Technical Guideline on Reporting Incidents

Guidance on the incident reporting scheme in Article 13a

Version 1.0 – 2011-12-10

enisa

European Network and Information Security Agency

Contributors to this report

Authors: Dimitra Liveri, Daniele Catteddu, Lionel Dupré.
Peer Review: Dr. Marnix Dekker.

Agreements or Acknowledgements

For the completion of this report ENISA has worked closely with a working group of experts from national regulatory authorities and ministries from across Europe: PTS (SE), Ministry of Economic Affairs (NL), FICORA (FI), Ofcom (UK), ANACOM (PT), ComReg (IE), EETT (GR), ITST (DK), CPNI (UK), RTR (AT), ANCOM (RO), EA “ECNIS” (BG), ANSSI (FR), Bundesnetzagentur (DE), BIPT (BE), MITYC (ES), MPO (CZ), CERT LT (LT), MFSR(SK), ILR (LU), APEK (SI), MCA (MT), Ministry of Economic Development (IT), OCECPR (CY). We are grateful for their valuable input and comments.

About ENISA

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

Contact details

To contact ENISA, or to enquire about this document or about ENISA's activities regarding Article 13a, please email: resilience@enisa.europa.eu.

Contents

Guidance on the incident reporting scheme in Article 13a

1 Executive Summary

EU Directive 2009/140/EC amends existing directives on electronic communications networks and associated facilities (2002/19/EC, 2002/20/EC, 2002/21/EC). The directive, which had to be transposed to national legislation by the EU member states in May 2011, introduces Article13a on security and integrity of public communication networks. Paragraphs 1 and 2 of Article 13a say that providers of public communications networks should take measures to guarantee the security and integrity of these networks and to ensure continuity of services provided over these networks. Paragraph 3 of Article 13a says that providers should report significant security breaches and losses of integrity and that, annually, summary reports about significant incidents should be sent to ENISA and the EC.

In 2010, ENISA, the European Commission (EC), Ministries and Telecommunication National Regulatory Authorities (NRAs), initiated a series of meetings (workshops, conference calls) to achieve a harmonised implementation of Article 13a. In these meetings, a working group of representatives of both NRAs and the EC reached a consensus on two non-binding technical documents providing guidance to the NRAs in the member states: Technical guidelines for incident reporting (this document) and Technical guidelines for minimum security measures.

This document gives guidance to NRAs about the implementation of Article 13a and, in particular, the two types of incident reporting mentioned in Article 13a: the annual summary reporting of significant incidents to ENISA and the EC and ad hoc notification of incidents to other NRAs in case of cross-border incidents. This document defines the scope of incident reporting, the incident parameters and thresholds. This document also contains a reporting template for submitting incident reports to ENISA and the EC, and it explains how the incident reports will be processed by ENISA.

The directive also asks NRAs to implement national incident reporting schemes for electronic communication services and network providers in their constituency. There is diversity between the different member states in this respect; some have already have established (in a few cases for several years) a well-functioning scheme, while others are still in the initial stage of deployment. This document does not go into details about how NRAs can design and implement national incident reporting schemes, but it does, by providing a single definition of incident parameters and thresholds, provide a baseline also for these national schemes.

The meetings of the working group will continue beyond the publication of the documents, to further support harmonised implementation of Article13a across the EU.

2 Introduction

In this document, we provide guidance to NRAs on implementing Article 13a and in particular the obligations of undertakings to report incidents.

This document has been drafted by a working group comprising NRAs and representatives of the EC, supported by ENISA (see preface). This document is not binding and is published by ENISA to provide guidance to NRAs on the technical aspects of implementing Article 13a.

2.1 Article13a

As a reference, we reproduce below the text of paragraph 3.

> *"3. Member States shall ensure that undertakings providing public communications networks or publicly available electronic communications services notify the competent national regulatory authority of a breach of security or loss of integrity that has had a significant impact on the operation of networks or services.*
>
> *Where appropriate, the national regulatory authority concerned shall inform the national regulatory authorities in other Member States and the European Network and Information Security Agency (ENISA). The national regulatory authority concerned may inform the public or require the undertakings to do so, where it determines that disclosure of the breach is in the public interest.*
>
> *Once a year, the national regulatory authority concerned shall submit a summary report to the Commission and ENISA on the notifications received and the action taken in accordance with this paragraph. "*

ENISA will establish a reporting scheme for NRAs' annual summary report to ENISA and the EC that is consistent with the national breach reporting schemes.

1. Article13a introduces three types of incident reporting: The notification from providers to NRAs;

   "Member States shall ensure that undertakings providing public communications networks or publicly available electronic communications services notify the competent national regulatory authority of a breach of security or loss of integrity that has had a significant impact for the operation of networks or services." [Article 13a §3]

2. The annual summary report from an NRA to the EC and ENISA, which is also depicted in Figure 1, is referred:

   "Once a year, the national regulatory authority concerned shall submit a summary report to the Commission and ENISA on the notifications received and the action taken in accordance with this paragraph". [Article 13a §3]

3. The ad hoc notification of incidents between NRAs and to ENISA, which is depicted in Figure 2, is referred to:

   "Where appropriate, the national regulatory authority concerned shall inform the national regulatory authorities in other Member States and ENISA. The national regulatory authority concerned may inform the public or require the undertakings to do so, where it determines that disclosure of the breach is in the public interest." [Article 13a §3]

