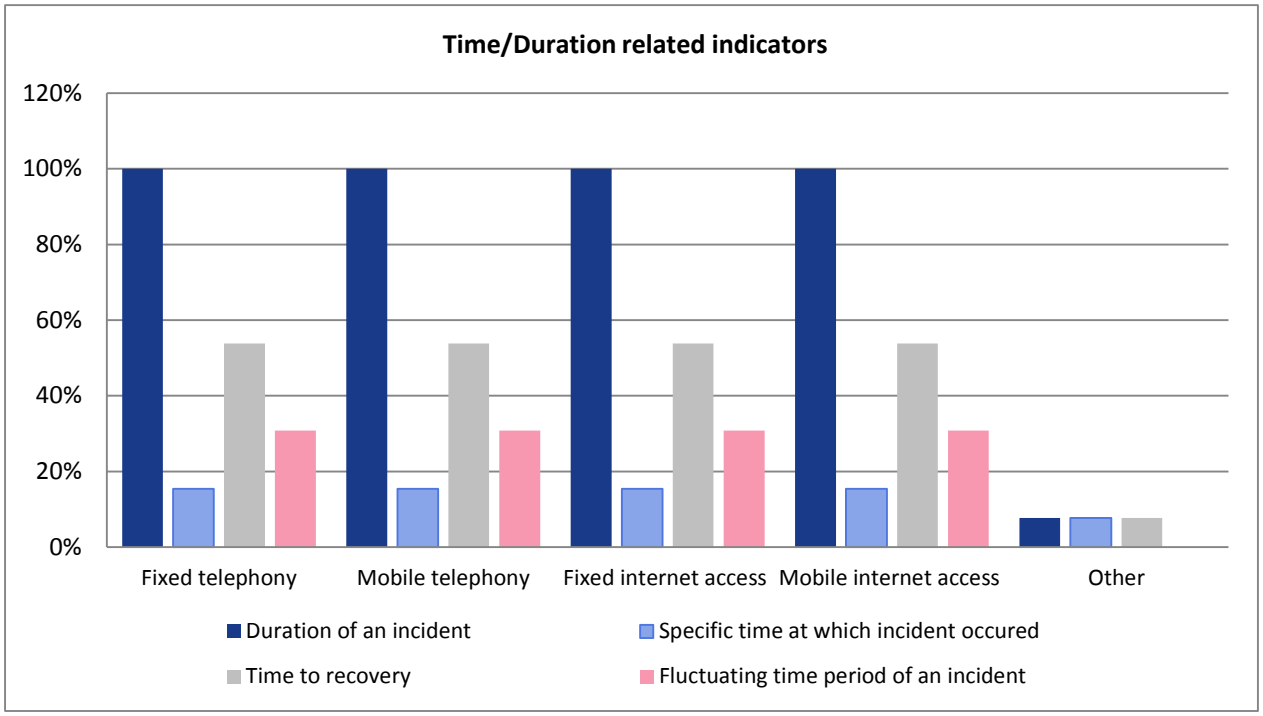
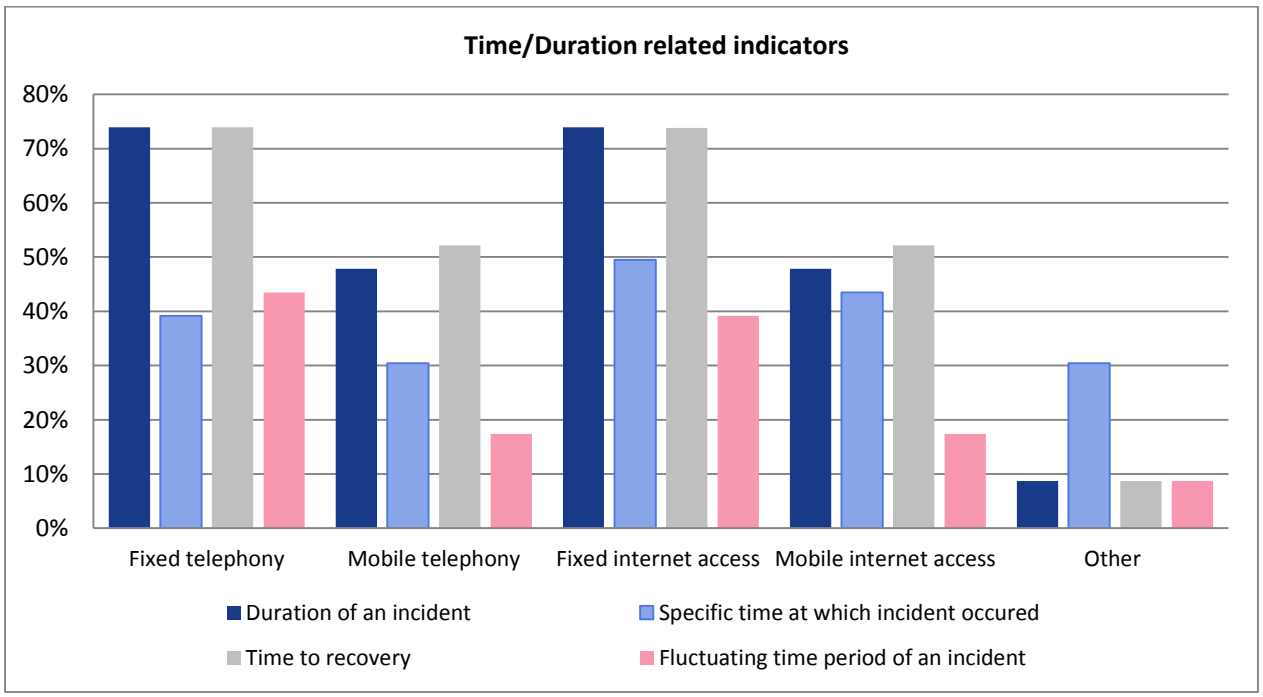


Figure 15: Measuring incidents based on time- Providers perspective



Similarly providers were more commonly using the same two indicators ("time duration" and "time to recovery") in comparison to the other time related indicators too. 74% replied that they were measuring the duration of an incident and time to recover from an incident for fixed telephony and internet technologies. The same is also true for mobile technologies which were used by 48% for "duration of an incident" and 52% for "time to recovery".

3.2.1 Duration of an incident

The time duration of an incident can be assessed from the moment at which the incident is identified until full recovery of the connections (i.e. up until the last connection is restored on the last based station affected).

However, the challenges that some providers have expressed is that there is a lapse of time during which service starts to degrade but is not reported by the providers. Therefore the incident may not fully reflect the total duration of an incident interruption.

Another way to calculate duration of an incident is to break it down into several sections including when the incident started, when it is estimated to be over, and when it is actually over. This helps in determining how long the interruption lasted. Determining the time duration of an incident is a beneficial approach as it is possible to see how long it took to recover from the incident and thus measure how efficient the provider was in resolving it.

In some cases, duration of an incident is only measured after the incident has been resolved, not during resolution.

3.2.2 Specific time at which an incident occurred

Incidents can also be measured based on the specific time at which they occurred. For example, an incident that happened on the weekend can have a different impact from that which took place during a weekday (and that too during working hours). This is because, the chances that more people were making use of telecommunications services during that time are greater, and thus the impact of the incident as well as its consequences, would have also been greater. So, this indicator would be addressed if the number of affected users was calculated based on statistic usage curves (which vary throughout the day) and not based on provisioned customers.

3.2.3 Time to recover

Time to recover can often be confused with duration of an incident. Therefore it is necessary to create a distinction between the two. Where duration of an incident reflects the action taken from beginning to end of an incident, time to recover is calculated from the moment the restoration work has started on the incident and ends with full recovery. Time to recover from an incident (i.e. hours or minutes etc.), often takes less time than the actual duration of the incident.

That being said, there are also some additional complexities with measuring this indicator. This is because it is often hard to differentiate between when an incident actually occurred, in comparison to when it was realized or acknowledged. Furthermore, in terms of calculating the time to recover from an incident, NRAs and providers also expressed that they found it a bit challenging to know on what basis to measure the recovery of an incident. For example, does this depend on the time it took for all services and users to fully recover from an impact of an incident, or did this depend on when the number of users and services affected, were within a certain range (i.e. below the defined threshold).

