

About ENISA

The European Network and Information Security Agency (ENISA) is a European Union (EU) agency which acts as a centre of expertise for the EU Member States and European institutions. It gives advice and recommendations on good practice, and acts as a “switchboard” for exchanging knowledge and information. The agency also facilitates contacts between the European institutions, the Member States, and private business and industry.

Internet: <http://www.enisa.europa.eu/>

Contact details

Authors:

Dimitra Liveri, Daniele Catteddu, Lionel Dupre

Peer Review:

Marnix Dekker

Resilience and CIIP, resilience@enisa.europa.eu

Press and Inquiries:

Ulf Bergstrom (ulf [dot] Bergstrom [at] enisa [dot] Europa [dot] eu)

Acknowledgments

For the completion of this report ENISA has worked closely with a dedicated working group of stakeholders from all across Europe; namely some agencies and organizations that supported this procedure: PTS (SE), MINEZ (NL), FICORA (FI), Ofcom (UK), ANACOM (PT), ComReg (IE), EETT (GR), ITST (DK), CPNI (UK), RTR (AT), ANCOM (RO), ESMIS (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 and Development (IT), OCECPR (CY).

We are grateful for your valuable input and comments.

Legal notice

Notice must be taken that this publication represents the views and interpretations of the authors and editors, unless stated otherwise. This publication should not be construed to be a legal action of ENISA or the ENISA bodies unless adopted pursuant to the ENISA Regulation (EC) No 460/2004 as lastly amended by Regulation (EU) No 580/2011. This publication does not necessarily represent state-of-the-art and ENISA may update it from time to time.

Third-party sources are quoted as appropriate. ENISA is not responsible for the content of the external sources including external websites referenced in this publication. This publication is intended for information purposes only. It must be accessible free of charge. Neither ENISA nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication.

Reproduction is authorised provided the source is acknowledged.

© European Network and Information Security Agency (ENISA), 2011

Preface

Directive 2009/140/EC of the European Parliament and of the Council amends Directive 2002/19/EC, on access to, and interconnection of, electronic communications networks and associated facilities, Directive 2002/20/EC on the authorization of electronic communications networks and services, and Directive 2002/21/EC, on a common regulatory framework for electronic communications networks and services. The directive asks ENISA to contribute to the security of electronic communications and to contribute to the harmonization of technical and organizational security measures taken by the member states.

Paragraph 1 and 2 of Article 13a state that MSs should ensure that providers of public communication networks take measures to guarantee security and integrity of these networks and to ensure continuity of services provided over these networks¹. Paragraph 3 of Article 13a says that the MSs should report about significant security breaches and losses of integrity to the EC and ENISA.

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 harmonized implementation of Article 13a. In these meetings, a working group of representatives of NRA's and EC reached consensus about two technical non-binding documents.

- Technical guidelines for incident reporting (this document): Guidelines to support Member States in implementing paragraph 3 of Article 13a. Paragraph 3 concerns the notification of NRAs in case of a significant security breach or loss of integrity of networks, and it concerns annual reporting of these incidents to the EC and ENISA.
- Minimal Security Measures : A list of minimum security measures (MSMs) that NRAs have to take into account when evaluating compliance of electronic communications providers to paragraph 1 and 2 of Article 13a.

The meetings of the working group will continue beyond the publication of these documents to further support a harmonized implementation of Article 13a across the EU. In the context of the implementation of Art.13a Member States face the challenge of introducing, in their national practices, security measures which have to be coherent and harmonized at European Union level. The diversity between the MSs is vast due to the fact that some have already established (in few cases even for years) a well-functioning scheme for reporting security breaches by telecommunication providers, though most of others were still either in initial stage of the deployment or in planning phase.

¹ In technical jargon this would be called network availability.

All the decision taken in the context of this working group have been subject of the approval of all the parties (at the exception of ENISA and the Commission), therefore the content of this technical guidelines should be considered as expression of consensus between participating MSs.

Table of Contents

1 – Introduction	7
1.2 Article13a	8
1.3 Role of ENISA under Directive 2009/140	10
2 – Incidents Reporting Scheme	13
2.1 Objectives	13
2.3 Describing the reporting mechanism	14
3 – Defining the Scope	16
3.1 Scope of incident reporting	16
3.2 Non-exhaustive list of electronic communications networks and services	16
4 – Impact parameters and thresholds	19
4.1 Parameters	19
4.2 Thresholds	22
5 – Incident Report Data	27
5.1 Root Cause of a Security Breach	27
5.2 Reporting Template	32
5.3 The Reporting Channel	36
6 – Usage and Confidentiality	37
6.1 Confidentiality of reported information	37
Glossary	41
References	44
Appendix A – Side Notes	45
Appendix B – List of Vulnerabilities	46
Appendix C – Traffic Light Protocol	48



1 - Introduction

In this document, we provide guidance to the NRAs to implement in a harmonic way across Europe, the reporting scheme of security breaches. The recommendation of this document is not binding. However an effective pan European scheme can ensure that the stakeholders, who must be aware of a security breach that occurs, learn about it quickly. It ensures that national authorities can follow up with network operators in a regulatory capacity and finally it would enable the collection of data about security breaches, threats and prior experiences to be used for further analysis and as a basis for issuing recommendations.

In this context, reporting of security breaches 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,
- ✓ national authorities can propose and enforce follow up actions with networks and services managers in their capacity of regulators,
- ✓ the analysis of threats and vulnerabilities,
- ✓ the identification of good practices based on lesson learnt in the security breach management process;

1.2 Article13a

The DIRECTIVE 2009/140/EC introduces in the Framework Directive of the regulatory framework a new chapter on Security and Integrity which is reproduced below².

Article 13a

Security and integrity

1. Member States shall ensure that undertakings providing public communications networks or publicly available electronic communications services take appropriate technical and organizational measures to appropriately manage the risks posed to security of networks and services. Having regard to the state of the art, these measures shall ensure a level of security appropriate to the risk presented. In particular, measures shall be taken to prevent and minimize the impact of security incidents on users and interconnected networks.
2. Member States shall ensure that undertakings providing public communications networks take all appropriate steps to guarantee the integrity of their networks, and thus ensure the continuity of supply of services provided over those networks.
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.

² Source: http://ec.europa.eu/information_society/policy/ecomm/doc/library/regframeforec_dec2009.pdf

4. The Commission, taking the utmost account of the opinion of ENISA, may adopt appropriate technical implementing measures with a view to harmonizing the measures referred to in paragraphs 1, 2, and 3, including measures defining the circumstances, format and procedures applicable to notification requirements. These technical implementing measures shall be based on European and international standards to the greatest extent possible, and shall not prevent Member States from adopting additional requirements in order to pursue the objectives set out in paragraphs 1 and 2.

These implementing measures, designed to amend non-essential elements of this Directive by supplementing it, shall be adopted in accordance with the regulatory procedure with scrutiny referred to in Article 22(3).

ENISA will establish a reporting scheme for the annual summary report from the National Regulatory Authorities (NRAs) to ENISA and the European Commission which is coherent with the national breach reporting schemas.