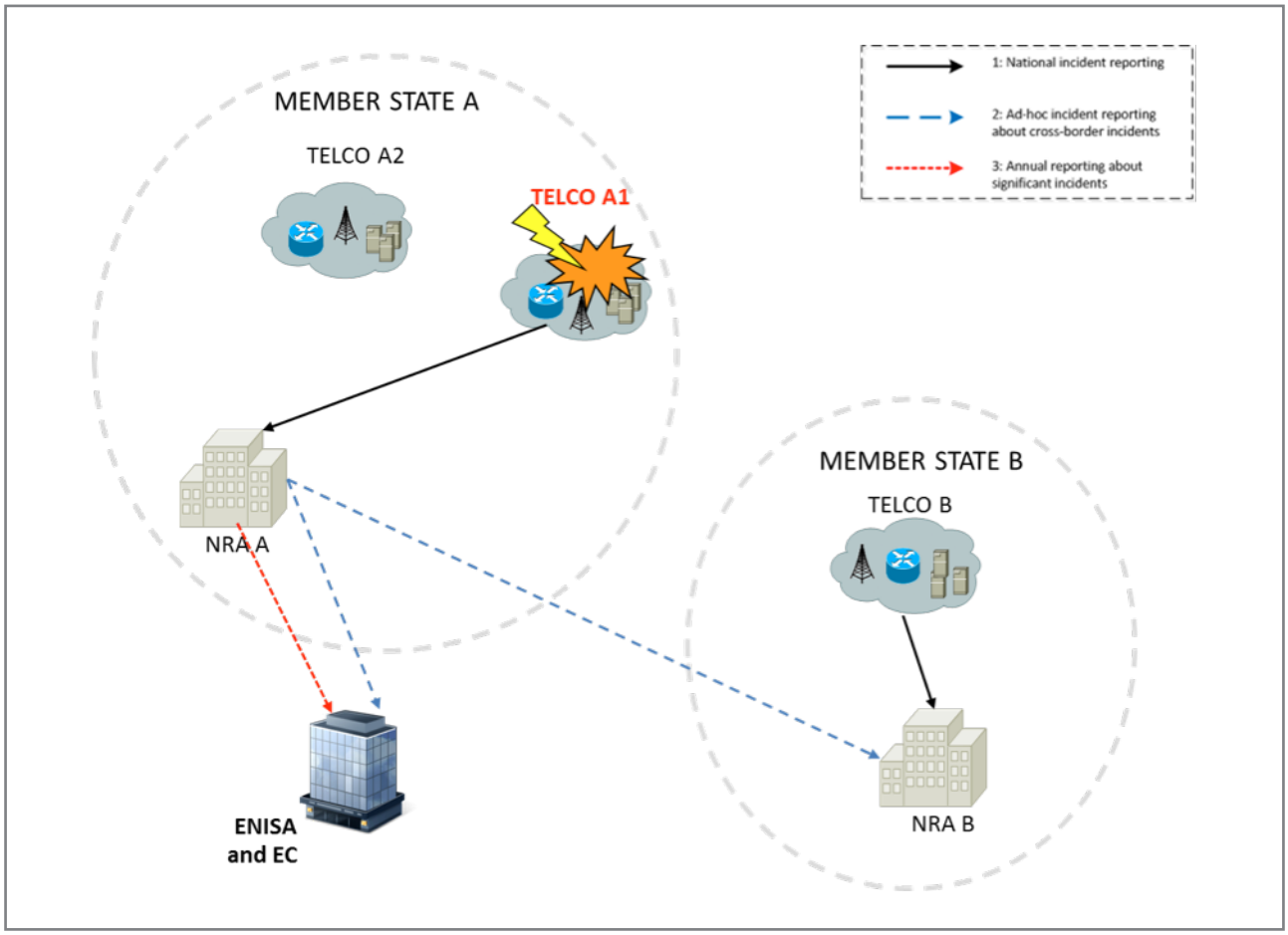

Figure 1 Reporting schemes of Article13a

The first notification scheme between operators/providers and NRAs is outside the scope of this document;

The current document deals with, and analyses the second and refers to the third type of reporting scheme. A reference to the notification of incidents both between NRAs and to ENISA (ad hoc notification) is proposed, but the implementation details will be decided at a later stage. ENISA currently drafts a contacts' list for the facilitation of the ad hoc notification procedure.

2.2 Role of ENISA under Directive 2009/140

- ENISA is mentioned numerous times in Directive 2009/140. ENISA is asked to contribute to enhancing the level of security of electronic communications by, among other things, "providing expertise and advice, and promoting the exchange of best practice".
- The Directive also explains that, should the European Commission adopt appropriate technical implementing measures with a view to harmonising the measures referred to in paragraphs 1, 2, and 3 of article 13a, then ENISA would contribute to the harmonisation process with expert advice on those measures. The Commission will take the outmost account of the opinion of ENISA.
- Once a year all NRAs shall submit to both the EC and ENISA a summary report on the notifications received and the actions taken in accordance to paragraph 3 of Article 13a.

In this context, the reporting of incidents plays an important role in enhancing the security and resilience of communications networks. In particular, it contributes to ensuring:

- Access to a wide pool of expertise about such breaches or losses,
- That national authorities can propose and enforce follow-up actions with networks and services providers in their capacity of regulators,
- The analysis of threats and vulnerabilities,
- The identification of good practice, based on lessons learned in the incident management process.

2.3 Wider policy context

The European Union's institutions have recognised the importance of public electronic communications and the need to expand efforts to ensure their resilience.

- In 2006, the EC issued a communication on A Strategy for a Secure Information Society – Dialogue, Partnership and Empowerment (COM (2006) 251[1]), which was endorsed the following year by the Council (Council Resolution 2007/068/01[2]). One of the main actions announced in the strategy was a multi-stakeholder dialogue on the security and resilience of networks and information systems as the Information and Communication Technology (ICT) sector-specific approach within the overall European Programme for Critical Infrastructure Protection[3] (EPCIP) that was adopted by the EC at the end of 2006.

[1] http://eur-lex.europa.eu/LexUriServ/site/en/com/2006/com2006_0251en01.pdf
[2] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0149:FIN:EN:HTML
[3] http://europa.eu/legislation_summaries/justice_freedom_security/fight_against_terrorism/l33260_en.htm

• In 2008, ENISA published a report analysing the policies and regulations status across Europe providing policy recommendations. There incident reporting is mentioned for the first time as a recommendation for the MSs to follow and the EC to provide assistance to.

• The EC further adopted, in March 2009, a communications and action plan on Critical Information Infrastructure Protection (CIIP), called Protecting Europe from Large Scale Cyber-Attacks and Disruptions: Enhancing Preparedness, Security and Resilience (COM (2009) 149[4]). This communication focuses on "prevention, preparedness, and awareness" and defines an immediate action plan to strengthen the security and resilience of CIIs.