3.2.4 Fluctuating time period of an incident

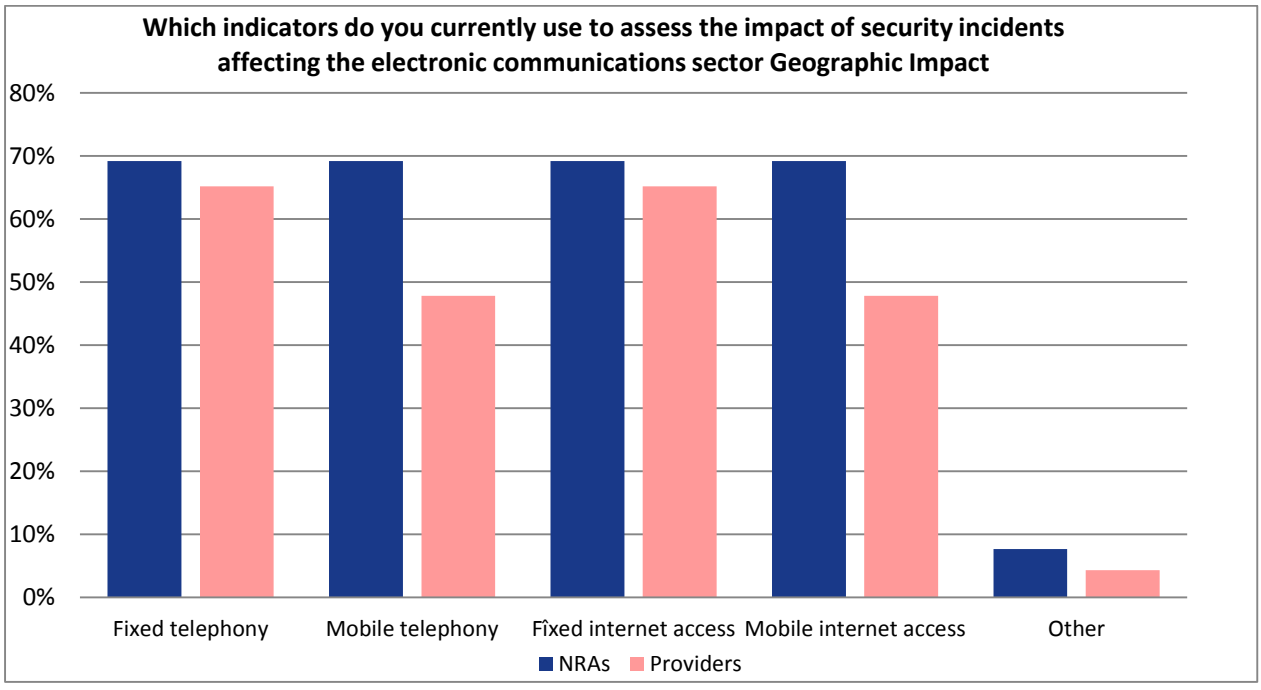
Measuring the fluctuating time period of an incident might prove challenging because the quality of the offered service usually will not degrade instantly. There may be some fluctuations in the services' functionality which could still be rather volatile, for a certain amount of time, before the service eventually results in total failure. Focus should be placed on service degradation.

That being said, when providers report on time/duration related indicators, they need to be specific on what basis they are measuring "time". This is because if one provider has calculated the impact based on time to recover from the incident, whereas the other has done the same based on time duration of the incident, the end information reported to the NRAs cannot be accurately measured nor compared between one another.

3.3 Geographical area related indicators

Measuring security incidents which affect certain geographical areas, allows NRAs and providers to identify which region is most affected by an incident. The benefit of measuring security incidents using this approach is that, through this, it is possible to determine whether or not the geographic landscape of a location plays a role in the frequency at which an incident takes place and in determining the type of incident that has occurred. Geographic impact, on both fixed line and mobile services, is calculated by almost all respondents of the survey.

Figure 16: Measuring incidents based on area impacted



Calculating the geographic spread of an incident is especially important to consider in countries with diverse surroundings. For example, places that are urbanised and better connected would experience less disruptions, but the disruptions would affect more people than when compared to areas that are less urbanised. That being said, the impact of an incident affecting an island near the sea would be

greater due to poor network coverage. Furthermore, the chance of an incident occurring in remote areas is greater due to national hazards such as storms and bad weather.

3.3.1 Impact based on location

Security incidents can be measured as per the number of square km affected. For instance, in countries where access to certain areas is rather remote (i.e. mountains, isolated islands, forests etc.), an outage can impact either half the city, or nobody at all (which should be taken into consideration).

Furthermore, depending on the size of the geographic area and the impact which the incident caused, the incident is either requested to be reported to the NRA, or not reported at all. Whether or not to report an incident depends on the thresholds set by the NRA. In most cases, the NRAs were found to have followed the guidelines provided by ENISA when defining such thresholds.

For some NRAs, it's difficult to assess the location of an incident as one incident can affect several locations. Furthermore, if there is an area with only one operator and this operator experienced an interruption of services, there is an increased chance that the consequences of the incident will be more severe.

3.3.2 Geographic area based on infrastructure coverage

Another way to measure incidents' impact can be based on the geographical coverage of the networks. Some NRAs did not use a specific geographic area to measure this indicator as one base station can cover many areas. Instead, this indicator can be measured by calculating the number of base stations that are affected. By identifying the number of base stations impacted, it is possible to identify each of the different areas that are associated with that base station and hence, calculate the geographic spread.

3.3.3 Geographic area based on number of customers affected

Measuring the geographic impact of an incident can also be calculated by combining the geographic spread with the number of customers affected. That being said, regardless of the area which was impacted, the total number of customers can be measured first. Based on the total number of customers that are impacted, it was later easy to identify the area in which the incident took place.

3.3.4 Geographic area based on number of services affected

Similarly, geographic impact can also be calculated based on the number of services affected and the areas where they are provided. Services such fixed or mobile telephony, voice and internet access services are included in this calculation. Taking the example of fixed line services, if 500 or more customers are affected, then the incident is considered as significant (depending on the thresholds set by the country), and as such should be reported to the NRA. Determining the number of services affected ant the area where the services are provided, can help determine and locate the geographic spread of the incident.

3.4 Indicators related to affected infrastructure and services

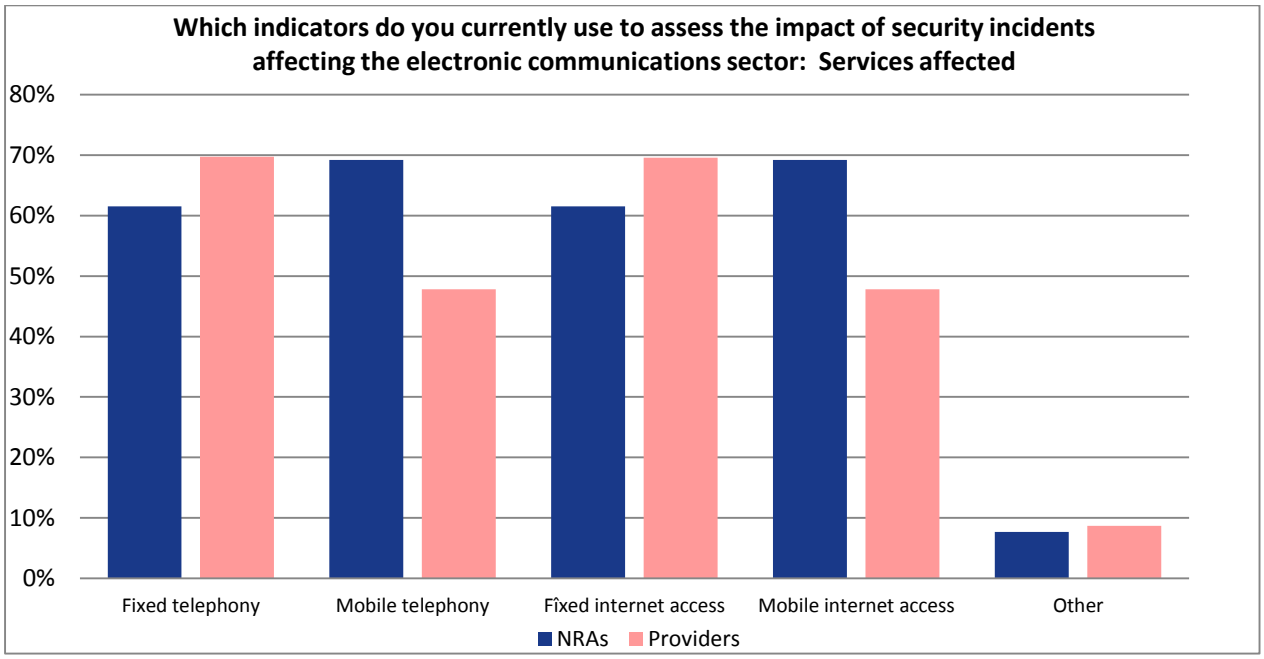
Providers are requested to assess the types of infrastructures and services that are affected following an incident. Assessing the types of infrastructure and services affected can enable an overview of the ones that are most vulnerable to threats. Precaution can therefore be taken on those assets and investment in newer infrastructures can also be made if needed.

