Incident Reporting and Information Sharing - an EU Perspective

Background

A need for EU to increase the level of security in the information society and to harmonise the implementation of measures in the MS.

- In 2006, the EC issued a strategy for a secure information society
- In 2009, the EC adopted the CIIP Action Plan
- In 2009 the new telecom directive package incl. rules on security measures and incident reporting – Art 13a
- In 2011 the new rules were implemented in the MS
- In 2013 an EU Cyber Security Strategy and a proposed directive on NIS – incident reporting also for other sectors (Finance, eServices, Energy, Transport etc.)

Why incident reporting

Common need to analyse and understand the nature of security incidents in the information society

- What incidents
- What impact
- Why they occur
- Experience from the incidents

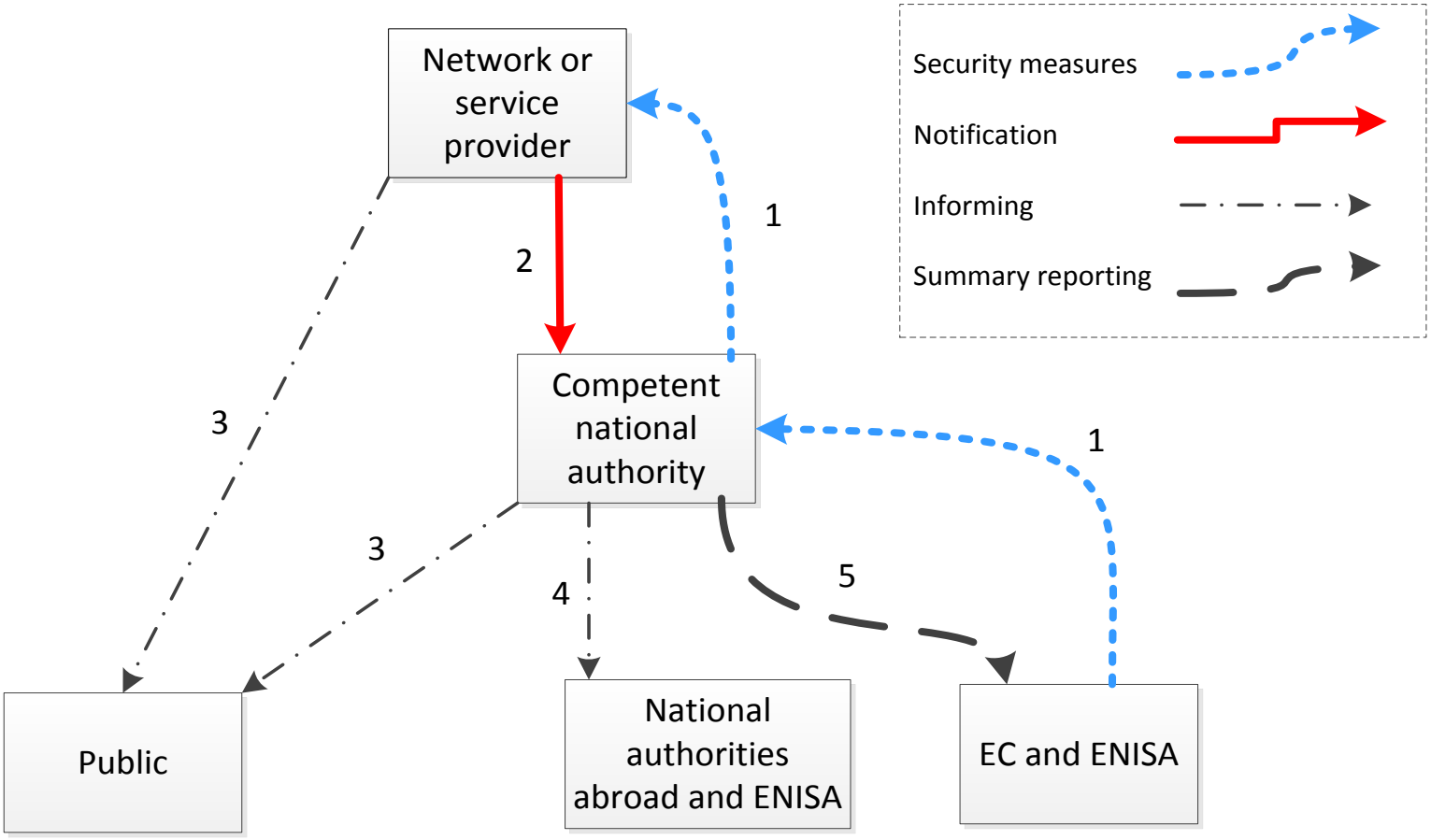
In order to take action from lessons learned