• The Council Conclusion on CIIP on May 2011[5], taking stock of the results achieved since the adoption of the CIIP action plan in 2009, launched to strengthen the security and resilience of vital Information and Communication Technology Infrastructures.

[4] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0149:FIN:EN:PDF
[5] http://register.consilium.europa.eu/pdf/en/11/st10/st10299.en11.pdf

3 Incident reporting scheme

In this section we describe the objectives of the reporting scheme and the steps of the overall reporting scheme.

3.1 Objectives

The objective is to put in place an incident reporting scheme for collecting annual reports and an ad hoc notification scheme for incidents with cross-border relevance (i.e. where appropriate, the NRA concerned shall inform the NRA in other Member States and ENISA). The aim of the collaboration between ENISA and NRAs was to find a baseline that could be adopted as a foundation by all and create a framework through which the different NRAs would communicate in a common language with each other, and also with ENISA and the EC.

The collected data will be used by ENISA to:

1. Inform NRAs and relevant EU institutions about:
   - Incidents that have significant impact.
   - Root causes of security breaches and losses of integrity.
   - Lessons learned from the detection, response and recovery measures taken both during and after the incident by providers and competent MS authorities
2. Support the knowledge transfer between NRAs, based on their internal experience and lessons learned, and between providers.
3. Understand the impact of incidents on interconnections (including the understanding of the impact of weakest link failures).
4. Develop possible incident scenarios to be used for future pan-European exercises.
5. Issue recommendations to private sector and policy makers.
6. Analyse the suitability of any relevant good practice being followed and make changes.
7. Understand possible future trends.

A reporting scheme is a set of agreed rules, established procedures and actions taken that create an incident reporting mechanism. The key elements of an effective and efficient reporting scheme are:

✓ Clear definition of the categories of root causes, the reason why the incident occurred.

✓ The reporting template, whose fields must be well defined and easily understood.

✓ The criteria/parameters taken into account when reporting an incident.

✓ The thresholds to be used to evaluate the significance of the incident and "trigger" the reporting mechanism.

The procedures of the 'incidents reporting scheme' are summarised in the following steps (i.e. a sequence of actions the NRA should execute for each incident reported by the Telco):

1. Assess the impact of the incident; did it affect a service which is in the scope of Article13a and does the incident fall under the scope of the reporting.
2. Determine if the incident is significant; according to the parameters and thresholds set, does this incident trigger the reporting scheme?
3. Submit the report

In detail:

Step 1: The first step is to determine whether the incident falls under the scope of reporting. The scope of incident reporting is described in section 3.1 followed by the list of electronic communication networks and services under this scope, as described in section 3.2.

Step 2: the next step is to determine if the incident is significant and if it triggers reporting. This is done by using parameters, section 4.1, and thresholds, section 4.2.

Step 3: Additional information should be gathered in order to fill in the report accordingly, i.e. the root cause of the incident. A categorisation of root causes is provided in these guidelines, and a list can be found in chapter 5. We provide the reporting template and the reporting process in section 6.1 and section 6.2. More information on the confidentiality of the content of the incidents report you can find is section 6.3. The objective of this standardised 'incident reporting template' is to make sure that the information sent from NRAs to the EC and ENISA is of the same type and in the same format.

4 Defining the scope

In this section we define the scope of the reporting scheme, including the services which are covered by the technical guideline as agreed with the working group.

4.1 Scope of incident reporting

Under Article 13a the scope of the reporting scheme is described as follows:

"…breach of security or loss of integrity that has had a significant impact on the operation of networks or services."

In this document we used the following working definition of an incident:

> Incident is herein defined as an event which can cause a breach of security or a loss of integrity of electronic communication networks or services.
>
> Reportable Incident: A breach of security or a loss of integrity that has a significant impact on the operation of electronic telecommunications networks and services.

For the initial period, ENISA and the NRAs working group decided to focus the initial technical orientation of the incident reporting and notification scheme on the scope described below; its scope might be broadened in the light of experience gained.

> "Network and Information security incidents having a significant impact on the continuity of supply of electronic communications networks or services."

Note that in general, considerations about the criticality of an infrastructure served by a telecommunications provider will not be part of the scope of the reporting to ENISA (the rationale being that Critical Infrastructure and Critical Information Infrastructure are not subject to the Regulatory Framework for electronic communications).

For the purpose of reporting we consider that the form of incident that is to be reported may be triggered by issues of security or integrity but the context of the document is to address service impacts howsoever caused. Operators and NRAs do not need to focus on the difference between a lack of security or/and a lack of integrity as this will be assessed to the extent necessary when NRAs and ENISA consider the root cause analysis.

4.2 Non-exhaustive list of electronic communications services[6]

In this section we give guidance by providing by way of example a non- exhaustive list of the services that should be considered in scope. Definitions are based on the ETSI Terms and Definitions Database Interactive (http://webapp.etsi.org/Teddi/).

Service	Platform
Telephony / Voice	The network supports communication for voice. Examples of platforms : fixed, mobile, broadcast etc.
Data: service that comprises a non-audio primary service component and, optionally, additional secondary service components	**Internet** A worldwide interconnection of individual networks a) with an agreement on how to talk to each other, and b) operated by government, industry, academia, and private parties.
	(Short) Message Services A service in mobile telephony systems that allows the user to send and receive messages independently of voice calls; a nearly real-time service that stores messages in message centres if the receiving mobile telephone cannot be contacted
	Email Service: messages automatically passed from one computer user to another, often through computer networks and/or via modems over telephone lines.

Figure 2. Electronic Communication Services

Note that, as stated already, this is not an exhaustive list of assets. It is at the discretion of the NRA to provide a definitive list for the networks/services under its jurisdiction.

[6] Definitions are based on the ETSI Terms and Definitions Database Interactive: http://webapp.etsi.org/Teddi/

5 Impact parameters and thresholds

In this section we describe the parameters and thresholds that qualify the significant impact of the incident and trigger whether it should be reported.