3.4.1 Network infrastructure and assets

Using indicators to measure security incidents on network infrastructure and assets is generally quite straightforward. Providers are requested to give information to their NRAs on the types of infrastructures that have been impacted. This includes information such as the providers' internal networks (core networks and active networks) that are affected as well as on the type of services that were affected (TV services, voicemail services etc.).

However, it is not always clear on how to measure this aspect. The main question that needs to be asked is does this calculation depend on the number of services and assets that have resulted in total shut down, or does this instead refer to a percentage in the number of service that are impacted (20% of services for example).

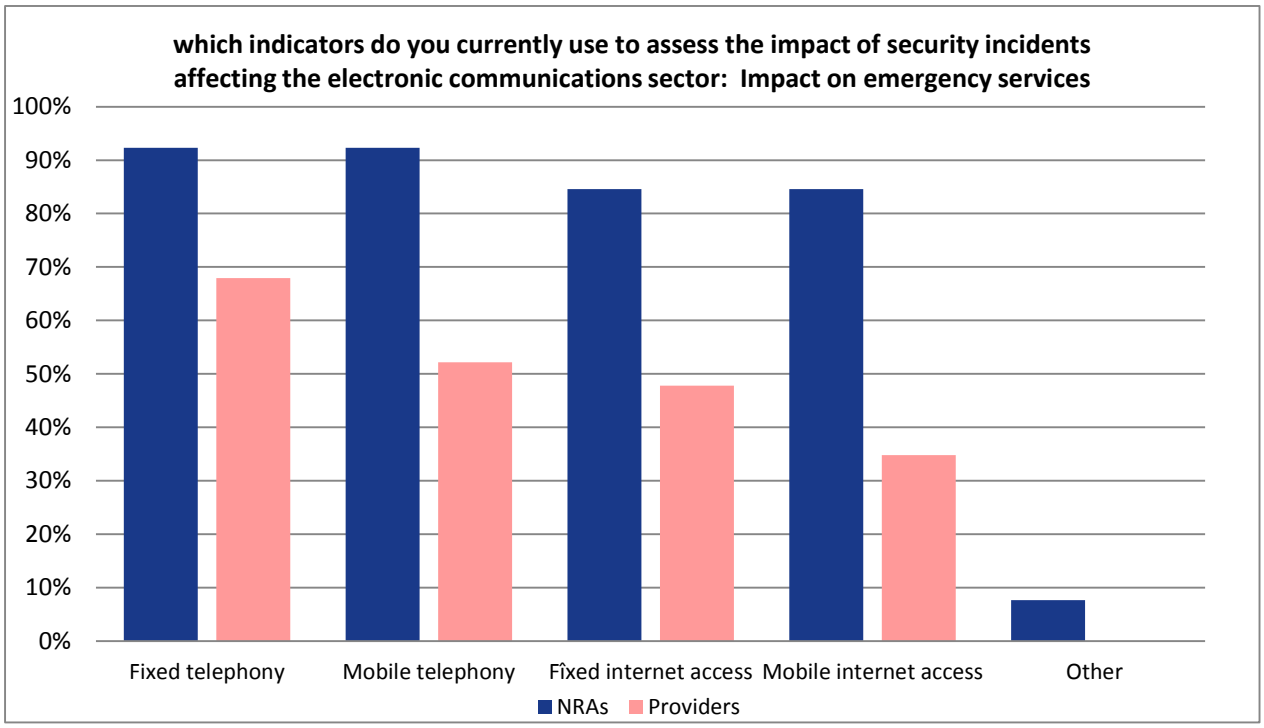
Figure 17: Measuring incidents based on services affected



3.5 Impact on emergency services

Ensuring that security incidents do not impact emergency services is highly important in the telecommunications sector. In case of any emergency, people expect to be able to reach the right services and on time. This includes dialling numbers such as 112, to report events such as accidents, burglary, fires etc. Emergency functions should be working at all times in order to protect the general safety of the public.

Figure 18: Measuring incidents based on emergency services



Analysing the impact of incidents on the emergency services was measured for all technology types such as fixed telephony, fixed internet access, mobile telephony and mobile internet access. This is especially true for NRAs wherein 92% were measuring the former for fixed technologies and 85% for mobile.

That being said, measurement methods can be complicated because for example, if an incident affects a phone service, it can potentially affect emergency service calls as well. In some cases, only the emergency services are affected while other telecommunications services are still functioning. The numbers of affected users are counted differently here as users may still have their services working while being unable to reach the emergency services. In this situation, the number of users is the number of users that cannot connect to an emergency number. As stated by most of the respondents, for determining the impact on emergency services, it is often the case that NRAs and providers rely on estimates (such as previous statistics etc.).

3.6 Root causes dependent indicators

Determining the impact of an incident based on the analysis of the root cause, can be a good approach. Determining what went wrong, and what led to the incident to occur in the first place, can minimize or monitor similar patterns of the incident should such an incident occur in the future.

However, some issues that providers can be faced with, is that although they were required to report the root cause of the incident, the form which they had to complete, was structured in a way that made it difficult to understand. The form was sometimes too technical and those completing it were not able to provide enough precision on the specific reason for the incident. Without enough precision on the root cause of the incident, it makes it difficult for NRAs and even providers to clearly analyse what went wrong and assess the points of improvement.

Malicious attacks also falls under this category but has been explained more in detail in section 3.8 of the report

3.6.1 Human errors

Using "human errors" as a measurement to assess security incidents can help to assess whether the incidents have taken place due to negligence and/or lack of awareness of people. Human error incidents are usually caused during the operation of equipment or facilities, the use of tools and the executions of procedures, etc. In order to avoid this kind of error in the future, trainings can be conducted for the relevant parties involved. That being said, human error also includes things such as misconfigurations. If a system is not properly configured, it can lead to security incidents.

3.6.2 System failures

Measuring the impact of security incidents as a result of system failures, such as hardware and software failure, can encourage the NRAs but mostly providers to put in place rigorous monitoring mechanisms of their systems. Furthermore, in case there are a lot of incidents that have occurred due to system failures, providers can look to invest in newer infrastructures. Nevertheless, this process can get quite technical. Therefore, by analysing the reason for which the incident resulted in system failure and thereafter providing high-level information on this can help the necessary people concerned to determine whether or not to spend on new infrastructure.

3.6.3 Natural phenomena

The indicator "natural phenomena" includes measuring incidents that are caused by severe weather, earthquakes, floods, wildfires, and so on. After measuring the probability of an incident occurring due to natural hazards, providers can build stronger infrastructure or backup systems in order to ensure continued availability. That being said, after identifying the areas which are most likely to be affected by natural phenomenon and/or measuring the probability of natural phenomenon occurrence, means that providers can be better prepared for such incidents and take the necessary precautions accordingly.

3.6.4 Internal vs. Third party failure

Third party failures are an important variable when measuring security incidents. If the incident was due to an outside vendor technical issues, is an important thing to consider, as outsourcing some of the services to outside parties is a common approach of providers nowadays. Determining if an incident is internal or external can assist providers in the identification of whom the incident will impact and areas to approach in order to mitigate the incident. 16% of all incidents reported in 2014[2] to ENISA, were third party failures.