A clear distinction exists, in the letter of Article 13 a, between

- the notification from undertakings (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]

- the annual summary report from an NRA to the European Commission and ENISA

"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]

- the notification of security breaches between NRAs and to ENISA

"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]

The first notification scheme between operators / providers and NRAs is not under the scope of this document; in 2009 ENISA issued a Good Practice Guide on Reporting Incidents to support NRAs in implementing a reporting process between the undertakings (providers/ operators) and NRAs. The current document deals with and analyses the second type of notification scheme: the annual reporting to EC and ENISA from the NRAs (picture below). A reference to the notification of security breaches between NRAs and to ENISA (ad hoc notification) is proposed, but the procedure details will remain at the discretion of the NRA.

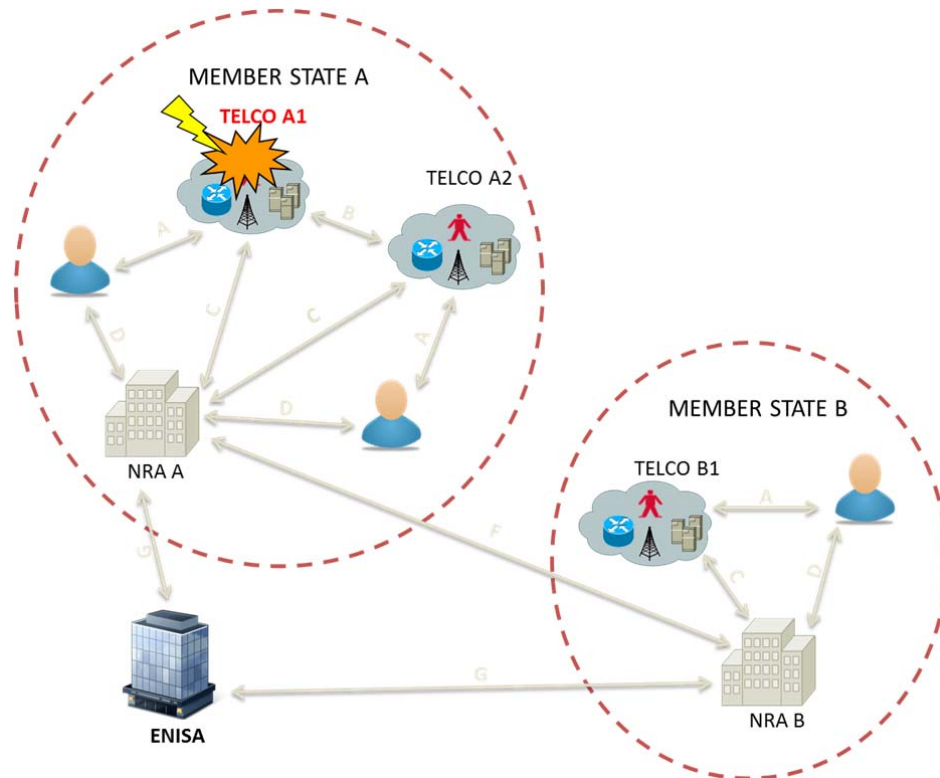


Figure 1. Information flow in the Reporting Scheme

1.3 Role of ENISA under Directive 2009/140

ENISA should contribute to enhance the level of security of electronic communications by, among other things, "providing expertise and advices, and promoting the exchange of best practices". Should the European Commission deem necessary to adopt appropriate technical implementing measures with a view to harmonizing the measures referred to in paragraphs 1, 2, and 3 of article

13a, ENISA will contribute to the harmonization process with expert advice on that measures³. The opinion of ENISA will be duly taken into account by the Commission.

To perform its duties ENISA should have the necessary means, including powers to obtain "sufficient information in order to assess the level of security of networks or services as well as comprehensive and reliable data about actual security incidents that have had a significant impact on the operation of network and services". Therefore, ENISA together with the Commission will receive from the Member States annual summary of the security breaches reported at the national level and the action taken to mitigate them.

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 the paragraph 3 of Article 13a. With such a reporting, ENISA will be better equipped to provide added value and support to Member States and European Policy makers in their effort to:

- develop a clear understanding of the asset at stake
- feed into effective business decision and policy making
- assess the level of security and the success of previously implemented regulatory, organizational and technical measures
- increase market transparency

Wider policy context

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

- In 2006, the European Commission issued a communication on "A Strategy for a Secure Information Society – Dialogue, Partnership and Empowerment" (COM (2006) 251), which was largely endorsed the following year by the Council (Council Resolution 2007/068/01). 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 under the overall European Programme for Critical Infrastructure Protection (EPCIP) adopted by the European Commission at the end of 2006.

³ See Directive 2009/140/EC, considered Recital n. 44, 46.

- The European Commission further adopted, in March 2009, a communication and an 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). This communication focuses on “prevention, preparedness, and awareness” and defines a plan of immediate actions to strengthen the security and resilience of CIIs.”

2 – Incidents Reporting Scheme

In this section we describe the objectives of the reporting scheme and the steps for the NRAs to follow when reporting to ENISA and EC.

2.1 Objectives

In this context the objective is to put in place a security breach reporting schema to collect annual reports and ‘ad hoc’ notifications of security breaches with cross border relevance. The goal of the collaboration between ENISA and Member States was to find a baseline which could be adopted as foundation by all and create a framework through which the different MSs will communicate in a “common language” between them and with the Commission and ENISA.

The collected data will be aggregated and analyzed by ENISA with the final goal to:

1. Inform Member States and European Union relevant Institutions on:
 - The impact of significant security breaches
 - Root causes of security breaches and losses of integrity
 - Lessons learned from the detection, response and recovery measures taken during and after the security breach from providers and Member States’ competent authorities
2. Support the knowledge transfer between Member States based on their internal experience and lesson learnt and between providers.
3. Understand the impact on interdependent critical assets at supra-national level (including the understanding of the impact of weakest link failures).
4. Develop possible security breach scenarios to be used for future Pan European Exercises
5. Issue recommendations to relevant policy makers of Member States and private sector
6. Analyse the suitability of relevant good practices in use and propose integrations and/or amendments if required
7. Understand possible future trends

2.3 Describing the reporting mechanism

A reporting and/or notification schema is the complex of rules settled, procedures established and actions taken to create a security breach reporting mechanism. The initial and generic procedures of the reporting scheme of security breaches can be summarized in the following steps (sequence of actions the NRA should execute for each incident reported by the Telco):

1. Define the scope of the incident; (did it affect a service which is in the scope of Article13a and if so, it was affected in a way that falls in 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. Collect data (in order to fill in the report with the information included in the template)
4. Report (ad hoc, annual)

Besides a clear definition of the scope and objectives of the reporting there should be a clear idea of what security breaches should be reported. Four key elements for an effective and efficient reporting scheme are:

- ✓ clear definition of the categories of the root cause, the reason why the security breach occurred,
- ✓ the reporting template, whose fields must be well defined and easily conceivable,
- ✓ the criteria/parameters taken into account to report a security breach and
- ✓ the thresholds to be used to “trigger” the reporting mechanism.