- Share experiences and good practice
- Improve security measures
- Prioritise what security measures to focus on

Art 13a in the telecom package

- Appropriate security measures
  - to minimize impact of security incidents on users and interconnected networks
  - to guarantee network integrity, thus ensuring continuous supply of services over the networks
- Incident reporting
  - Providers report significant incidents with impact on operation of services to their Regulator (NRA)
  - NRAs can inform or require the provider to inform the public when this is in the public interest
  - NRAs inform other NRAs abroad and ENISA when cross border incidents
  - NRAs provide an annual summary report to ENISA and the EC

Overview of Article 13a flow



Art 13a - ECS in scope

Electronic Communications Services (ECS) in scope for reporting to the EC and ENISA:

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

Not in scope for annual reporting: SMS and E-mail

Thresholds for annual reporting

A combination of affected percentage of the national user base of an ECS and the duration of the incident

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

The role of ENISA

- Provide aggregate (statistical) analysis of incidents for policy makers, NRAs, the industry and the public
- Issue recommendations and guidance for NRAs, the private sector and policy makers
- Facilitate the exchange of experiences, good practice and lessons learned among NRAs
- Develop more realistic incident scenarios for pan-European exercises

Art 13a Expert Group

- Chaired by ENISA
- NRAs from the EU Member States and EC as observer
- Meet three times a year and online
- Goal - work towards a harmonised approach
- **Discuss** implementations of Art13a
- **Develop** guidelines and procedures about Art13a
- **Share** information on incidents, discuss lessons learned and how to address certain incident patterns

Output Art 13a EG

- Non-binding technical guidance for NRAs
- Consensus among the NRAs

- Technical Guideline on Security Measures
  - 7 security domains/areas
  - 25 security objectives

- Technical Guideline on Incident Reporting
  - Thresholds for reporting
  - Root cause classification
  - Reporting procedure

eComms Reference Group

- includes European electronic communications providers
- addresses topics across the Electronic Communications area, eg:

➢ security measures and incident reporting (Art 13a)

➢ Personal data protection and breach reporting (Art4)

➢ Botnets

➢ Interconnections

eComms Reference Group

The reference group is set up by ENISA to:

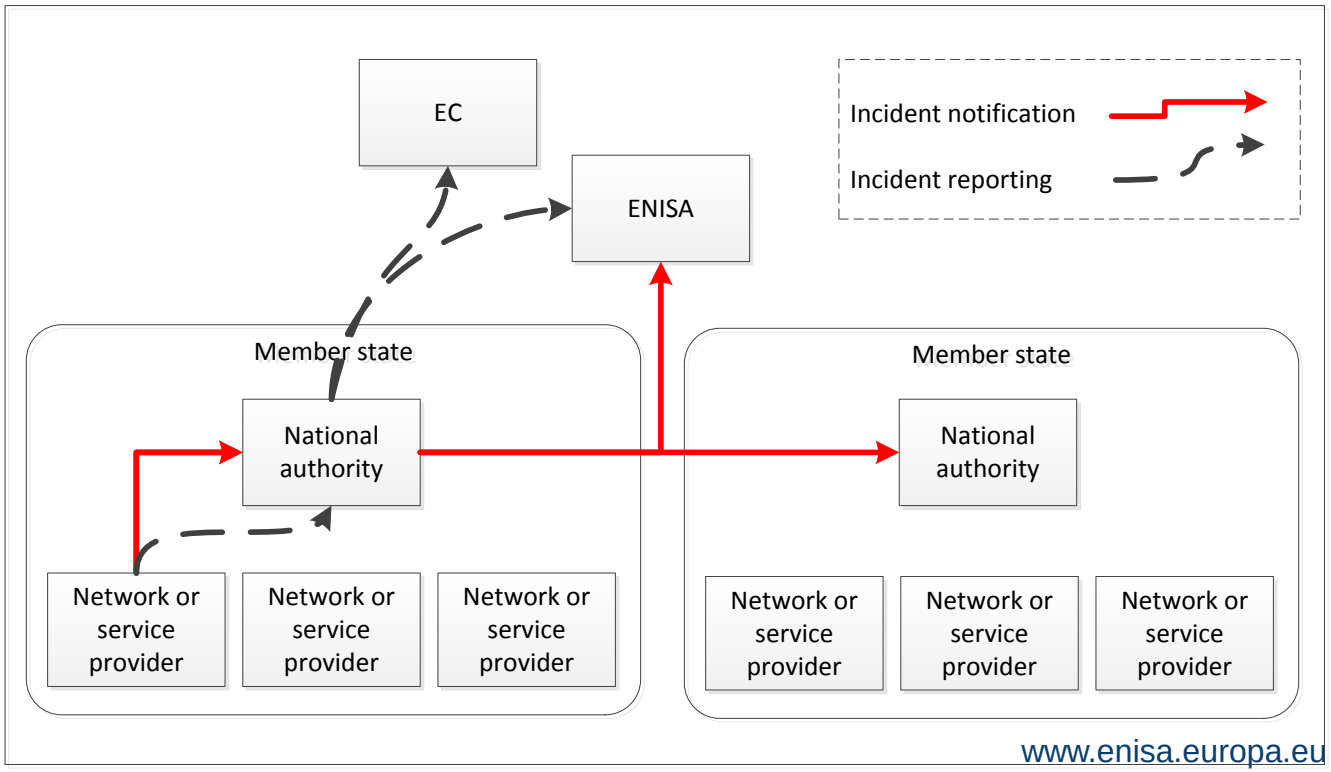
- give feedback on experiences with regulation and supervision to ensure effectiveness and efficiency,
- exchange and discuss about threats, vulnerabilities and incidents, to ensure that there is a common understanding about common threats, vulnerabilities and incidents, across the EU,
- exchange and discuss best practices,
- point to gaps and issues that require attention from ENISA and/or government regulators (NRAs, DPAs, security agencies, ministries, European commission etc), to ensure that important topics and issues are being addressed.