We used the following set of requirements for the definition of incident reporting thresholds:

- The procedure for determining the significance of an incident (use of parameters and thresholds) should be kept simple and allow a certain level of flexibility.
- Practical aspects should be taken into account, e.g. the number of incidents to report.
- The significance of a disruption should be measured against its impact on end-users and interconnected networks.
- At national level, the definition of the significance of an event should not be left to the discretion of the telecom operators; this should be defined by the competent regulatory authority.
- a report should be triggered only by the absolute number of end-users impacted, not a percentage, to ensure equal treatment of all EU citizens.
- Percentages should be translated into fixed figures, taking into account the population per country and adjusting the numbers according to the size of the country.

5.1 Parameters

In this paragraph we identify and describe the parameters[7] that should be used by NRAs to determine the significance of the impact of an incident. The four parameters are:

- Number of users affected
- Duration of incident
- Geographic spread/region
- Impact on emergency calls

5.1.1 Definitions of parameters

1. Number of users affected: This parameter concerns the percentage of a MS's total users of a service (see figure 2) which were affected by the incident (e.g. 10% of the end-users of fixed network telephony/voice in MS X). For the end-users of mobile telephony services the number is an estimate, based on the report from the

[7] [Rec. ITU-T E.800] A quantifiable characteristic of a service with specified scope and boundaries

provider. The totality of users refers to the total national users of the specific service.

The reporting mechanism is triggered whenever an incident affecting a pre-established percentage of users (of a specific service) takes place.

In order to properly assess the number of affected users we addressed subsidiary issues: in the prior analysis the difference between 'service users' and 'service reseller[8]' occurred and further clarifications were required. Usually electronic communications operators and service providers are aware of the percentage of end-users whose services are provided via a reseller. In the context of Article13a, only the number of affected end-users (or 'clients' as they are referred to in the Directive) is relevant; the term "reseller" refers to the intermediate user, not the end-user.

It should be noted that this parameter is purely quantitative (% of users affected) and it will not take into consideration the types of users affected. In other words, the weight assigned to each user is the same and there is no distinction between, for instance, a home user, bank or hospital.

2. Duration of the Incident: This parameter concerns the duration of the incident. The time can be measured in minutes, hours, or days etc.; e.g. the disruption of services could last for 1 hour. The duration of the incident is the time span between when the service starts to degrade and when the service is available again to the end-user, or simply the length of time the end-user was unable to use the service. This parameter will be used to judge if the incident reported by the electronic communications provider or operator should be reported to ENISA. The exact duration of the incident is not included in the reporting template.

3. Geographic spread/region: this parameter concerns the area impacted when the incident happened. In a major incident a whole region can be affected. The impact is different, depending on the geographic spread/ region and on the density of population, e.g. "the incident affected the area of region X". This metric can be additionally displayed as a percentage of the country. NRAs may consider that some geographic regions, such as islands within its territories, should have special thresholds applied with appropriate geographic reporting. This will be a matter for individual NRAs to consider. Each NRAs should assess the according areas in the country according to the density of the population and the services available. In a given country, the criteria for defining a rural area must be common to all operators. Furthermore, in some scenarios an operator can identify the areas and/or % of the country that is affected, based on the sum of impacted network nodes and its interconnections. However this is en estimation and not a perfectly delimited area.

4. Impact on emergency calls: This parameter signifies an incident as having an impact on calls to emergency numbers (e.g. 112) and therefore affecting the continuity of these services. This can be a stand-alone parameter meaning that if an incident impacts on

[8] A "reseller" is a provider who purchases electronic communications services from another electronic communications service provider and then resells them to end-users as a component part of the purchased services, or integrates them into a mobile telecommunications service. Source: http://apps.leg.wa.gov/rcw/default.aspx?cite=82.04.065

emergency calls, the reporting scheme is triggered regardless of the duration or users affected. We use this parameter to address network connectivity to emergency services and 112/999 call centres (where this is under the scope of the NRA).

5.2 Thresholds

An incident should be reported to ENISA every time the impact is equal to, or higher than, a set of predefined thresholds agreed between ENISA and NRAs. In this section we define the thresholds.

The thresholds in this section are intended to define what, as a minimum, should be considered by NRAs as 'an incident with significant impact'. Based on these thresholds, NRAs can introduce a more detailed set of thresholds in their own countries. As already mentioned above, the thresholds defined are intended as a minimum entry level and each NRA is free to impose stricter and more granular thresholds to trigger the reporting at national level e.g. the geographic characteristics of each country. However, the same thresholds will be used to trigger the process of reporting to ENISA.

The reporting from NRAs to ENISA should be done according to the thresholds defined by ENISA. The reporting of incidents below the thresholds should only be performed when the incident requires specific attention, especially at EU level. At the same time, NRAs have to report to ENISA every incident whose impact is above the level agreed in the thresholds. The respective NRAs will have to select, from the total incidents collected throughout the year, those incidents that trigger the thresholds defined in these guidelines and report them to ENISA.

The same thresholds apply regardless of the number of providers affected by the incident.

The four reporting parameters, as mentioned in the previous paragraph, can be used for the purpose of the reporting, either as a single criterion (e.g. 'the telephone service in a large area like Sardinia or Corsica has gone down') or as a combination of two or more of them (e.g. '10% of the total number of users of a voice communication service affected for 8 hours').

Stand-alone

NRAs have to report to ENISA every incident whose impact is above the level agreed in the thresholds, which are described below:

1. **Number of users affected:** If an incident occurs which affects more than 15% of the total number of users of service or network, then this should be included in the annual reporting to ENISA.
2. **Duration of the incident:** If an incident affects the availability or continuity of a service or network for more than 4 hours, then this should be included in the annual reporting to ENISA.
3. **Geographic spread/ region:** this parameter can be used as stand- alone only in certain circumstances such as when an incident affects a designated area like Scot-

land, Sicily, Canary Islands (island, designated region etc). In any other case it will be considered as a combined parameter.

4. Emergency calls: this parameter is considered as stand-alone only; if a disruption occurs which makes the service unavailable regardless of duration, to the affected users or the geographic spread/ region, it should be reported to ENISA and the EC.