The scope of the incident reporting, as agreed by the working group is described in [section 3.1](#) followed by the electronic communication networks and services falling into Article13a, in [section 3.2](#).

If the incident falls into the scope of reporting, the next step is to determine if it triggers the reporting scheme; one of the main issues that were broadly discussed was the definition of the parameters –[paragraph 4.1](#) - and thresholds – [paragraph 4.2](#).

When the incident satisfies all the prerequisites additional information should be gathered in order to fill in the report accordingly i.e. the root cause of the incidents. The root cause of a security breach is the result of a threat which exploits a vulnerability of an asset. A categorization of root causes is provided in this guideline. A list of root causes can be found in [paragraph 5.1](#).

We provide a reporting template in [section 5.2](#). The objective of this standardized security breach reporting template is to make sure that the information sent from NRAs to the Commission and ENISA are of the same nature and with the same format. The information collect and aggregated on annual basis will be then used by ENISA to produce a report of the state of electronic communications with regards services security and continuity. The use of a standard template will make the process of data collection and analysis more effective and efficient and it is meant to avoid incoherencies.

In [paragraph 5.2](#), these fields are also described in details in order to avoid misinterpretations and to better guide NRAs in their annual reporting procedure.

3 – Defining the Scope

In this section we define the scope of the reporting scheme including the services which fall under the article13a.

3.1 Scope of incident reporting

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

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

The need for clarifications was evident from the very first meetings of the working group. A more concrete definition of the incident:

“Incident, in the context of Article13a, is defined as an event of a breach of security or loss of integrity that has a significant impact on the operation of electronic telecommunication networks and services.”

In the context of these technical guidelines, the working group of Member States and ENISA decided to focus⁴ the initial technical orientation of the security breach reporting and notification scheme on:

“Network and Information security incidents having a significant impact on the continuity of supply of electronic communication networks and services.”

3.2 Non-exhaustive list of electronic communications networks and services⁵

The electronic communications networks and/or services affected by the security breach need to be specified as an added value on the comprehensiveness of the reporting framework. Important information to be provided is the asset affected when this breach occurs as well as the impacted

⁴ We decided to narrow down the scope of the reporting for the initial period; when experience is gained the scope could be broadened

⁵ Definitions are based on the ETSI Terms and Definitions Database Interactive: <http://webapp.etsi.org/Teddi/>

service for the end-users. In the context of this technical guideline, we suggest to take as a basis the following non-exhaustive list of common/ typical assets that could be impacted by a security breach:

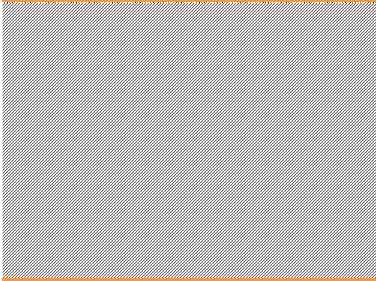
Service	Fixed Network	Mobile Network
Telephony / Voice	A domestic telecommunications network usually accessed by telephones, key telephone systems, private branch exchange trunks, and data arrangements.	The network supports digital communication for voice and Internet/data services on cell phone networks.
Data : service which 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.	
		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.	
Satellite communication	Radio communication service between Earth stations at given positions when one or more satellites are used; the given position may be a specified fixed point or any fixed point within specified areas; in some cases this service includes satellite-to-satellite links, which may also be effected in the inter-satellite service, the fixed-satellite service may also include feeder links for other space radio-communication services	An aeronautical mobile-satellite service reserved for communications relating to safety and regularity of flights, primarily along national or international civil air routes

Figure 2. Typical Telecommunication Assets

Disclaimer: As designated already, this is not an exhaustive list of assets and it does not have to be adopted by the Member States as is, if not under the jurisdiction of the NRA, when they launch the reporting scheme.

4 – Impact parameters and thresholds

In this section we describe the parameters and thresholds which signify the impact of the incident and if it should be reported.

4.1 Parameters⁶

In this paragraph, we identify and describe the parameters which should be used by NRAs to describe the significance of the impact of a security breach:

- Amount of users affected
- Duration of Incident
- Geographic Spread / Region
- Impact on emergency calls

Those parameters were selected and supported between ENISA and MSs; the parameters are used to generate the thresholds, which will trigger the reporting scheme (between ENISA and MSs) when a security breach with significant impact occurs. The parameter utilized to set the threshold and thus the obligation of reporting, will be chosen by the NRA. Combinations of parameters are legitimate.

Definitions

- 1. Amount of users affected:** The percentage of the total users of a service (see service category table 1) which were affected by the security breach (e.g. 10% of the end users of fixed telecommunications' service in MS X). For the end users of mobile telephony services the number is an estimation, according to the report from the provider.

The mechanism of reporting from NRAs to ENISA is triggered any time a security breach affecting a pre-established percentage of users (of a specific service) takes place. In the case of a root cause affecting more than one provider i.e. an earthquake, the NRA will gather reports individually from each provider/ operator. In the annual report, since the name of the provider is excluded, these incidents could be reported either as individual incidents or as one

⁶ [Rec. ITU-T E.800]A quantifiable characteristic of a service with specified scope and boundaries

major. If in the individual case the number of users affected per provider/ operator don't trigger the reporting thresholds, and then it can be reported as a major incident.

In order to properly assess the number of affected users, it is suggested that the reporting mechanism take into consideration the difference between 'service users' and 'service resellers'

A "reseller"⁷ is "a provider who purchases telecommunications services from another telecommunications service provider and then resells to the end users as a component part of, or integrates the purchased services into a mobile telecommunications service."

Usually the telecommunication operators and the service providers are aware of the percentage of end-users, to which the provided services are through a reseller. Under the context of Article13a, only the number of the affected end- users (client as referred in the Directive) is relevant; the term "reseller" refers to the intermediate and not to the end user.

Member States can use the thresholds suggested in this guideline by ENISA as a minimum level of significance. It should be noted that this criterion is purely quantitative (% of users affected) and it won't take into consideration the type of users affected. In other terms the weight assigned to each user is the same and there is no distinction between, for instance, a home user and a bank or a hospital. In general considerations on the criticality of an infrastructure served by a telecommunication provider won't be part of the scope of the reporting to ENISA (the rationale is that Critical Infrastructure and Critical Information Infrastructure are not the subject of the Regulatory Framework for electronic communications).

- 2. Duration of the Security Breach:** How much time did the security breach last? Time can be measured in any means of time (minutes, hours, days etc) e.g. disruption of the services for 1 h. The duration of the security breach is the time span starting when the service is starting to degrade until when the service is available again to the end user or the duration while the end-users could not use the service. This parameter will be used to judge if the incident reported by the telecommunications provider or operator, will be reported to ENISA. The duration of the incident is not an element of the reporting template.