3.6.5 Malicious actions / cyberattacks

Incidents related to cyber-attacks can also have an impact on telecommunications services. As such NRAs and providers should also consider measuring security incidents from this point of view. This is especially true for internet services (both fixed and mobile). For example, denial of service attacks (DOS), or attacks on the network (related to cyber-attacks) can result in downtime. As with the telecommunications

[2] Annual Incident Report 2014

sector, cyber-security related incidents can affect a varied range of industries. There is plenty of information on how to calculate the impact of an attack, detailing the use of algorithms etc.

Source/destination of "attacks"

Measuring the source or destination of an incident can help NRAs and providers to identify the cause of an attack as well as its target. This also helps in identifying incident's criticality as well as the severity of its impact. Understanding the severity of the impact can be derived by studying who the former will affect: the customers, the network or the whole country. Necessary measures to mitigate the risks depending on the destination of the attack can thereafter be put in place. That being said, identifying the source of an attack helps in determining if or not the incident was intentional. The need to identify "attack" incident types is becoming more and more common as such incidents are being encountered on an often basis. NRAs and providers should be prepared to handle such situations. Furthermore, there are different types of cyber security attacks and the necessary measures to address them, may differ from one another.

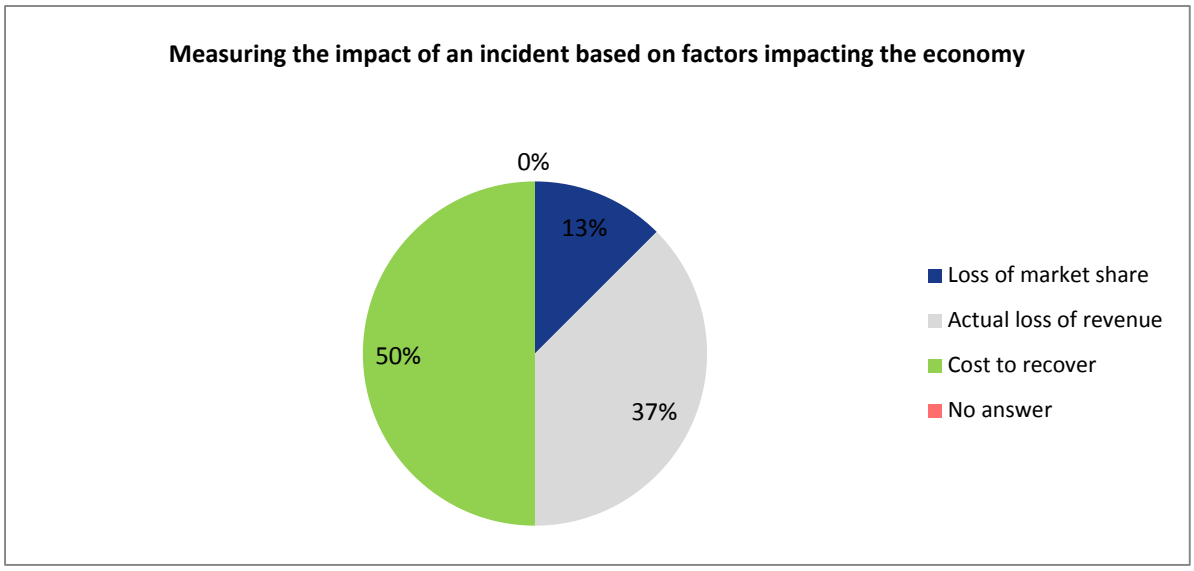
Vulnerabilities within networks and services

Taking into account network and services vulnerabilities can also be another approach to take. As a provider, knowing and understanding vulnerabilities within the network can be an advantage when addressing incidents. For example, if one segment of the network can be made unavailable due to a serious vulnerability, that may be also present in other segments, knowing the situation and how to address it can help the provider in preparing the response to the incident and can help him prevent similar incidents in the future.

3.7 Economic impact related indicators

Though it was expressed by both the NRAs and providers that cost of damage was an indicator which was not used commonly, assessing security related incidents from this viewpoint can lead to some benefits. Providers were using cost to recover from an incident more frequently to measure the impact of recovery of an incident (50%) than when compared with measuring the actual loss of revenue following an incident (38%) or measuring the loss of market share (14%).

Figure 19: Economic related indicators to measure security incidents

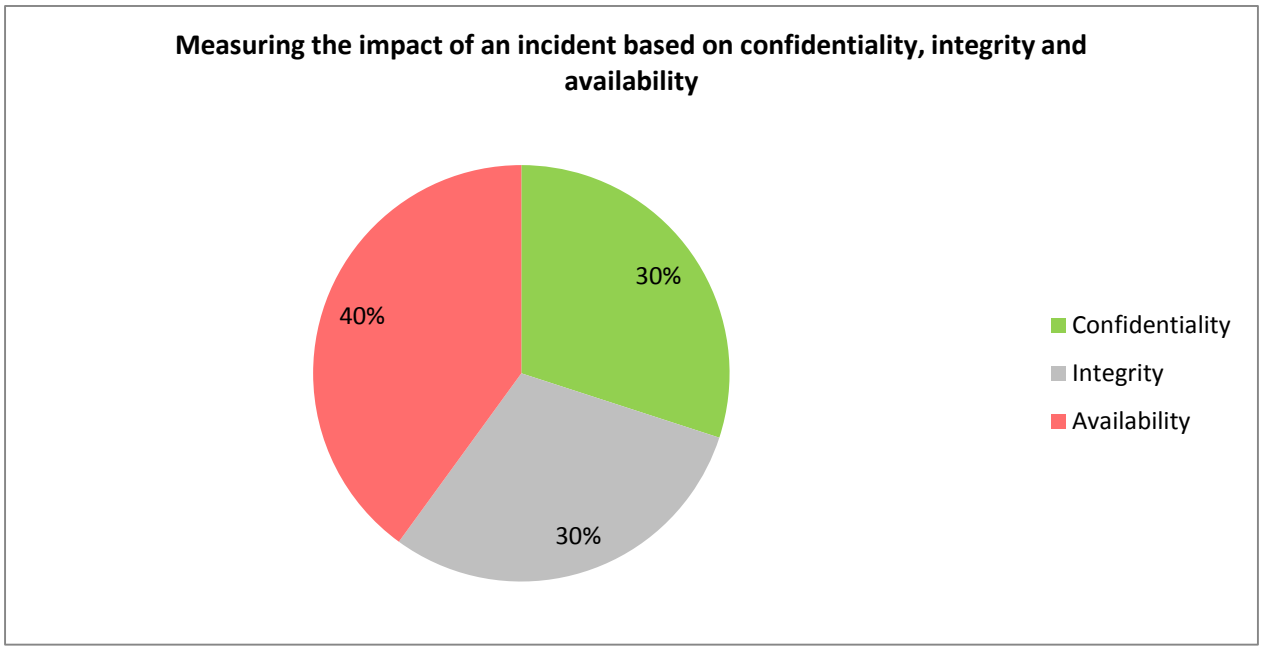


Examining economic impact related indicators can be used by the providers to assess the overall damage of an incident.