Annual reporting 2012

…for the first time in the EU, National Regulatory Authorities reported about security incidents at an EU level (ENISA and the EC)

Annual summary reporting 2012

- Scope: only relatively large outages
- Reported to ENISA and the EC in May 2012
- ENISA published a summary the 8th of October 2012

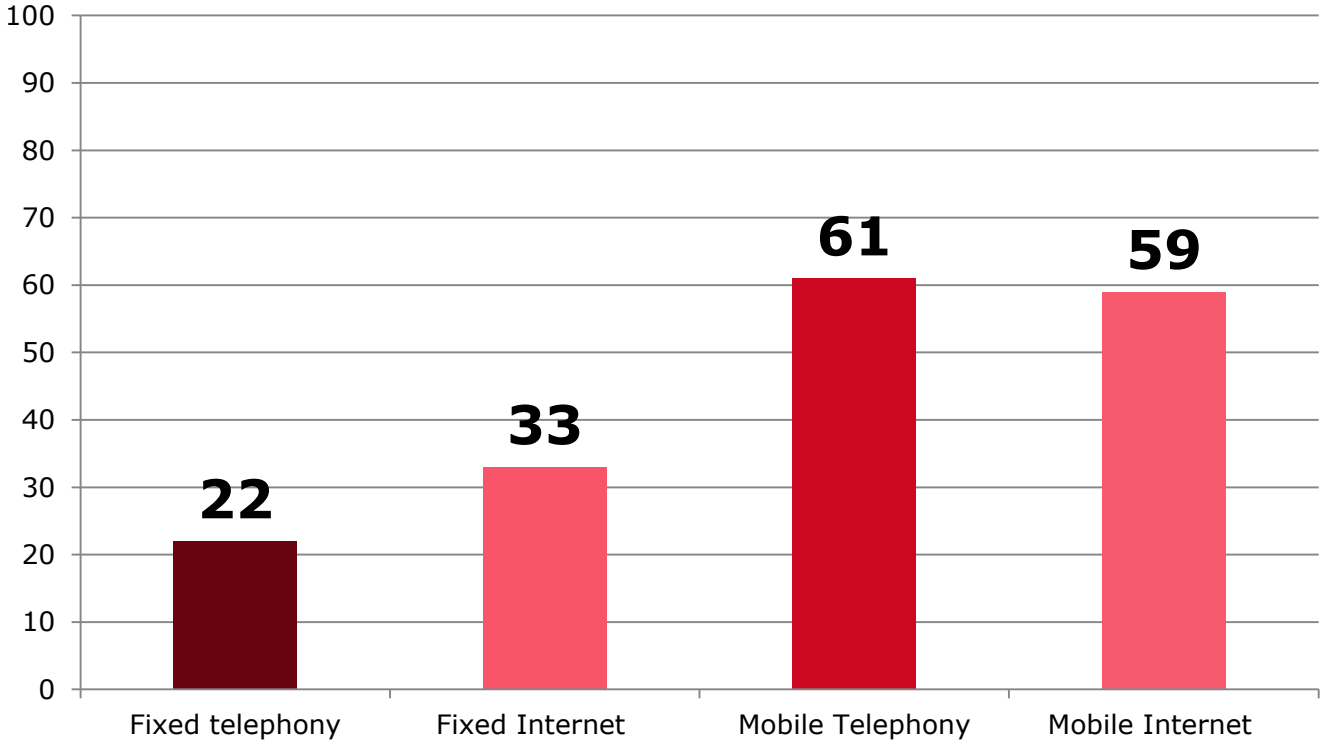


Annual analysis by ENISA