⁷ <http://apps.leg.wa.gov/rcw/default.aspx?cite=82.04.065>

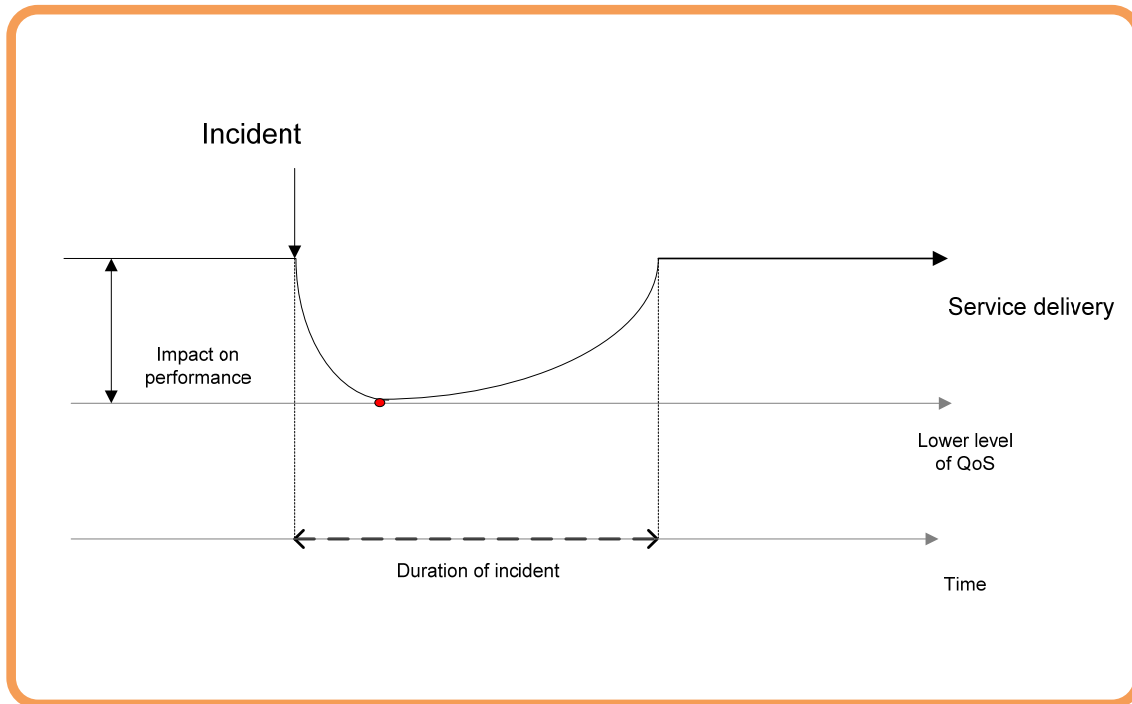


Figure 3. Timeframe of a security breach

- 3. Geographic Spread or Location (rural areas):** Signifies the area covered when the incident happens. In a major security breach a region can be affected. The impact is different depending on the geographic spread and on the density of population e.g. the security breach affected the area of region "X". This metric can furthermore be displayed as % of the country.
- 4. Impact on emergency calls:** Signifies a security breach having an impact on emergency numbers calls (e.g. 112) and affect the continuity of this service.

4.2 Thresholds

A security breach should be reported to ENISA every time the impact is equal or higher to a set of predefined thresholds agreed between ENISA and NRAs. Thus, thresholds are used to trigger the reporting procedures.

ENISA proposes the definition of high level thresholds which are meant to define what should be considered, as a minimum, by a NRAs as 'a security breach with significant impact'.

Based on ENISA proposed minimum level of significance, NRAs can introduce in their countries a more detailed set of thresholds.

Thresholds defined at national level cannot be higher than the once proposed by ENISA, in other words if ENISA should describe a security breach as significant when it affects 10% of the service subscribers for more than 8 hours, then a NRA cannot impose a thresholds which considered, for instance, a downtime of more than 12 hours affecting 10% of the subscribers as the entry levels of significance.

We decided upon set of requirements for the definition of security breach reporting thresholds:

- The procedure to determine the significance of a security breach (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 amount of security breaches to report.
- The significance of a disruption should be measured against their 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.
- A suggestion was made to consider a reporting triggered only by an absolute number of end-users impacted, not a percentage, to ensure equal treatment of all EU Citizens.
- Percentages should be translated into fixed figures, adjusted to the size of the country.

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

List of Thresholds: When do we report an incident?

We include in this paragraph a set of thresholds which should be used by NRAs as a minimum baseline to determine under which circumstances:

- National providers should report to NRAs when an incident occurs
- NRAs should annually report to Commission and ENISA
- NRAs should alert other NRAs and ENISA

As already mentioned above, the thresholds defined are to be intended as minimum entry level and each NRAs can impose more strict and granular thresholds too trigger the reporting at national level. However the same thresholds will be used to trigger the reporting process to ENISA.

The reporting from NRAs to ENISA should be done always according to the thresholds defined by ENISA. The reporting of security breaches which are below the thresholds should only be performed when the security breach requires specific attention especially at EU level. At the same time NRAs have to report to ENISA every security breach which impact is above the level settled in the thresholds. The according NRAs will have to select from the total of incident they collected throughout the year, the incidents that trigger the thresholds defined in this guideline and report those to ENISA.

Thresholds - Reporting from national providers to NRAs

National providers should report a security breach to the NRAs on the basis of thresholds defined by NRAs itself. National reporting threshold have to be based on the one established for the reporting to the Commission and ENISA, but they can be more stringent to match the needs and requirements of the NRAs. ENISA issued a Good Practice Guide⁸ in 2009, which can assist the MSs to establish this reporting scheme.

Thresholds - Reporting to ENISA

NRAs should report to ENISA every security breach which could have the following characteristics:

⁸ See more in the ENISA site under the Resilience section.

- With a HIGH (red) impact according to the scale proposed in the table below in which the impact is describe as a combination of % of affected users and service downtime (security breach duration):

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

Figure 4. Table of thresholds combination of users affected and duration

- Disrupts the Emergency number calls and makes the service unavailable;
- Makes a communication service or network unavailable for more than 4 hours in a rural area.

It should be noted that each NRA will define autonomously:

- the conditions under which emergency call unavailability represent a security breach with a significant impact,
- the areas in the respective country which should be considered as 'rural' (mountain areas, islands, etc.).

Disclaimer: In some cases the emergency calls, as well as the broadcasting services, do not fall under the supervision of the telecommunications NRA, who will implement Article13a provisions. Clearly expressed exemption is agreed for NRAs and the emergency call handling services incidents will not be required specifically in the incident reports.

Thresholds – Alert-Communication from NRA to NRA and to ENISA

Where appropriate, the national regulatory authority concerned shall inform the national regulatory authorities in other Member States and ENISA. It is left open to the judgment of a NRA to inform other NRAs and ENISA. In case of large scale phenomena such as thunderstorm, earthquake or power cuts, more than one operator could be affected. It could be the case that such incidents could be below threshold for each individual operator but above threshold for all operators together. The NRA will judge if these incidents must be included in the annual report. Since the name of the operator or provider is not included and the root cause of the incident is the same, the incident can be handled as one individual incident causing breach of security or loss of integrity to the totality of affected users.