3.8 Impact on confidentiality, availability and integrity (CIA)

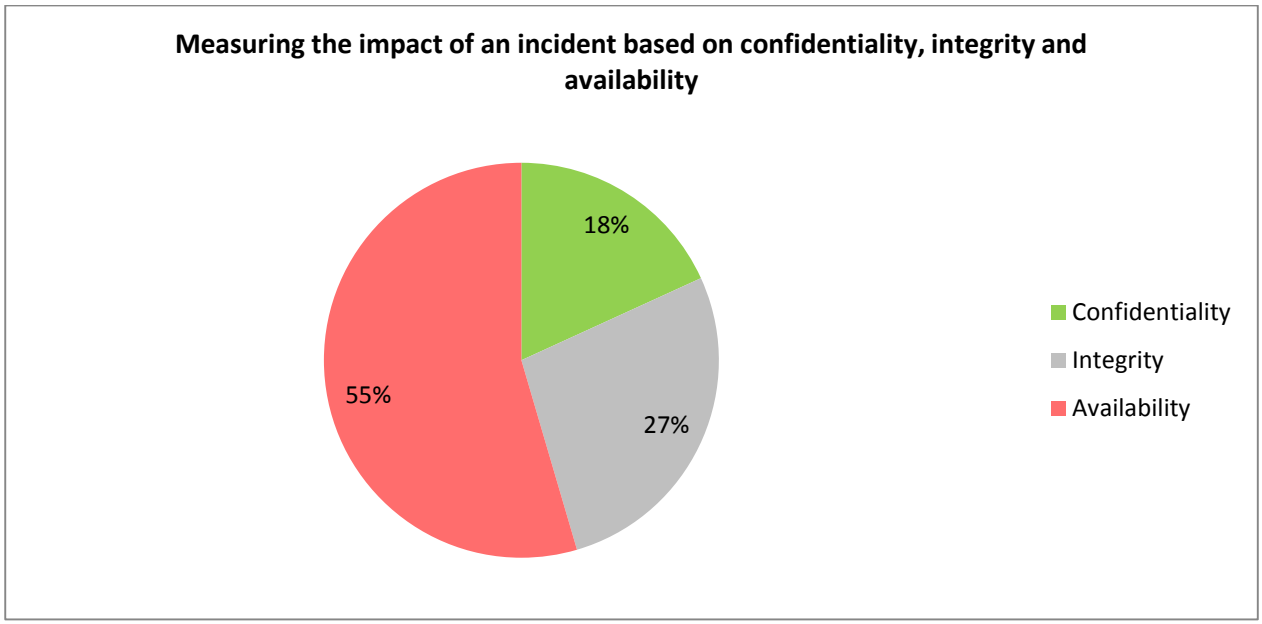
Evaluating the impact an incident has on availability, is the most pertinent factor in the telecommunications sector and the majority of providers were measuring impact of an incident based this metric (40% agreed). Nevertheless, security incidents can also negatively affect other areas too. If information is disclosed to unauthorized individuals, or if, for example, the information is not accurately available, businesses may suffer undesirable consequences. This could lead to a loss in customer confidence, contractual damages and can even result in financial losses

Figure 20: CIA related indicators to measure security incidents – provider's perspective



As a general remark, the CIA triad (confidentiality, integrity and availability) is designed to guide policies for information security within an organization. The triad can be adapted to telecommunications without only emphasising on availability. At the moment only 30% of providers are measuring incidents based on confidentially and integrity.

Figure 20: CIA related indicators to measure security incidents – NRAs perspective



Similarly, availability was the most commonly assessed indicator among NRAs, with 55% using this indicator to measure the impact of security incidents (mainly due to Art. 13a specific requirements). Integrity was measured among 27% and 18% focused on the confidentiality aspect to measure security incidents.

Protecting sensitive information is becoming a key topic, not only in telecoms but in information security as well and by measuring the impact an incident has on sensitive information and on the integrity of such information can be another angle by which to assess security related repercussions.

3.9 Indicators used per technology

A point which needs to be highlighted is that for some of the questions in the survey, respondents were allowed to select more than one technology when specifying the indicators used to measure security incidents (as seen in sections 3.1 to 3.9). For example, for the indicator "number of users impacted", providers answered that they used this indicator to measure the impact of an incident for "fixed telephony", "mobile telephony" and "fixed internet", "mobile internet" etc.

To identify the percentage of indicators used per each individual technology, the same data used in the sections above can be presented in a different way. Using this method it is possible to identify why some indicators were used a lot less or a lot more for some technologies than when compared to others.