- Statistical analysis of incidents
- Aggregated view of resilience and security of electronic communication networks and services
- No comparison or information about individual incidents, providers or member states

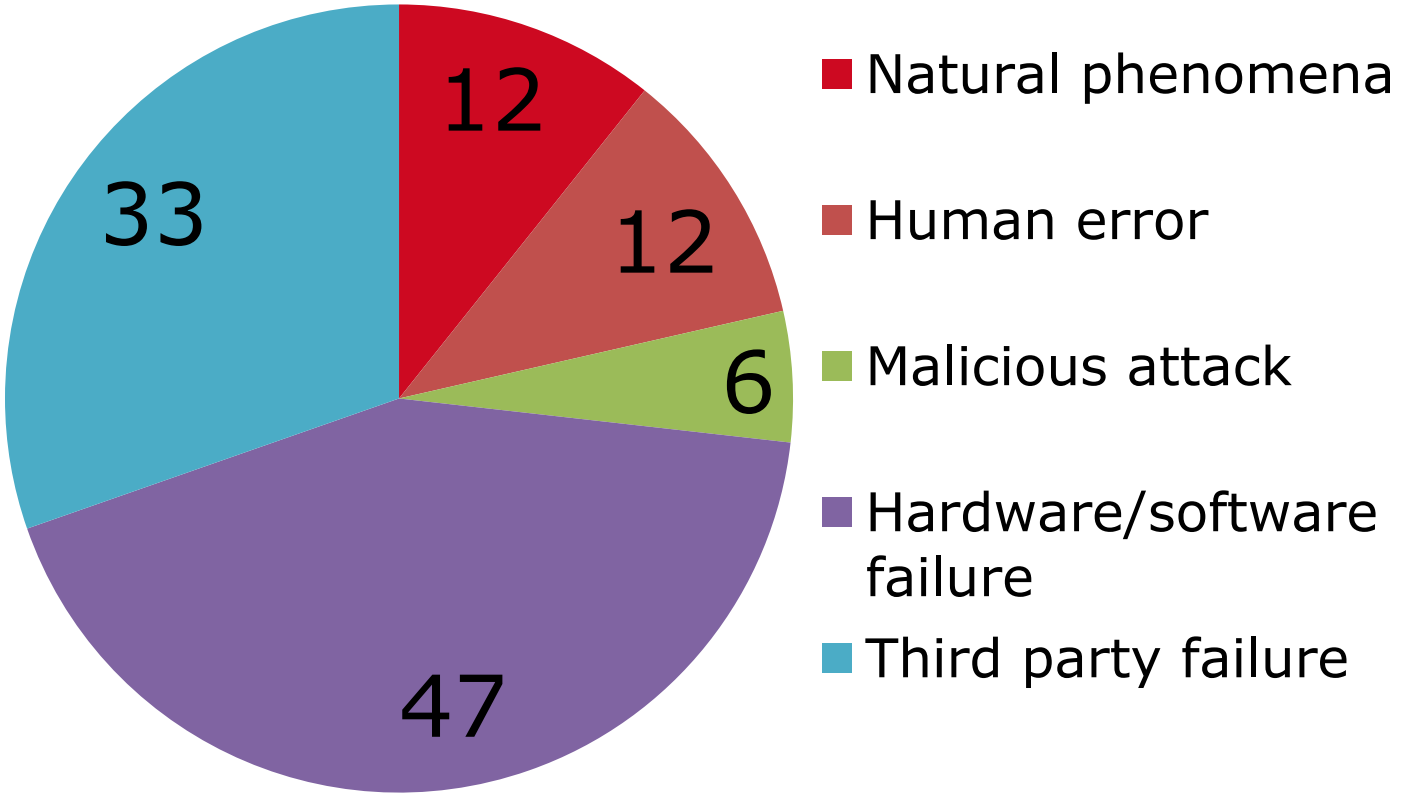
Incidents per service

- 60% involved impact on mobile networks
- 6% with impact on interconnections, 33% with impact on 112