It is evident that the NRAs will receive an incident report from the service provider or networks operator, once the incident has been handled and they will use the report to decide whether there is a need to supervise the compliance of the provider or not. The final report could be delivered to us up to two weeks after the incident occurred. It is important that the affected service provider is allowed to focus on resolving ongoing disturbances, rather than having to spend resources on providing information to the NRA about the incident. Therefore, the provider will only be required to provide very brief information about ongoing incidents to the according NRA. ENISA recommends NRAs to maximize the timely sharing of information on security breaches as that information could be useful to other NRAs to prevent a new security breach and to minimize its impact.

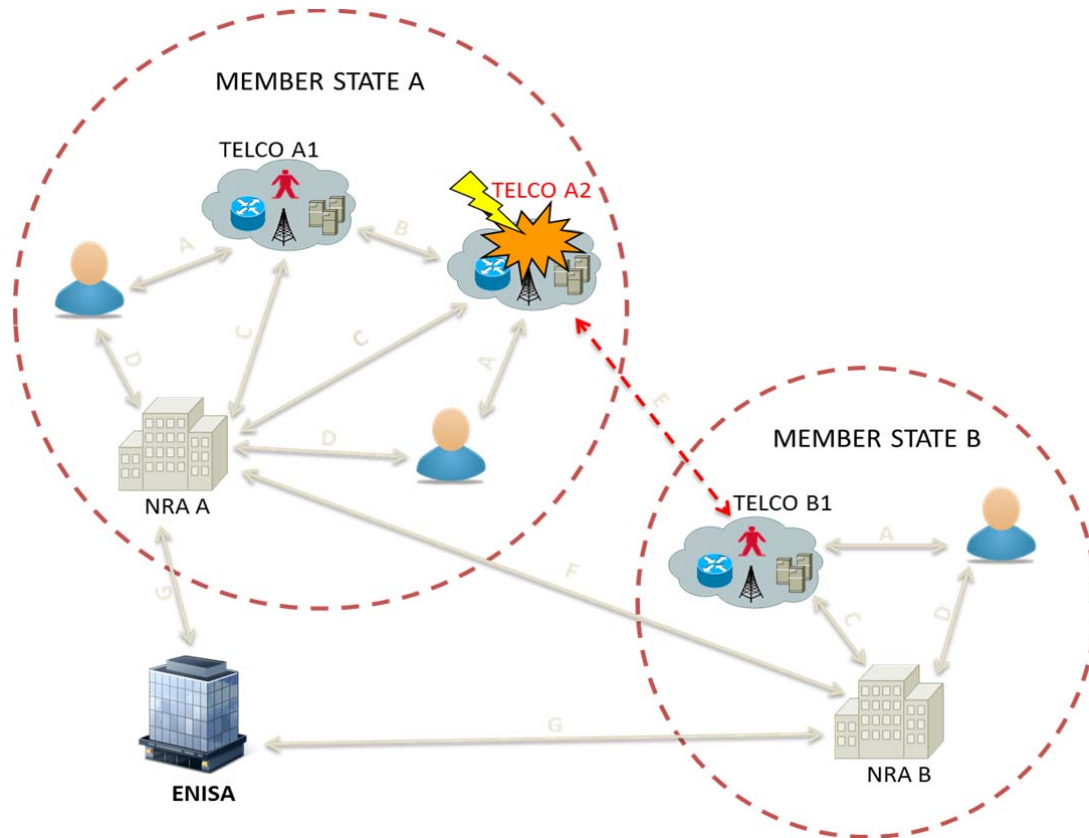


Figure 5. Information flow for cross border incidents

Under this light, ENISA suggests NRAs to alert their counterparts, at least:

- in case of a security breach that by its nature is likely to affect other MSs (i.e. 1) the root cause of the incident, 2) the affected assets or services, or 3) the action taken to mitigate or resolve the incident, clearly spans across the borders of two or more MS)
- in case that the information on how the security breach was handled in NRA could be useful to other MSs.

With the objective to facilitate the exchange of information between NRAs, the Commission and ENISA, the Agency will establish a list of relevant point of contact in competent NRAs. By the end of 2011, all the MS will be asked to update this list with the according contact point in the National regulatory Authorities. This list will be disseminated to the according stakeholders and updated in a periodic basis.

5 – Incident Report Data

In this section we describe the reporting template and its content, the categorisation of the root cause and finally how the reports will be sent to ENISA.

5.1 Root Cause of a Security Breach

The classification of root causes of a security breach which is described in this paragraph is based on the document “Explanatory notes to Regulation 9 on the obligation to notify of violations of information security in public telecommunications” published by FICORA⁹.

The document was taken as main source of inspiration for the classification of the security breach root causes, because Finland represents the first EU MS with a mandatory security breach reporting schema in the electronic communications sector. It should be noted that another references used is: “Security Procedures - Telecommunication Systems and Services”, issued by CESG, the UK National Technical Authority for Information Assurance (not a public document).

The classification of security breach root causes is meant to serve as a direct support for the national authorities (NRAs) in their annual reporting to the Commission and ENISA. NRAs will use the root causes classification suggested in this document as a guide to communicate to the Commission and ENISA the reasons of the occurrence of a security breach in the context of predefined set of possible causes.

It should remain clear that NRAs will be asked to report, at minimum, only the general root cause category. Nevertheless, ENISA encourages NRAs to share voluntarily with the Commission and the Agency itself as much details as possible, including the specific nature of the root cause.

The root cause classification could also serve as an indirect support to NRAs in their effort to create and implement their national security breach reporting scheme.

⁹ <http://www.ficora.fi/attachments/englantiav/5k8yJAS9R/FICORA07B2009M.pdf>

For the sake of this classification we have identified five (5) categories of root causes. The drawing below shows the initial hierarchy foreseen, both in literature and recent publications:

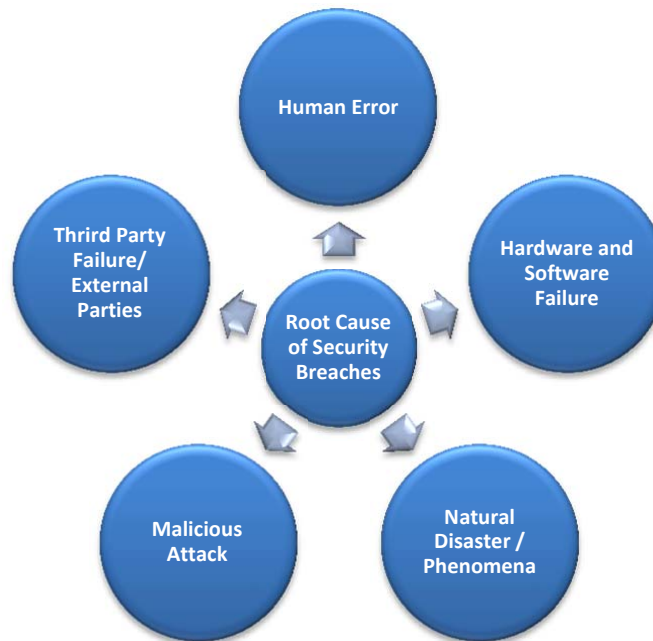


Figure 6. Categories of Root Cause

The list includes/ distinguishes security breaches that can cause a breach of security and loss of integrity and availability, by their root cause. Many of these security breaches violate both service availability as well as the confidentiality or/and the integrity of the information that is managed by the provider of electronic communications. Confidentiality does not fall under the scope of Article 13a, but when an incident happens affecting integrity and confidentiality i.e. unauthorized access, will be reported as a loss of integrity incident.