Figure 21: Indicators used per technology- Fixed technology

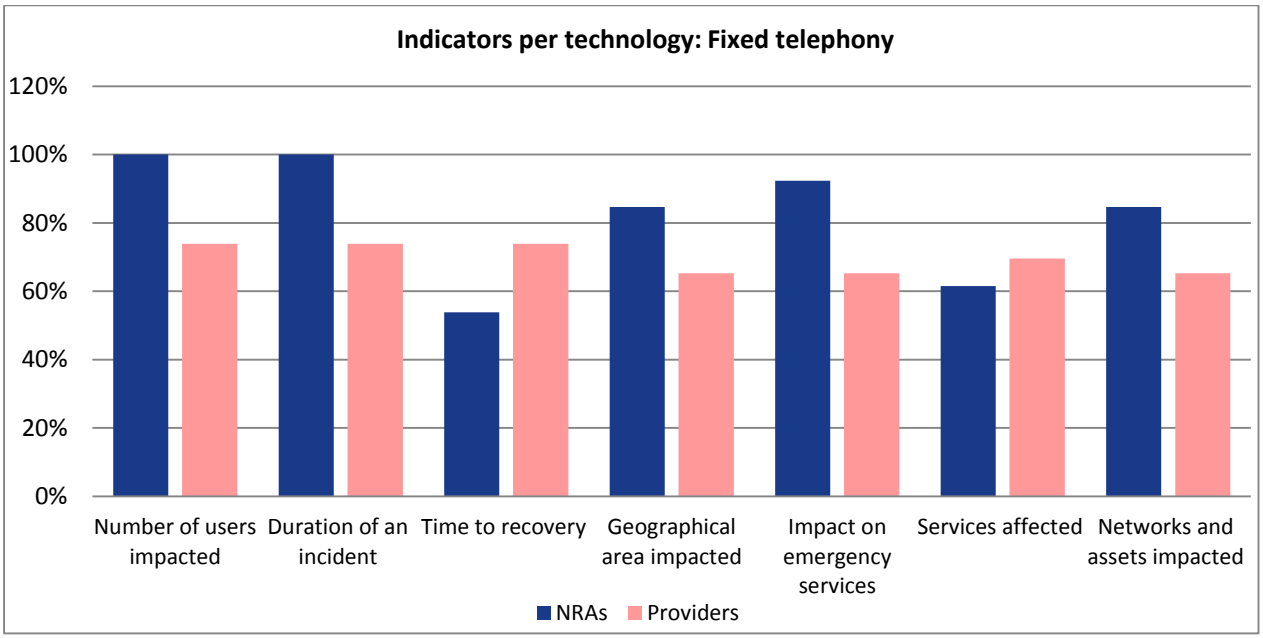


Figure 22: Indicators used per technology- Mobile Telephony

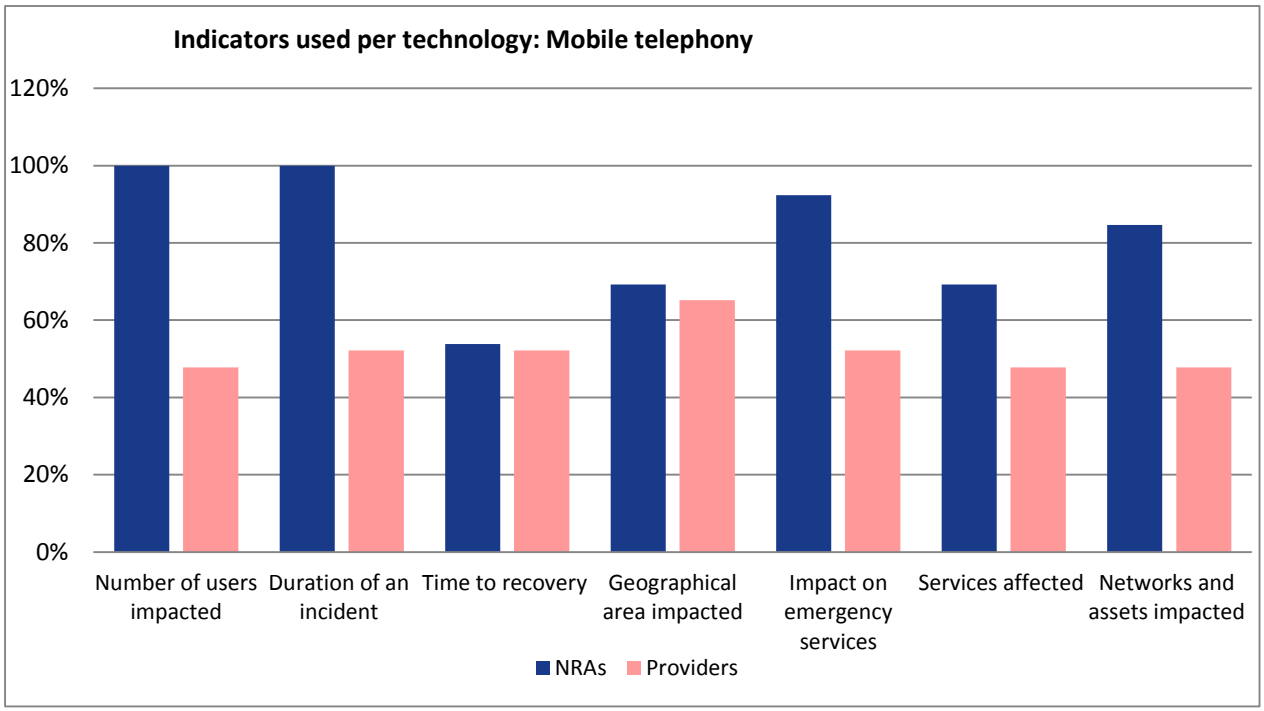


Figure 23: Indicators used per technology – Fixed internet

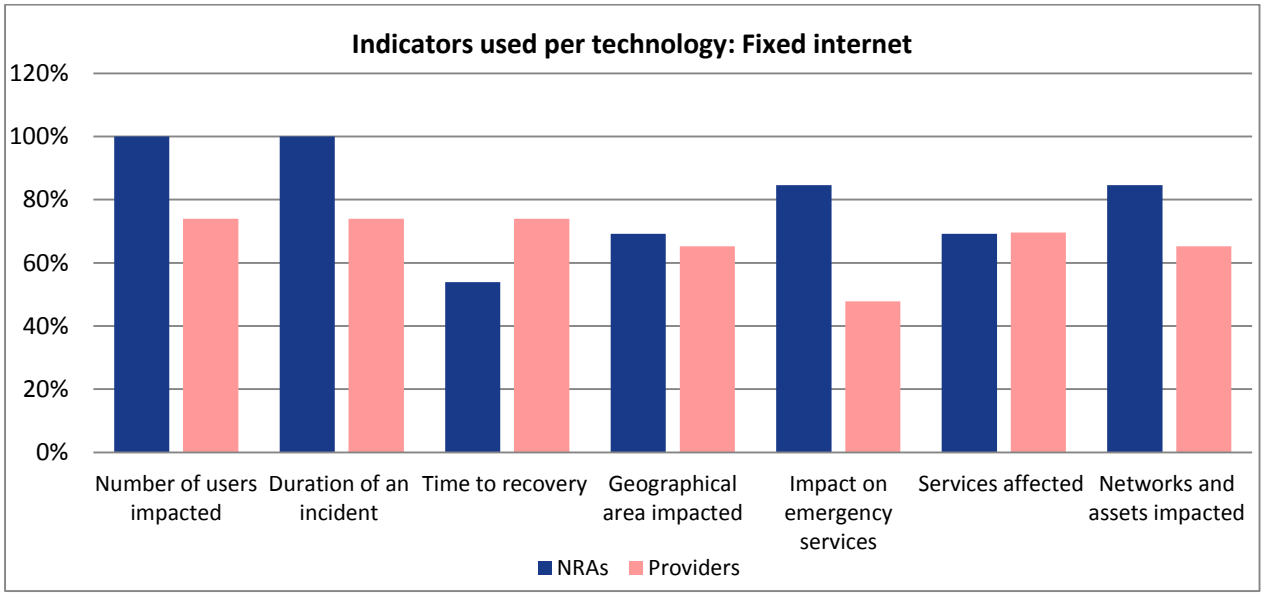
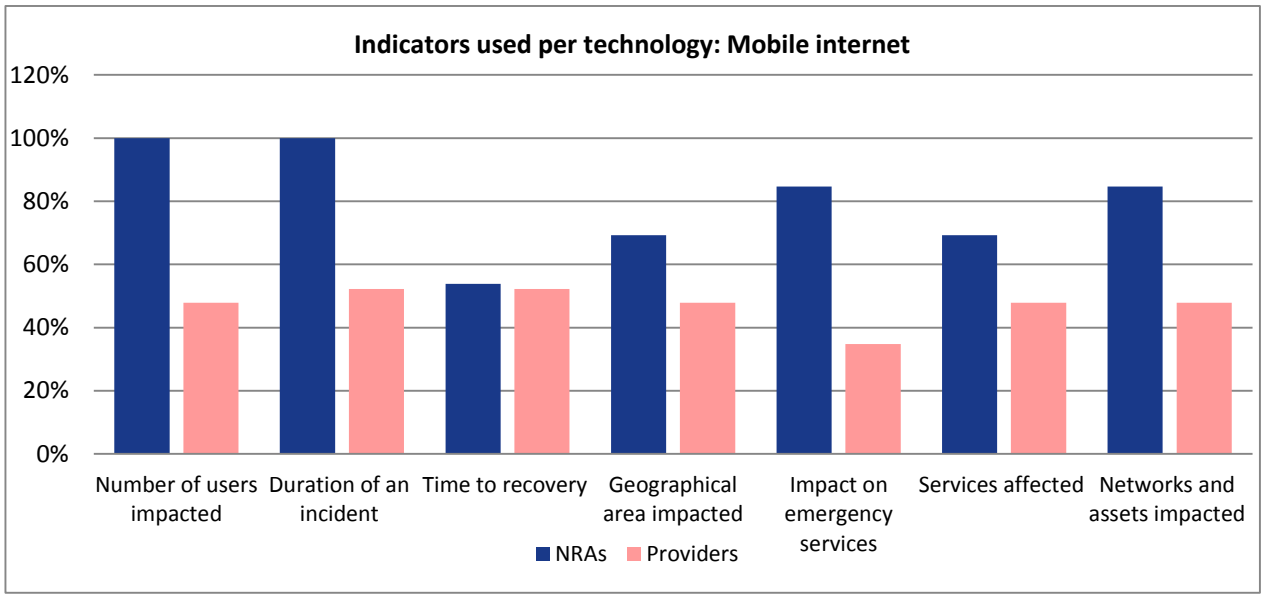


Figure 24: Indicators used per technology – Mobile internet



From the analysis it can be said that indicators used in the context of fixed technologies (both telephony and internet) were used in general more than when compared to mobile technologies, among both NRAs and providers.

To add to this point, it can be said that NRAs seem to be using the indicators more "effectively" than providers. For example, indicators such as "number of users impacted" and "duration of incidents", is used by all NRAs who answered to the survey, for all technologies (100%). Furthermore, at the NRA level, the answers were very similar from one technology to the other. On the other hand, this was not the case at the provider level. The extent to which each indicator was used, and that too for each technology depended a lot on the provider's level of maturity and also to a big extent on the provider's relationship with its NRA. On average, indicators were used quite well for fixed telephony technologies. However, the percentage of providers who were using the indicators (mentioned above), to measure the impact on mobile internet, was considerably less (almost half as less), for mobile technologies. The reason for this relates once again to the fact that knowing how to evaluate the impact of a fixed technology is more straightforward than that of mobile. As is described at the start of this section, there are many additional complexities involved in mobile telephony and mobile internet services that both NRAs and providers should consider.

4. Particularities regarding measuring the impact of incidents

4.1 Defining significance of an incident

Defining the significance of an incident is an important aspect for measuring its impact. That being said, some indicators are definitely more pertinent than others. The Article 13a group along with ENISA have established some informal indicators along with the corresponding thresholds, to be used by NRAs and providers in the EU. These are not imposed, however they can be used to measure the significance or severity of an incident and can also encourage NRAs and providers to use their own thresholds. Based on those thresholds and indicators, they could be adopted as is by the involved stakeholders or modified accordingly, based on their necessity. This was also the case of most NRAs that used the indicators and thresholds as an inspirations, but followed a national approach based on their particularities.

According to the data gathered during this study, ***significance is mostly measured based on two key indicators: the number of customers impacted, and the duration of an incident***. An additional indicator which is also commonly used is the ***number of services affected***. To derive appropriate results, NRAs and providers can use a combination of these indicators in their calculation methods. For example, significance can either be calculated based on the number of users impacted vs. duration of an incident, or the number of services affected vs. duration of an incident.