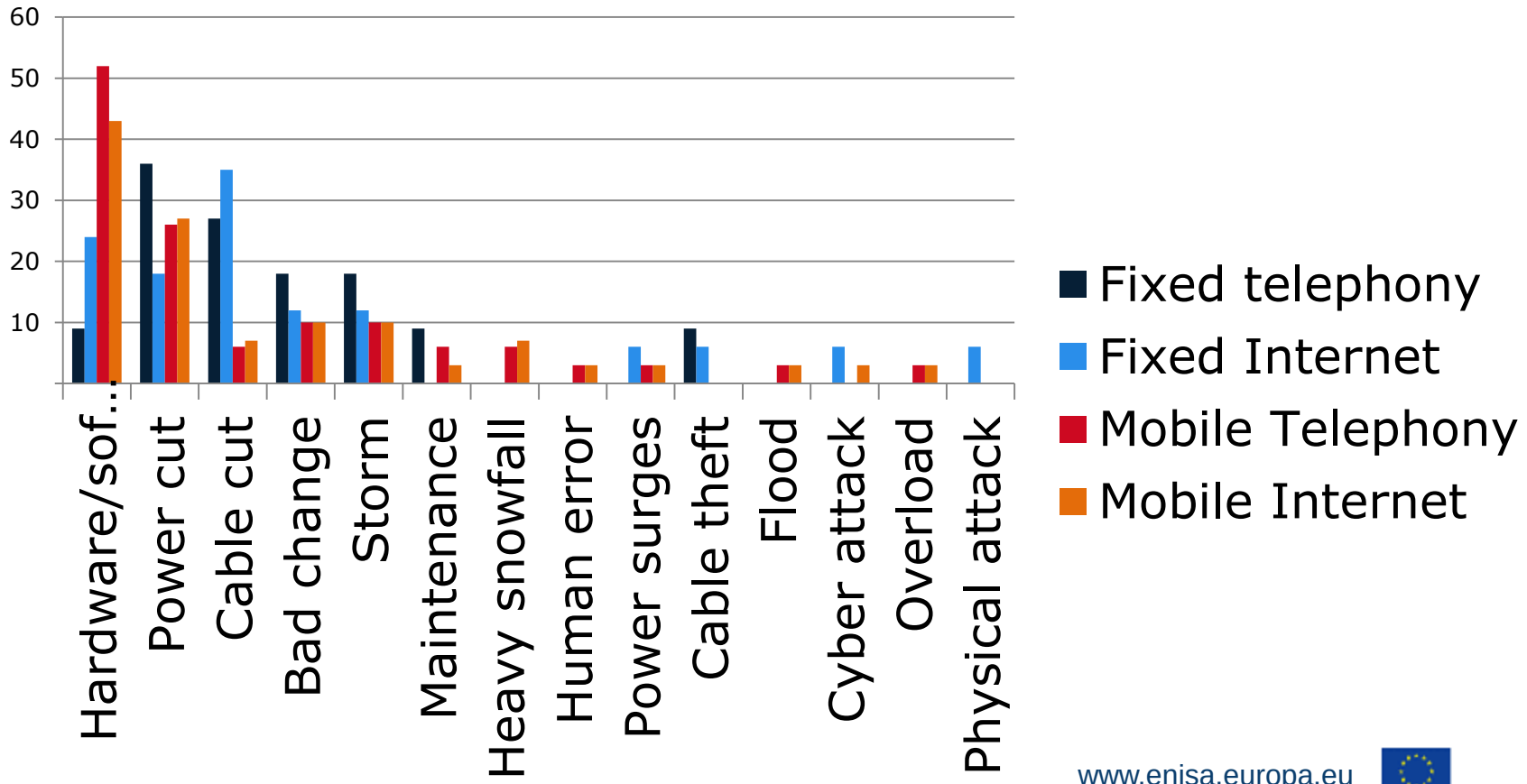
Root cause categories

- Most incidents were caused by hardware/software failure, or third party failure



Detailed causes per service

- Hardware/software failure more common in mobile outages



Annual reporting 2013

- Concerns reports on significant incidents in the ecomms sector during 2012
- NRAs reported about 80 significant incidents to ENISA and EC
- ENISA is now analysing the incident reports
- In June an analysis report will be published
- Already some conclusions can be drawn:

- Mobile networks are more affected by incidents than fixed networks
- The single most common root cause is hardware/software failure
- More conclusions will follow in the ENISA report in June