The final list of security breach categories (with examples) has been discussed and approved by the dedicated working group. Examples of each type of root cause are listed below which could be of relevance and be indicatively considered as potential root causes. The two categories of human error and hardware and software failure concern internal processes and assets, while the category of external parties covers the human errors or failures cause by external causes.

When filling in the report (based on the reporting template) in the field of root causes the check boxes indicate to those five categories. One incident might even be the result of two causes, in this case the editor has the option to select both; i.e. a common cause of disturbances is loss of power; commonly, power is lost due to bad weather. To some extent, the effects of main power loss can

be mitigated by the use of a UPS or diesel standby generator. But it is not reasonable to expect such backup power to be available for all parts of the network. This kind of incident can be categorized as having a root caused by a Natural Disaster / Phenomena and/or, if we focus on the fact that there was no backup power or redundant systems to kick in when mains power was lost, as Human Error due to bad implementation of the recovery plan.

Natural Disaster / Phenomena

- Impact of Natural disasters on Communication infrastructures
 - Severe weather (e.g. storms, heavy snowfall, heat wave),
 - Earthquakes
 - Tsunamis
 - Pandemic diseases
 - Floods
 - Fire
 - Landslides
 - Volcano disruptions
 - Space weather effects

Example incident that is in the scope of Article13a reporting scheme: An earthquake is causing disruption on the fixed telecommunication services affecting a large number (30%) of end-users for 5h.

When reported the root cause would be natural disaster even though one of the consequences could be hardware failure.

Malicious Attack

This describes a person or a program who/which gains logical or physical access without permission to a network, system, application, data or other IT resources. Such breach may be the result of a targeted attack, and could originate either from insider or outsider threat. The root causes included in this category are divided in two subcategories which are: “Logical Security Attacks” and “Physical Security Attacks”.

1. Logical Security

- Unauthorized logical access to:
 - Network devices;
 - Platforms;

- Applications (software);
- Backup;
- Database;
- Sensitive data (identification, customer and configuration data, network documentation data, traffic and location data or structure descriptions, etc).
- Unauthorized use of elevated privileges (privilege escalation from external user, privilege escalation from internal user, identity theft, social engineering attacks);
- Tapping 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 of security controls;
- Successful hostile log-in attempts into the information systems of telecom operators;
- Poor Configuration and Change Management;
- Traffic misrouting and rerouting (e.g. corruption of network traffic routing tables)
- Malware spreading (e.g. computer viruses, backdoor 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);
- Software and hardware vulnerabilities exploitation

2. Physical Security

- Unauthorized physical access:
 - to system hardware and make unauthorized changes;
 - physical break-ins to information systems' premises;
- Theft of equipment or media.

Example incident that is in the scope of Article13a reporting scheme: *A DoS attack to a telecommunications' system is causing disruption on a telecommunication services affecting a large number (40%) of end-users (malicious attack against logical security).*

Or

An intended theft of equipment of telecommunications' system is causing lack of continuity on a telecommunication services affecting a large number (30%) of end-

Human Error (internally caused)

- 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
 - Security Breach in management procedures

Example incident that is in the scope of Article13a reporting scheme: *A wrong configuration of telecommunications' system by a **staff member** is causing outage of a telecommunication service. A large number (60%) of end-users is affected.*

Hardware – Software Failure

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

Example incident that is in the scope of Article13a reporting scheme: *Failure of equipment due to wear causing disruption on a telecommunication services affecting a large number (60%) of end-users.*

Third Party Failure/ External Parties

- Human errors caused by external party (i.e. cut of a cable from excavation machines)
- External procedure failure affecting internal process
- Faults of the supply chain

Example incident that is in the scope of Article13a reporting scheme: *A cable cut due to excavation operations in the area causing disruption on a telecommunication services affecting a large number (60%) of end-users.*

5.2 Reporting Template

This is the report the MS will deposit to ENISA annually describing each major security breach.

ELECTRONIC COMMUNICATIONS SECURITY BREACH REPORT	
Country:	
Date and Time of occurrence	
Date:	Time:
Executive Summary	
Root cause:	Natural Disaster <input type="checkbox"/> Human Error <input type="checkbox"/> Malicious Attack <input type="checkbox"/> Hardware/ software Failure <input type="checkbox"/> Third Party Failure/ External <input type="checkbox"/>
Type of Security Breach:	
NRAs contacted:	
Security Breach Handling and Response measures:	
Post Security Breach Measures:	
Impact Description	
Affected Asset:	
Affected Service:	
<u>Telephony /Voice:</u>	

Fixed Telephony <input type="checkbox"/>
Mobile Telephony <input type="checkbox"/>
<u>Data :</u>
Message Services <input type="checkbox"/>
Internet <input type="checkbox"/>
Email <input type="checkbox"/>
<u>Satellite communication</u> <input type="checkbox"/>
Time to restore:
Interconnections Affected:
Users Affected:
Short Description, Analysis and Lesson Learnt

Description of Template fields

Country	
Description:	The country that <u>sends the report</u> to ENISA.
Date and time of occurrence	
Description:	Details of the date and time when the security breach took place (in National time). It can be interpreted as the time of discovery of the incident. Time should expressed in both CET and local time
Data sets/ values:	Example. 04022011/10:45 EET – 09:45 CET