Combination

In some cases the incident is considered after assessing its impact measuring two parameters. In this cases talk about combination of parameters and the thresholds are therefore different. Three distinct cases are analysed below. Keep in mind that the parameter of emergency calls is always a stand-alone parameter and thus not included in the combined parameters.

Case 1: Number of users affected and duration of the incident

NRAs should report to ENISA every incident that has the following characteristics:

- ❑ In the figure below the HIGH (red) impact area, according to the scale proposed, in which is described as a combination of the percentage of affected users and service downtime (incident duration). Incidents falling in this area should be reported.

	1h<...<2h	2h<...<4h	4h<...<6h	6h<...<8h	>8h
1%<...< 2% of users					
2% < ...< 5% of users					
5% <...< 10% of users					
10% <...<15% of users					
> 15% of users					

Table 1 Combination of thresholds

Case 2: Number of users affected and geographic spread/ region

NRAs should report to ENISA every incident that has the following characteristics:

- ❑ Making an electronic communications service or network unavailable in a rural area affecting more than 10% of the total number of users who are the main targets in this specific area.

Case 3: Duration of the incident and geographic spread/ region

NRAs should report to ENISA every incident that has the following characteristics:

❑ Making an electronic communications service or network in a rural area unavailable for more than 4 hours.

It should be noted that each NRA will autonomously define:

❑ The conditions under which the unavailability of emergency calls represents an incident with a significant impact.

❑ The areas in the respective country that should be considered as 'rural' (mountain areas, islands, etc.).

Thresholds – Ad hoc notification from NRA to NRA and to ENISA

In cases of cross boarder incidents, the NRA concerned shall inform the NRAs in other MSs and ENISA. The NRA in cases of great incidents which affect public electronic communication services/networks of another provider should in prompt time send a notification to the NRA concerned and ENISA. For example in cases of large-scale phenomena, such as thunderstorms, earthquakes or power cuts, more than one operator in more than one country could be affected. The NRA will assess if these incidents should be included in the annual report.

The same template can be used for the ad hoc notification which can be sent to ENISA and the NRAs via email.

In light of this as a minimum, NRAs alert their counterparts:

- When there is an incident which, by its nature, is likely to affect other MSs, i.e.:

  ❑ The root cause of the incident.

  ❑ The affected assets or services, or

  ❑ The action taken to mitigate or resolve the incident, clearly spans the borders of two or more NRAs)

ENISA will establish a list of relevant points of contact in competent NRAs with the objective of facilitating the exchange of information between NRAs, the EC and ENISA. By the end of 2011, all the NRAs will be asked to update this list with the relevant NRA contact points. This list will be disseminated to the relevant stakeholders and periodically updated.

6 Root cause of an incident

In this chapter contains the categorisation of root causes.

The classification of the root causes of an incident, as described in this section, is based on the following document:

1. Explanatory notes to Regulation 9 on the obligation to notify violations of information security in public telecommunications, published by FICORA[9].

2. Security Procedures - Telecommunication Systems and Services, issued by CESG, the UK National Technical Authority for Information Assurance.

We distinguish 5 categories of root causes (see figure 4) which are described below. These root causes are used to categorize the incidents which are reported annually to ENISA and the EC. The root cause classification could be used by NRAs in their national reporting.

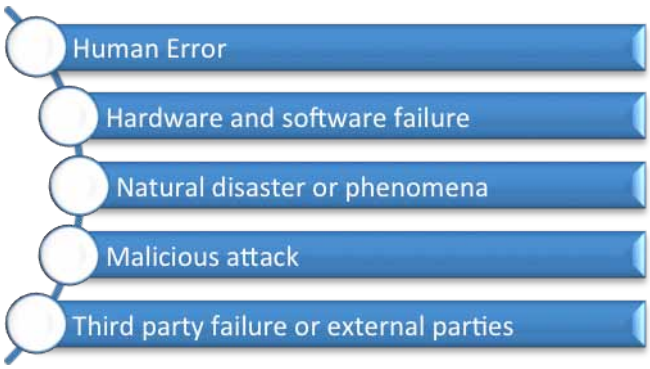

Figure 3 Categories of Root Cause

The list includes root causes which could result in a breach of security or loss of integrity. Below we explain the different categories of root causes and give examples.

The two categories of 'human error' and 'hardware and software failure' are related to internal processes and assets, while the 'external parties' category covers human errors or failures derived from external causes.

One incident might be the result of multiple root causes. For example, a common cause of disruption is loss of power, and loss of power is commonly due to bad weather; any further complications should be pointed out. To some extent, the effects of a major power loss can be mitigated by the use of a UPS (uninterruptible power source) or diesel standby generator. This kind of incident can be categorised as having both a 'natural disaster/phenomenon' as its root cause and 'human error', due e.g. to poor implementation of the recovery plan.

[9] http://www.ficora.fi/attachments/englantiav/5k8yJAS9R/FICORA07B2009M.pdf Note that the Finnish document has a legal background framework provided by the privacy directive. This document was used as the main source of inspiration for the classification of incident root causes, because Finland is the first EU MS with a mandatory incident reporting scheme in the electronic communications sector.

Natural Disasters or Phenomena

This category involves incidents caused by natural disasters or phenomena, such as:

- Severe weather (e.g. storms, heavy snowfall, heat wave),
- Earthquakes
- Tsunamis
- Pandemic diseases
- Floods
- Fire
- Landslides
- Volcanic eruptions

> **Example of an incident within the scope of this technical guideline for reporting security incidents:** An earthquake is causing disruption to fixed electronic communication networks, affecting30% of subscribers for 5 hours.
>
> The reported root cause would be 'natural disaster'.

Malicious Attack

This describes a person or programme gaining logical or physical access, without permission, to a network, system, application, data or other IT resources. Such a breach may be the result of a targeted attack, and could originate from either an inside or outside threat.