If an incident results in downtime, but the time taken to recover from the impact is below the threshold defined by the NRA, or the number of users that were affected by the incident is below a certain threshold, then providers are not obliged to report the incident to their NRAs, as the incident is not of a significant impact. As per the informal guidelines of the Article 13a group, incidents should only be reported if the incident reaches the red areas from the table below, as regards to the number of affected users and the duration:

Figure 25: Example of thresholds used for the Art.13a annual summary reporting

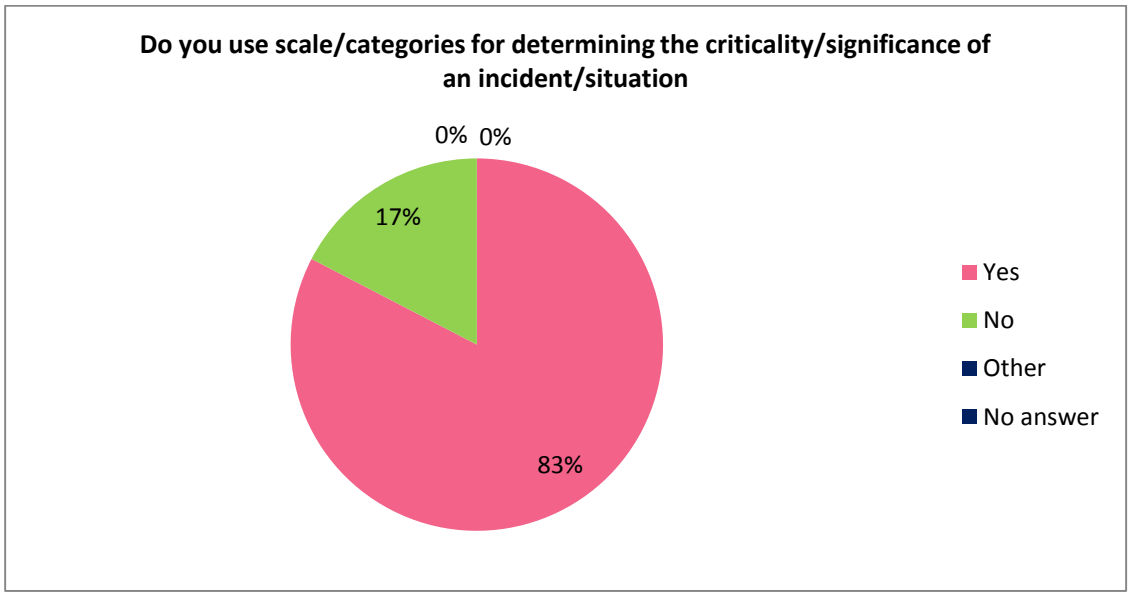
	1h-2h	2h-4h	4h-6h	6h-8h	>8h
1% - 2%					
2% - 5%					
5% - 10%					
10% - 15%					
> 15%					

4.2 Using scales of criticality for assessing the impact

Another approach to take when measuring the significance is to measure the criticality of the incident.

Using scales of criticality to assess a security incident, to a certain extent coincides with measuring the significance of an incident. NRAs and/or providers can categorize indicators into criticality levels such as: "red", "amber" and "green". If for example, several incidents took place within the same time frame, making use of the criticality levels can help in prioritizing which incident to resolve first.

Figure 26: Scales of criticality– provider's perspective



That being said, in cases where criticality levels were being considered, for the most part almost all relied on the ENISA metrics. 83% of respondents revealed that they were using this to categorize the impact of the incidents. One provider mentioned that the number of resources required to solve an incident also depended on its criticality. For them, the general rule they were using depending on the criticality of an incident is that a serious incident would be addressed by a specific department within the organization, a very serious incident, would require the help of several departments and finally, if the incident resulted in a crisis, the incident would be taken care of at operator level.

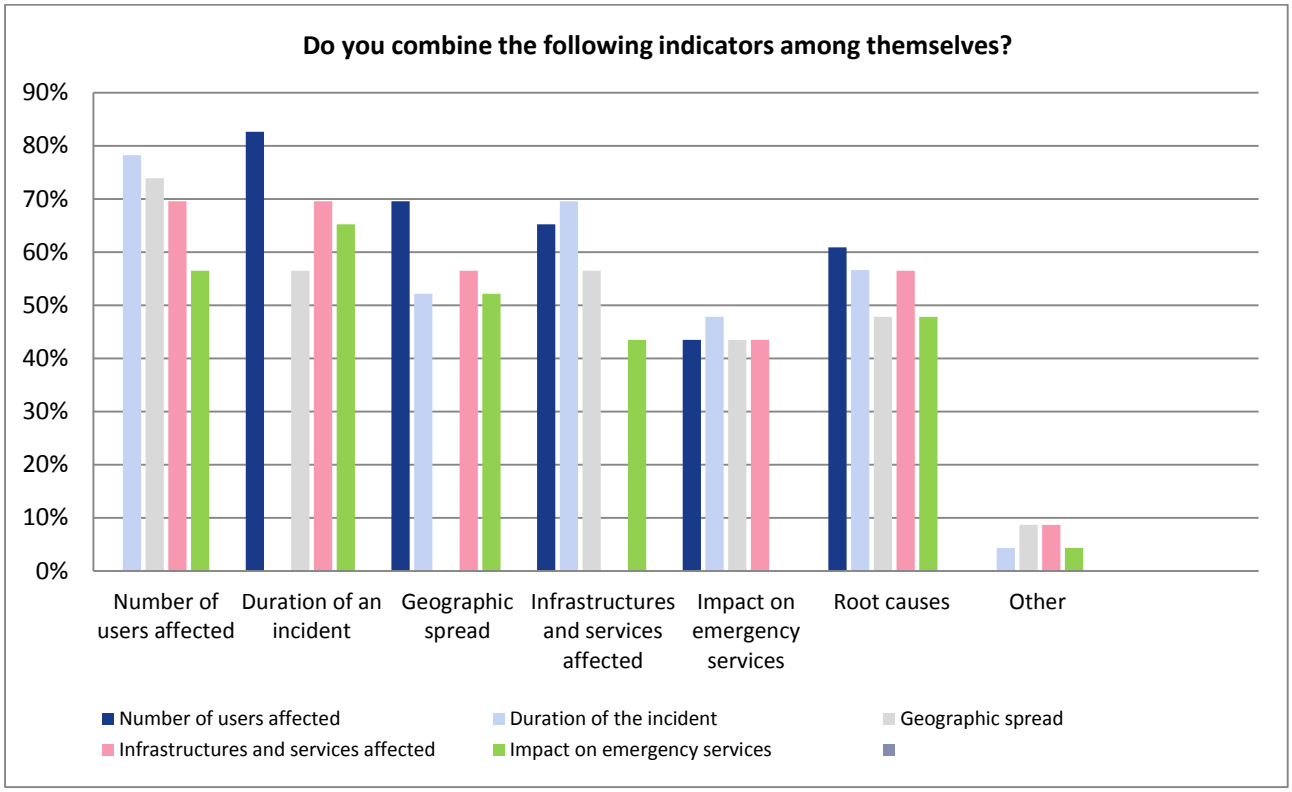
4.3 Using combination of indicators

To assess the severity of an incident and to also be able to know the level of resources required to solve the incident, the provider was relying on certain thresholds. The impact of an incident depended on the time duration as well as the number of users affected for each service category. Measuring security incidents using a combination of indicators is an interesting approach to take. Many providers and NRAs are already using this method and the main advantage is that they can observe the impact of a security incident from various perspectives.

Furthermore, combining indicators can help gather more precise information on the impact of an incident. For example, it can allow NRAs and providers to understand the correlation between the number of user vs. the number of services impacted, and the number of users vs. time duration etc. That being said, the indicators which can be use are countless, and it is up to the specific NRA and provider to

decide how the want to use the indicators, and on what basis they want to calculate the impact of an incident.

Figure 27: Using a combination of indicators – provider's perspective



Among providers, the most commonly used indicators were the following: number of users affected combined with duration of an incident (83%) and number of users affected combined with geographic spread (74%). Furthermore, providers were also calculating number of users affected with geographic spread (70%). The same is also true for NRAs wherein number of users impacted was often calculated in combination with the duration of the incident (for 85%).