Type of Security Breach	
Description:	The type of the security breach is the category where this breach belongs to e.g. DoS attack causing security breach of congestion in data services. Even though this will provoke the degradation of the quality of service and not its interruption, this will remain an incident that needs to be reported since it will have an effect on the continuity of the service. These could be subcategories of the root causes listed in the according section.
Root cause	
Description:	The initial cause of the security breach (human error, malicious attack etc)
National Regulatory Authorities contacted	
Description:	<p>The competent NRAs in other countries which were notified about the occurrence of the security breach. If authorities from other Member States or third countries are involved in the response action, they should be mentioned as well.</p> <p>Further information (voluntary): The reason a country contacted another MSs competent NRA (this can be also added in the "Additional Information" field).</p>
Security Breach handling and response	
Description:	All the actions taken after the discovery of the security breach and the measures adopted to restore the service to initial conditions/ level.
Post Security Breach Measures	
Description:	Include a description of any arrangements that were made to minimize the level of risk, and comment on how effective you thought these measures were.
Affected Asset	
Description:	An asset's loss potentially stems from the value it represents and the liability it introduces to an actor (organization- provider). Affected asset is the initial target of the security breach. The incident causing

	chain effects will end in the unavailability of a service to the end user. In this field the starting point of this chain is requested.
Data sets/ values:	Usually involves the catastrophe/ change of a physical asset. Example. Cut cable
Affected Service	
Description:	The affected service is the service which is made unavailable to the end user. In this field a description of the service which value and availability relates to the impact level.
Data sets/ values:	Given through check boxes – you can choose more than one
Time to restore/resumption	
Description:	<p>The time span from the discovery of the security breach (different from the time the security breach happened) until the service is back to the initial level.</p> <p>Further information (voluntary): The time span from the discovery of the security breach (different from the time the security breach happened) to the full service recovery.</p>
Data sets/ values:	Example. 5 hours.
Affected interconnections	
Description:	<p>If the affected service can cause damage/ change to an asset (or service) of another operator or provider then this is an affected interconnection. In case of a cross border security breach, it would be possible one MS can affect assets of another “interconnected” MS.</p> <p>Some concentrations of infrastructure are vulnerable and significant disruption can be caused by localised failure; cascading technical failures can be caused to interconnected systems.</p>
Affected Users	
Description:	The total number of users affected when a security breach occurs.
Data sets/ values:	Absolute number / Percentages

Short Description, Analysis and Lessons Learnt

Description: Describe any actions that were taken some time after the security breach to improve the security of the asset and what procedures will be followed (or measures taken) from then on.

5.3 The Reporting Channel

According to the scheme applied for the reporting procedure, proper channel(s)' requirements have to be specified.

- Email (dedicated mailing list through PGP)
- Web based forms (in the dedicated portal)

In this light after gathering all the annual reports from the MSs, ENISA will be able to gather and study the raw data and publish a report analyzing the trends, including a mapping of the security breaches all over Europe.

Coordination and Information distribution

The National Regulatory Authorities will have to annually report major security breaches to European Commission and ENISA through a suggested template. The summarized annual report will be send to ENISA on Q1 of the following year e.g. for 2011 security breaches the according parties should send the report on Q1 of 2012. ENISA might send notifications to the participants to kindly remind them the submission of the report. Some coordination clarifications are needed when setting the scheme to avoid collisions and bottleneck problems.

A list of contacts where the representatives and responsible of each party are included. This will enable the communication between the NRAs across Europe and ENISA.

After ENISA analyses the information gathered, a report will be distributed to all the participants. This could be done through a dedicated mailing list or a dedicated portal where it would be published.

6 – Usage and Confidentiality

All the elements of the reporting scheme have been explicitly analyzed in the previous chapters, leaving the details of the confidentiality and usage of the information of the reporting to be described in the last section.

6.1 Confidentiality of reported information

In consideration of the obligation assigned to the Member States under Article 13a (3) of Directive 2009/140/EC to notify security breaches to ENISA and to the European Commission, it is clear that the Member States may have an interest in objecting to the disclosure of documents and information as provided in this Directive. The grounds for such objections may be either of business or of security nature.

In case of the information sensitive from the business perspective a relevant legal basis for their classification is provided 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.*"

In case of the information that might be sensitive to the national security, an adequate framework can be found in Art.4 of Regulation 1049/2001 regarding public access to European Parliament, Council and Commission documents¹⁰. This Regulation is particularly relevant due to the exceptions provided in its 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 the Member States may:

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).

- request the institutions to not disclose a document originating from that Member State without a prior agreement¹¹ (Art.4(5))

- indicate, when consulted by the Commission/ENISA, that the information comprised in the notification is important for the public security (Art.4(4)). It needs to be noticed that the European Commission as well as ENISA¹² both have an obligation to consult the third party¹³ from which a given document originates with a view to assessing whether the exceptions to the access to the document should be applied).¹⁴

In the light of the above, the Commission and ENISA will have to acknowledge any indication by the Member State that given information should be treated on the restricted way.

6.2 Intended use of the Information Gathered

The information on security breaches with significant impact on electronic communications will be collected by ENISA with the purposes of:

- 1) Drafting an annual report of the status of electronic communications with regards to security, integrity and continuity of service;
- 2) Issue recommendations, advices and good practices on:
 - a. Security Breach Collection, e.g. how to improve the security breaches reporting scheme in MSs and how to improve the information sharing between NRAs, Commission, ENISA and private sector
 - b. Security Breaches Management, e.g. how to maximize the value of the lesson learnt at National and EU level in the security breach management process, creation of benchmarks for incident management process, etc
 - c. Investments, research funding, identification of incentives for the market, etc
- 3) Creation of statistical series

The preconditions for the above objectives to be achieved are:

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) of Regulation 1049/2001" [...] a Member State may request the institution not to disclose a document originating from that Member State without its prior agreement".

- Collection of enough reports to be analyzed
- Richness and accuracy of data
- Resources to perform the analysis.

Content of the Annual Report published by ENISA

Depending on the quality and quantity of the reports received by the end of the reporting period (see ch.4.1) the annual report might include, between other information, the following:

- Which were the most common breaches?
- Which are the most common root causes of incidents?

Usually the root cause is described as a THREAT which exploits VULNERABILITY(ies), therefore if providers will offer sufficiently detailed information (non-confidential), statistics on the most common threats and vulnerabilities (e.g. Which is the most important threat to be addressed?) will be included in the report. As confidential information are NOT going to be shared, a possible analysis of the most common vulnerabilities will not be based on technical details (which will not be reported and shared with ENISA), but rather on general categories of vulnerabilities (e.g. HW or SW misconfiguration, see appendix C). Answers on questions as the following could be included:

- Services vulnerabilities (Which are the most affected services?)
- Common threats: Which is the most common root cause for security breaches affecting a specific service? (i.e. most common root causes affecting fixed telephony are natural phenomena)
- Trends analysis: percentage of affected users in Europe each year, percentage of affected type of services per year. (What are the trends in Europe?)
- Attacks analysis: For the security breaches caused by a malicious attack, how can these attacks be characterized? If compared with attacks collected in the previous years, which differences can be highlighted? (More sophisticated, more targeted, combination of several methods, not easy to detect, etc)
- Common time framework: security breaches time distribution (when most of the security breaches happened in Europe?)

- Mapping of the profile of the attacks (Scan, probe, worms, DoS, spam etc.)
- Interconnections Affected: In a security breachincident case how do the interconnections work? How does one service affect the other? Create a map of interconnections in a national level and in a Pan European one.
- Impact escalation: Which category of assets if affected can cause a greater impact on the service? Why?
- What are the conclusions after studying the time to restore from security breach to security breachincident to incident according to their classification and type of service?
- Which is the mean time to restore the service level?

Disclaimer

This report will not include any direct comparison between MSs, therefore information such as:

- Number of security breaches per country,
- Average impact per security breachincident in country X,
- Mean time to security breaches discovery in country X,
- Mean time to recovery in country X;

will not be part of the annual report ENISA will publish.