The root causes included in this category are divided in two sub-categories: 'Logical Security Attacks' and 'Physical Security Attacks:

1. Logical Security Attacks

- Unauthorised logical access to:
  - Network devices
  - Platforms
  - Applications (software)
  - Backups
  - Databases
  - Sensitive data (identification, customer and configuration data, network documentation data, traffic and location data or descriptions of structure, etc).

- ❑ Unauthorised use of elevated privileges (privilege escalation from external user, privilege escalation from internal user, identity theft, social engineering attacks);
- ❑ Taping and monitoring devices, installations and software in the communications network or in the information systems or facilities of the telecom operator (this activity does not directly result in a compromise or denial of service);
- ❑ Loss of data affecting the security of the network, infrastructure or systems;
- ❑ Alteration of critical system files or data as well as service data;
- ❑ Tampering with security controls;
- ❑ Successful hostile log-ins into the information systems of telecom operators;
- ❑ Traffic misrouteing and re- routeing (e.g. corruption of network traffic routeing tables)
- ❑ Malware spreading (e.g. computer viruses, back-door installation programs, Trojans, spyware or sniffer programs that affect the operating system) in the telecom operator's information systems;
- ❑ Denial-of-service attacks (DoS) or Distributed DoS;
- ❑ Sudden increase of traffic (spam, targeted attacks, etc);
- ❑ Exploitation of software and hardware vulnerabilities.

2. Physical Security

- Unauthorised physical access:
  - ❑ Accessing system hardware and making unauthorised changes;
  - ❑ Physical break-ins to information systems' premises.
- Theft of equipment or media.

Example of an incident within the scope of this technical guideline for reporting security incidents: A DoS attack on an electronic communications system is causing disruption to a communications service affecting 40%) of end-users (malicious attack against logical security).

The reported root cause would be 'malicious attack'.

Example of an incident within the scope of this technical guideline for reporting security incidents: Theft of copper cables belonging to an electronic communications provider is causing a lack of continuity of communications services affecting 30% of subscribers (malicious attack against physical security).

The reported root cause would be 'malicious attack'.

Human Error (internally caused)

This category involves incidents caused by human error by internal staff.

- Misconfiguration or mis-deployment of:
- Network devices
- Platforms
- Applications (software)
- Backups
- Databases.
- Erroneous application of procedures:
- Configuration management procedures
- Change management procedures
- ID and Access control management procedures
- Incident in management procedures.

> **Example of an incident within the scope of this technical guideline for reporting security incidents:** An electronic communications system configured incorrectly by a staff member is causing the outage of a telecommunication service affecting 60% of subscribers.
>
> The reported root cause would be 'human error'

Hardware – Software Failure

- Faults in the hardware
- Faults or bugs in the software.

> **Example of an incident within the scope of this technical guideline for reporting security incidents:** Failure of equipment due to wear is causing disruption to a telecommunication services affecting 60% of subscribers.
>
> The reported root cause would be 'hardware failure'

Third Party Failure/External Parties

- Human error caused by an external party (e.g. cable cut by excavation machine).
- External procedure failure affecting internal process.
- Faults in the supply chain.

Example of an incident within the scope of this technical guideline for reporting security incidents: A cable is cut due to excavation operations in the area, causing disruption to telecommunications services affecting 60% of subscribers.

The reported root cause would be 'external party error'

7 Reporting template and reporting channels

In this section the reporting form and the procedure to submit it are described

7.1 Reporting Template

This is the report the MS will submit to ENISA annually, describing each major incident. In the case of ad hoc notification the competent authorities may use the same template if they find it appropriate.

Article 13a Incident Reporting Form
Country:
Date and time:
Incident impact and root cause
Impacted services (select one or more): **Fixed telephony** ☐ **Mobile telephony** ☐ **(Short) Message Services** ☐ **Internet** ☐ **Email** ☐
Impact parameters (fill in as appropriate): **Number of users affected:** **Duration:** **Geographic spread/region:** **Impact on emergency calls:**
Further details about the impact:
Root cause (select one or more): **Natural disaster or phenomena** ☐ **Human error** ☐ **Malicious attack** ☐ **Hardware or software failure** ☐ **Failure at third party or external party** ☐

Further details about the root cause:
Other incident information
General description:
Incident handling and response actions:
Post incident actions:
Interconnections affected:
NRA's contacted (in case of a cross-border incident):
Lessons learnt:
Further remarks:

Description of template fields

Country	
Description:	The country that sends the report to ENISA.
Date and time	
Description:	Details of the date and time when the incident took place (in national time). It can be interpreted as the time the incident was discovered. Time should be expressed in both CET and local time.
Impacted Services	
Description:	The affected service: the service rendered unavailable to the end-user. This field includes a description of the service whose continuity and availability are affected by the impact level. It should be noted that assessing the LoS (Level of Service) and QoS (Quality of Service) introduces complexity into the analysis criteria and can become subjective.
Incident parameters	
Number of users affected	The total number of users affected when an incident occurs. (% of all users of that service in a given country). The national report to the NRA may include absolute number which the NRA would have to translate to percentages for inclusion in the annual report to ENISA and the EC.
Duration	The duration of the incident
Geographic spread/region	If available the region impacted by the incident.
Emergency calls	If available emergency service impacted by the incident.

Further details about the impact	
Description:	Fill in any further information you can share of the impact of the incident.
Root Cause	
Description:	The initial cause of the incident (human error, malicious attack etc)
Further details about the root cause	
Description:	The incidents to be reported should focus on network integrity and service continuity. These could be sub-categories of the root causes listed in the relevant section.
Incident handling and response actions	
Description:	All the actions taken after the discovery of the incident and the measures adopted to restore the service to its initial conditions/level.
Post incident actions	
Description:	Should include a description of any arrangements that were made to minimise the level of risk.
Affected Interconnections	
Description:	If the affected service can cause damage/change to an asset (or service) belonging to another operator or provider, then this is an affected interconnection. In cases of cross-border incidents, it might be possible that a security breach in one MS affects the assets of another 'interconnected' MS. Some concentrations of infrastructure are vulnerable, and significant disruption can be caused by localised failure; interconnected systems can be subject to cascading technical failures.
NRAs contacted	
Description:	The competent NRAs in other countries that were notified about the occurrence of the incident. If authorities from other NRAs or third countries are involved in the response action, they should be mentioned as well.
Lessons learnt	
Description:	Describe any actions that were taken after the incident to improve the security of the asset and the procedures that will be followed (or measures taken) from then on. The difference between this field and the field of "Post Incidents measures" is that in this field we refer to long-term actions.