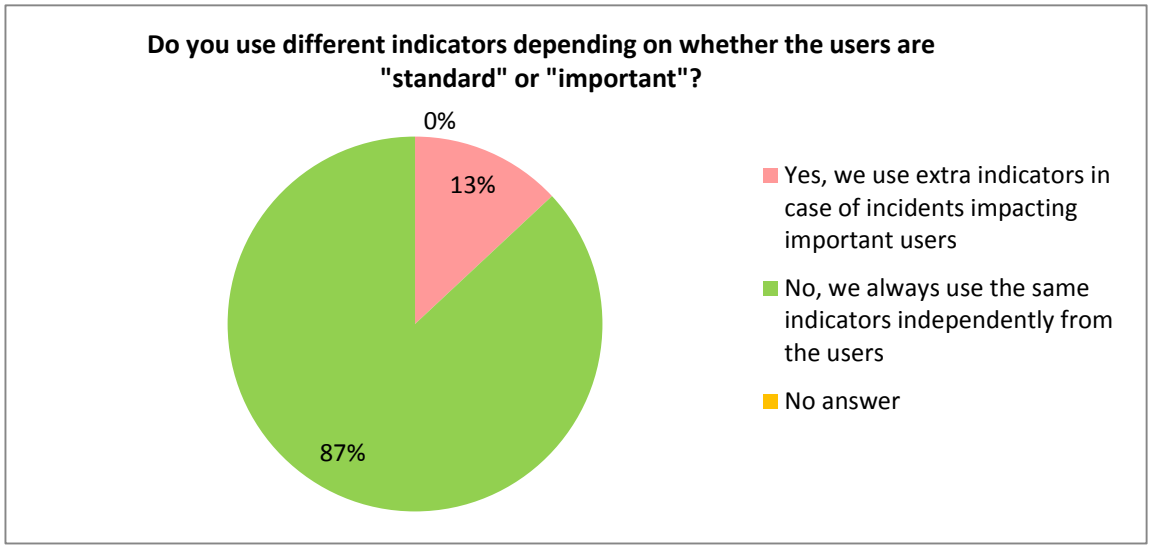
4.4 Assessing impact of incidents based on customer "importance"

Assessing the impact of an incident based on customer "importance" is another methodology which can be used mostly by providers.

From the viewpoint of the NRA, measuring incidents based on customer importance can service to the needs of high profile clients, or critical infrastructure clients who deal with sensitive information, such as banks, special government institutions, hospitals etc. Focusing on these clients can also help ensure greater security overall.

From the viewpoint of the provider, measuring security incidents based on customer importance has other merits, since this can help towards gaining customer loyalty and trust. Furthermore, doing so can improve the customer's perception of reliability with regards to the providers, thus resulting in competitive advantage and customer retention.

Figure 28: "Standard" vs "Important" clients – provider's view



However, measuring incidents based on customer importance is not so widely used among NRAs and providers. All 100% of the NRAs stated that a distinction between important and standard users was not made. Nevertheless, during interviews it was identified that most providers had a special group of customers, with whom either they held extra SLAs or who they knew is critical for them. For those customers, most providers, kept a more close watch and notified them should anything happen. This is especially true for critical infrastructures (banks, hospitals, etc.)

4.5 Assessing impact of incidents based on quality and service degradation

There are quite a lot of differing opinions on how to measure the impact of an incident based on quality and the degradation level of services. While at the moment, this indicator is not being used, the concept of service degradation and assessing the quality of a service remains important. That being said, clarification needs to be made surrounding the concept of what is considered "service degradation". For example, does this refer to the moment at which providers experience a loss in service to some of their systems (while others are still functioning), or is this the moment at which all services are completely unavailable. Furthermore, since service degradation can fluctuate, is this indicator calculated during the time period at which systems are facing service degradation or will this be later measured after the incident has occurred. Using the correct terminology can help providers and NRAs achieve more accuracy when measuring the impact of a security incident based on this indicator. This includes knowing how to differentiate between concepts such as "services failing", "services going down", "services affected", "total failure" and "services that are not working correctly" etc.

To summarize this point however, it is important to emphasise that technology is always changing, meaning that measurement methods which could seem appropriate at one point in time may not necessarily be so at another. The same is also true for service degradation in particular where in the future due to more advanced technologies, it may be the case that systems would not face total or complete loss of service, but rather periods of service degradation instead.

4.6 End-user requirements

End-users can play a vital role in the security incident reporting process as they are the ones who essentially make use of these infrastructures and services. Furthermore, bringing more transparency

into the process by informing end-users of the indicators used for measuring security incidents and also informing them of the incidents that have taken place, can be a beneficial approach. Empowering end-users with the necessary skills on incident identification and reporting could be an approach to be adopted, as suggested by some respondents.

So far, almost all providers report incidents to their NRAs only, while end-users do not have access to such information. To add to this point, end-users have to either specifically request for this information if they need it, or wait for the yearly reports from the NRAs or ENISA. However, the information that they receive will most likely be of past incidents that have occurred in the year, and therefore may not be so relevant to them anymore. Similarly, end-users many only find out about the incidents through the media.

Only one provider, who was interviewed, mentioned that apart from the yearly reports sent to the NRA, they already had in place another reporting process which was being used in parallel to ensure that end-users were also made aware of the security incidents. The majority however, stated that they had no direct interaction with their end-users whatsoever. Thus, the former can be seen as a potential area for further improvement and/or development. Working more closely with end-users can lead to gaining the trust of the customer and at the same time, further result in greater competitive advantage which is a key priority from the view point of the providers. However, as a provider, going public with details regarding incidents can be disadvantageous in certain situations (e.g. exposing a service/technology/infrastructure vulnerability which increases the appetite for attacks).

That being said, some end-users require more attention than others. These end-users include organizations such as banks that not only need to be informed immediately of the incidents but also have to have a contractual agreement with the providers, such as an SLA with which they may rely on the measurement of certain indicators like uptime etc. This is especially needed in the banking sector.

To summarize on this, further information has not been collected from the NRAs or from providers regarding the requests/satisfaction of end users on the specific matter of indicators.

5. Conclusions

The overall purpose of this document is to provide guidelines to national regulatory authorities (NRAs) and telecommunications providers within EU member states and to assist them in the process of measuring the impact of security incidents affecting the availability of electronic communication services. Therefore, interested stakeholders have at their disposal a catalogue of indicators to be used to tailor impact assessment and design the corresponding solutions.

A milestone in measuring the significance of incidents within the telecommunications sector in EU was set up along with the adoption of the Framework Directive (Directive 2009/140 EC) within the 2009 Telecom Package, which included Art. 13a. This article aims at ensuring the security and integrity of electronic communication networks and services in EU. 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.

Measuring the significance of telecommunications incidents became a necessity within the EU, and led to numerous debates between involved stakeholders. A lot of work has been done in this area both by ENISA, along with the Art. 13a expert group, and also by private or independent bodies, as some work is publicly available online. This report comes as a practical approach, and contains the view of both NRAs and providers within the EU, on real indicators used for measuring significance of incidents affecting the availability of telecommunication network and services.

As the survey performed had also the objective of analysing the approached taken by NRAs and providers in defining indicators and significance, the results indicated that while there are some discrepancies between NRAs and providers in terms of why they measure security incidents, and for what purpose they use certain indicators over others, it is still plausible to state that the ***approaches taken and indicators used by both parties are more similar than they are different***, as more than half of the respondents have stated this. Further developments regarding harmonisations of the approaches taken are still needed but overall the situation is running smoothly, the processes are in place, and the reporting of significant incidents is being done at national and EU level. From the study, it was realized that approaches taken by NRAs and providers varied depending on certain ***country-level factors***. Some were much more mature than others. Due to several advantageous circumstances, some NRAs experienced strong cooperation with their providers when it came to implementing the necessary changes.

Having said this, is it advised that making use of a standardized approach among NRAs and providers can help derive more precise results in the incident reporting process. So, the key recommendation from the study is that NRAs and providers should further increase the level of harmonisations in the approach taken to measure security incidents.

ENISA will continue to support the community through the Art. 13a group, and continue to provide best practices, guidelines and support for all stakeholders in members states.

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-04-15-917-EN-N

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

ISBN: 978-92-9204-156-4
DOI: 10.2824/887699