The list above is not meant to be considered as exhaustive, and the suggested information and metrics should be seen only as examples of what is not going to be included in the Annual Report.

Glossary

Attack [b-ITU-T H.235.0]: The activities undertaken to bypass or exploit deficiencies in a system's security mechanisms. By a direct attack on a system 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 to be in a state to perform a required function at a given instant of time or at 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

Disasters Recovery / Business Continuity [Rec. ITU-T E.800]: All activities associated with the restoration of a network provided service after disasters. Examples of such disasters are fire, earthquakes, vandalism, bombings, or software malfunctioning.

Electronic Communications Network [Directive 2002/21/EC]: transmission systems and, where applicable, switching or routing equipment and other resources, including network elements which 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 provided for remuneration which consists wholly or mainly in the conveyance of signals on electronic communications networks, including telecommunications services and transmission services in networks used for broadcasting, but exclude 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 consist wholly or mainly in the conveyance of signals on electronic communications networks;

End-user [Directive 2002/21/EC] : a user not providing public communications networks or publicly available electronic communications services.

Event [ITU-T E.409]: An event is an observable occurrence which is not possible to (completely) predict or control.

Incident [ITU-T E.409]: An event that might have led to an occurrence or an episode which is not serious

Integrity [ITU-T H.235.0]: The property that assets have not been altered in an unauthorized manner.

Interconnection [Directive 97/33/EC]: the physical and logical linking of telecommunications networks used by the same or a different organization in order to allow the users of one organization to communicate with users of the same or another organization, or to access services provided by another organization. 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 Member State with any of the regulatory tasks assigned in this Directive and the Specific Directives;

Provider [Rec. ITU-T E.800]: An organization that owns a telecommunications network for the purpose of transporting bearers of telecommunication services.

Public communications network [Directive 2002/21/EC]: an electronic communications network used wholly or mainly for the provision of electronic communications services available to the public which support the transfer of information between network termination points;

Quality of Service [Rec. ITU-T E.800]: Totality of characteristics of a telecommunications service that bear on its ability to satisfy stated and implied needs of the user of the service.

Security [ITU-T X. 800]: The term 'security' is used in the sense of minimizing the vulnerabilities of assets and resources. An asset is anything of value.

Service Provider [Rec. ITU-T E.800]: An organization that provides services to users and customers.

Telecommunications security incident: Any real or suspected adverse event in relation to the security of telecommunications. This includes:

- Intrusion into telecommunication systems via the network;
- Occurrence of computer viruses;
- Probes for vulnerabilities via the network into one or more computer systems;

- PABX call leak-through;
- Any other undesired events arising from unauthorized internal or external actions.

Telecommunications services [Directive 97/33/EC]: services whose provision consists wholly or partly in the transmission and routing of signals on telecommunications networks, with the exception of radio and television broadcasting;

Threat [b-ISO/IEC 13335-1]: A potential cause of an unwanted security breach that may result in harm to a system or organization.

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

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

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.800-200809-1>
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 organizations 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 telecommunications 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 Of Violations Of Information Security In Public Telecommunications, FICORA, December 2009,
<http://www.ficora.fi/attachments/englantiav/5mCqE9KKW/FICORA09D2009M.pdf>

Appendix A – Side Notes

Other parameters

We suggest in this paragraph other parameters that could be considered at National level to establish more precise thresholds and to generate a better understanding of the significance of a security breach. Those parameters won't be, at least for the time being, taken into account in the reporting to Commission and ENISA. Nevertheless a MSs might want to consider to voluntarily adopt these parameters when preparing the annual report to Commission and ENISA.

- 1. Time of the day:** This parameter is used to qualify the impact according to the time of occurrence of the security breach e.g. during rush hours, during night time. A rush hour is a part of the day during which the work load and traffic conjunction reaches the highest level. Normally it occurs twice a day on working days and typically, rush hour lasts from 10–1 pm (10:00 – 13:00) and from 2–5 pm (14:00–17:00) local time.
- 2. Special Occurrence:** Days of the year which have significant importance e.g. national elections day, day of conduction of a national exercise.
- 3. Traffic congestion / Capacity:** this parameter is used to determine the impact that network congestion has on “acceptable level of service”
- 4. Interconnections:** Impact on interconnections (for the definition of interconnection refer to the Glossary)

Appendix B – List of Vulnerabilities

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

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

In the Telecommunications area, we may distinguish the main following vulnerabilities classified by Category of assets:

- Network infrastructure
 - Inadequate Topology / Redundancy / Resilience;
 - Lack 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 Antimalware management;
 - Noncompliance with Intellectual Property regulations;
 - Usage of unlicensed software components in the software architecture / urbanism;
 - 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
 - Unauthorized repair personnel
 - No training on emergency shutdown procedures
 - Hardware failure
- Human factor
 - Social engineering;

Article13a Implementation

- Inadequate personnel security policies;
- Inadequate training on new employees on ethical responsibilities;
- Training of personnel/contracts 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);

Appendix C – Traffic Light Protocol

1. The Traffic Light Protocol (TLP) is used to exchange unclassified but sensitive material.
2. The originator of any such material will mark the information in accordance with the TLP before distribution. All recipients will provide the material with the appropriate protection based upon the requirements of the TLP.
If the originating source offering the information does not designate such a level, the information will be assumed to be AMBER, and the source [identity of the providing organization] be assumed to be RED.
If a recipient has any doubt about the information `sharing level being used, he/she will contact the originating source to clarify the position before taking any further action.
3. Where a recipient needs to redistribute material with a restrictive TLP marking to personnel outside of the agreed group then authority must be sought from the originating source before such redistribution takes place.
4. If a member of the group believes that material has been incorrectly categorized in accordance with the TLP, that member will request a re-designation from the originator.
5. Information sharing with the private sector, notably critical infrastructure operators, is important and should be supported. When possible, MS should designate information that may be disclosed to them.
6. All member organizations will adhere to their national security requirements for the protection of classified or protectively marked material.

The TLP is composed of four levels:



Red

RED - Non-disclosable information restricted to either personnel present at a particular meeting or involved in face-to-face discussions or voice / video communications. No written material allowed. Personnel may not disseminate any such information without the agreement of

the data owner. Guests & others such as visiting speakers who may be present at such a discussion will be required to leave before any such information is disclosed.



Amber

AMBER – default classification. Limited Disclosure and restricted to participant organizations; personnel within their organizations, with the authority of the originating source, to other government departments, Information Exchanges or private organizations which may have a need to know in order to take any appropriate action, i.e. For Official Use Only - NOT for publication or broadcast in a public venue.



Green

GREEN - Information can be shared with other organizations, Information Exchanges or individuals in the cyber security, information assurance or private organizations at large, but not published or posted on the web.



White

PUBLIC - Information that is for public, unrestricted dissemination, publication, web-posting or broadcast. Any member may publish the information, subject to copyright.