7.2 Reporting Channel

The annual summary report of significant incidents can be submitted via two channels:

- Web-based form
- Email

For the annual summary report to be sent to ENISA the reporting template will be implemented as a web form in the Article13a portal, in an area where access will be granted only for the people in the contacts list. Usage of traffic light protocol is recommended (see annex 3).
ENISA will also publish a contact list with email addresses and phone numbers of points of contact in competent NRAs in Europe. This will facilitate communication between ENISA and all the NRAs in Europe. This list will also include the relevant contact points from ENISA and the EC.

7.3 Confidentiality of incidents report

Providers can object in the disclosure of the incidents' report. Confidentiality of incident reports is covered in in Art. 5(3) of Directive 2002/21: "Where information is considered confidential by a national regulatory authority in accordance with Community and national rules on business confidentiality, the Commission and the national regulatory authorities concerned shall ensure such confidentiality."
Where the information might be sensitive with regard to national security, an adequate framework can be found in Article 4. of Regulation 1049/2001 regarding public access to European Parliament, Council and Commission documents[10]. This Regulation is particularly relevant because of the exceptions provided in Article 4, paragraph 1, which reads as follows:
"1. The institutions shall refuse access to a document where disclosure would undermine the protection of:
(a) the public interest as regards:
— public security, […]"
In line with this provision NRAs may:

- Request the institutions not to disclose a document originating from that Member State without prior agreement[11] (Art.4 (5)).
- Indicate, when consulted by the EC/ENISA, that the information comprised in the notification is important for public security.
- Art.4 (4)). It needs to be noted that both the EC and ENISA[12] have an obligation to consult the third party[13] from which a given document originates with a view to assessing whether the exceptions to access to the document should be applied).[14]

In light of the above, the EC and ENISA will acknowledge any indication by the MS that an incident report should be treated as confidential.

[10] REGULATION (EC) No 1049/2001 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 30 May 2001 regarding public access to European Parliament, Council and Commission documents (OJ L145/43, 31.5.2001).

[11] Art.4(5) of Regulation 1049/2001: 1. The institutions shall refuse access to a document where disclosure would undermine the protection of (a) the public interest as regards: — public security."

[12] Recital 8 of Regulation 1049/2001 says that: "In order to ensure the full application of this Regulation to all activities of the Union, all agencies established by the institutions should apply the principles laid down in this Regulation".

[13] Art. 3(b) defines a 'third party' as any natural or legal person, or any entity outside the institution concerned, including the Member States.

[14] Art. 4(4) pf Regulation 1049/2001: " […] a Member State may request the institution not to disclose a document originating from that Member State without its prior agreement".

8 ENISA's annual report

The reports of significant incidents will be used by ENISA to publish an annual report, for the purposes of:

1) Drafting an annual report on the status of electronic communications with regard to security, integrity and continuity of service.

2) Issuing recommendations, advice and good practice on:

a. 'Incident Collection', i.e. how to improve the incidents reporting scheme in NRAs and how to improve information sharing between NRAs, the EC, ENISA and the private sector, issuing good practices on how to analyse the information gathered from the incidents and on the benefit driven of this analysis.

b. 'Incidents Management', i.e. how to maximize the value of the lessons learnt at national and EU level in the Incident Management process, such as the creation of benchmarks for the incident management process, etc.

c. Preventive actions, investments, research funding, identification of incentives for the market, etc.

3) Creation of statistical analysis series.

Depending on the quality and quantity of the reports received by the end of the reporting period the annual report might include, together with other information, the following:

- Which were the most common breaches?
- Which are the most common root causes of incidents?
- Service vulnerabilities: Which services are the most affected?
- Common threats: What is the most common root cause for incidents affecting a specific service? (e.g. The most common root causes affecting fixed telephony are natural phenomena).
- Trend analysis: The percentage of affected users in Europe each year and of affected types of services per year. (What are the trends in Europe?).
- Attack analysis: Where incidents are caused by a malicious attack, how can these attacks be characterised? If compared with attacks collected in previous years, what differences can be highlighted? (more sophisticated, more targeted, a combination of several methods, not easy to detect, etc)
- Common time framework: Incidents time distribution (when most of the incidents happened in Europe?)
- Mapping of attack profiles (scan, probe, worms, DoS, spam etc.)

- Interconnections affected: In the case of an incident, how do the interconnections work? How does one service affect the other? Create a map of interconnections at both national and pan-European levels?
- Impact escalation: Which category of assets, if affected, can make a greater impact on the service, and why?
- What are the conclusions, after analysing the time to restore from 'incident' to 'incident' by classification and type of service?
- What is the mean time for restoring service levels?

Note

This report will not include any direct comparison between NRAs. So information such as the following (non- exhaustive list), will not form part of the annual report published by ENISA:

- Number of incidents per country,
- Average impact per incident in country X,
- Mean time to discovery of incidents in country X,
- Mean time to recovery in country X,
- Name of operators or providers,

9 Glossary

The NRAs may use other established definitions when and where appropriate.

Attack [b-ITU-T H.235.0]: The activities undertaken to bypass or exploit deficiencies in a system's security mechanisms. By attacking a system directly, they exploit deficiencies in the underlying algorithms, principles, or properties of a security mechanism. Indirect attacks are performed when they bypass the mechanism, or when they make the system use the mechanism incorrectly.

Availability ([ITU-T E.802]: Availability of an item so that it is in a state to perform a required function at a given, or any, instant of time within a given time interval, assuming that the external resources, if required, are provided.

Consumer [Directive 2002/21/EC]: Any natural person who uses or requests a publicly available electronic communications service for purposes which are outside his or her trade, business or profession.

Disaster recovery/business continuity [Rec. ITU-T E.800]: All activities associated with the restoration of a network-provided service after a disaster. Examples of such disasters are fire, earthquakes, vandalism, bombings or software malfunctions.

Electronic communications network [Directive 2002/21/EC]: Transmission systems and, where applicable, switching or routeing equipment and other resources, including network elements that are not active, which permit the conveyance of signals by wire, radio, optical or other electromagnetic means, including satellite networks, fixed (circuit- and packet-switched, including Internet) and mobile terrestrial networks, electricity cable systems (to the extent that they are used for the purpose of transmitting signals), networks used for radio and television broadcasting, and cable television networks, irrespective of the type of information conveyed.

Electronic communications service [Directive 2002/21/EC]: A service normally supplied for remuneration, which wholly or mainly provides the conveyance of signals on electronic communications networks, including telecommunications services and transmission services in networks used for broadcasting, but excludes services providing or exercising editorial control over content transmitted using electronic communications networks and services. It does not include information society services, as defined in Article 1 of Directive 98/34/EC, which do not wholly or mainly provide the conveyance of signals on electronic communications networks;

Interconnection [Directive 97/33/EC]: The physical and logical linking of telecommunications networks used by the same or a different, organisation, in order to allow the users of one organisation to communicate with users of the same or another organisation, or to access services provided by another organisation. Services may

be provided by the parties involved or other parties who have access to the network.

National regulatory authority [Directive 2002/21/EC]: The body or bodies charged by a MS with any of the regulatory tasks stipulated in this Directive and the Specific Directives.

Provider [Directive 2002/21/EC] is the undertaking providing public communications networks or publicly available electronic communications services.

Provision of an electronic communications network [Directive 2002/21/EC]: it means the establishment, operation, control or making available of such a network.

Public communications network [Directive 2002/21/EC]: An electronic communications network used wholly or mainly for the provision of publicly available electronic communications services that support the transfer of information between network termination points.

Threat [b-ISO/IEC 13335-1]: Potential cause of an unwanted incident that may result in harm to a system or organisation.

User [Directive 2002/21/EC]: Legal entity or natural person using or requesting a publicly available electronic communications service.

Vulnerability [b-ISO/IEC 13335-1]: Any weakness that could be exploited to violate a system or the information it contains.

10 References

1. DIRECTIVE 2002/21/EC of the European Parliament and of the Council on a common regulatory framework for electronic communications networks and services (Framework Directive).
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:108:0033:0033:EN:PDF
2. ITU E.800 : Definitions of terms related to quality of service.
http://www.itu.int/rec/T-REC-E.800-200809-I
3. ITU – T SERIES E: Overall network operation, telephone service, service operation and human factors.
4. Recommendation ITU-T X.1051 (2008) | ISO/IEC 27011:2008, Information technology – Security techniques – Information security management guidelines for telecommunications organisations based on ISO/IEC 27002.
5. ISO/IEC 27002:2005: Information technology – Security techniques – Code of practice for information security management.
6. ENISA: Good Practices on Reporting Security Incidents, 2009. http://www.enisa.europa.eu/act/res/policies/good-practices-1/incident-reporting-mechanisms/reporting-security-incidents-good-practices
7. Ofcom: Guidance on security requirements in the revised electronic communications Act 2003, Implementing the revised EU framework, May 2011, http://stakeholders.ofcom.org.uk/binaries/telecoms/policy/851653/guidance.pdf
8. Regulation on the Obligation to Notify Violations of Information Security in Public Telecommunications, FICORA, December 2009, http://www.ficora.fi/attachments/englantiav/5mCqE9KKW/FICORA09D2009M.pdf

11 Appendix A – Additional Notes

Other parameters

Additional parameters could be considered at national level for establishing more precise thresholds and generating a better understanding of the significance of an incident. These will not, at least for the time being, be taken into account in the reporting to the EC and ENISA. Nevertheless, NRAs might want to consider voluntarily adoption of these parameters when preparing the annual report to the EC and ENISA.

1. Time of the day: This parameter is used to qualify the impact according to the time an incident occurred, e.g. during the rush hour or at night. Rush hour is defined as a part of the day during which the workload and traffic congestion reach the highest level.

2. Special Occurrence: Days of the year that have significant importance, e.g. national elections, or when national events are taking place.

3. Traffic congestion/capacity: This parameter is used to determine the impact that network congestion has on an “acceptable level of service".

4. Interconnections: Impact on interconnections (for the definition of ‘interconnection’, please refer to the Glossary).

12 Appendix B – List of Vulnerabilities

Vulnerabilities are weaknesses of a given asset which could be exploited by a threat, thereby leading to a compromise or breach of confidentiality, integrity, or availability of information or services of a part or the totality of a Critical Asset:

- Confidentiality breach – unauthorised read access
- Integrity breach – unauthorised creation, modification, or deletion of files
- Availability breach – denial of service.

In the electronic communications area, we may differentiate the following main vulnerabilities by classifying them into asset categories:

- Network infrastructure
  - Inadequate topology/redundancy/resilience
  - Lack of , or inadequate, network administration and surveillance processes
  - Inadequate business continuity planning
  - Inadequate recovery processes
  - Insufficient recovery testing.
- Operating systems (software)
  - Poor software/application design
  - Reliance on unsupported management applications
  - Inadequate anti-malware management
  - Non-compliance with intellectual property regulations
  - Usage of unlicensed software components in the software architecture
  - Poor configuration management controls
  - Inadequate implementation
  - Excessive reliance on ‘response’ instead of ‘prevention’
  - Lack of encryption for critical information.
- Hardware
  - Inadequate physical protection of network equipment.
  - Inadequate access control
  - Inadequate hardware maintenance

- Unauthorised repair personnel
- No training on emergency shutdown procedures
- Hardware failure.

- Human factors
  - Social engineering
  - Inadequate personnel security policies
  - Inadequate training of new employees on ethical responsibilities
  - Training of personnel/contractors on new risk management processes
  - Lack of knowledge/ experience of the network's topology, equipment and infrastructure
  - Poor security management.
- Cascaded chain of events (interdependencies with other suppliers/equipment).

enisa

European Network and Information Security Agency