Annual Incident Reports 2012

Analysis of Article 13a annual incident reports

August 2013

www.enisa.europa.eu

About ENISA

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

Authors

Dr. Marnix Dekker, Christoffer Karsberg, Matina Lakka

Contact

For contacting the authors please email to resilience@enisa.europa.eu

For media enquires about this paper, please email to press@enisa.europa.eu.

Acknowledgements

For the completion of this report ENISA has worked closely with a group of experts from National Regulatory Authorities and ministries from across Europe. Listing the organizations (in not particular order): PTS (SE), Ministry of Economic Affairs (NL), FICORA (FI), Ofcom (UK), ANACOM (PT), ComReg (IE), EETT (GR), ADAE (GR), Centre for Cyber Security - CFCS (DK), RTR (AT), ANCOM (RO), CRC (BG), Ministry of Economics, Finance and Industry (FR), Bundesnetzagentur (DE), BIPT (BE), MITYC (ES), MPO (CZ), CTO (CZ), CERT LT (LT), TRASR (SK), ILR (LU), PECSRS (SI), MCA (MT), Ministry of Economic Development (IT), OCECPR (CY), NPT (NO), ETSA (EE), NMIAIAD (HU), ITSIRI (LV), OEC (PL), APEK (SI), Teleoff (SK), OFCOM (CH), HAKOM (HR)

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 Regulation (EU) No 526/2013. 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.

Executive summary

Yearly ENISA publishes an annual report about significant incidents in the electronic communications sector, which are reported to ENISA under Article 13a of the Framework Directive (2009/140/EC). This report covers the incidents that occurred in 2012.

This report provides an aggregated analysis of the incident reports about severe outages, looking at the impact of incidents, root cause categories and detailed causes. It does not include details about individual countries, individual providers, or individual incidents.

In total 18 countries reported 79 significant incidents, 9 countries reported no significant incidents., Below we summarize the main conclusions that can be drawn from the incident reports.

- Most incidents affected mobile telephony or mobile Internet (about 50 % of the incidents respectively). Incidents affecting mobile telephony or mobile Internet also affected most users (around 1,8 million users per incident). This is consistent with the high penetration rate of mobile telephony and mobile Internet.
- In 37 % of the incidents there was an impact on the emergency number 112.
- For most incident reports the root cause was “System failures” (75 % of the incidents). This was the most common root cause category also for each of the four services (fixed and mobile telephony and fixed and mobile Internet). In the category “System failures”, hardware failures were the most common cause, followed by software bugs. The assets most often affected by system failures were switches (e.g. routers and local exchange points) and home location registers.
- Incidents categorized with root cause third party failures, mostly power supply failures, affected around 2.8 Million user connections on average. Incidents involving the detailed cause overload affected around 9.4 million user connections on average.
- Incidents caused by natural phenomena (mainly storms and heavy snowfall) lasted the longest: around 36 hours on average.
- Incidents caused by overload followed by power failures respectively had most impact in terms of number of users affected times duration.
- Overall, switches and home location registers were the network components or assets most affected by incidents.

ENISA, together with the National Regulatory Authorities (NRAs) of the different EU Member States, discusses specific incidents in more detail in the Article 13a Expert Group. Where needed ENISA drafts technical guidance for NRAs and providers about mitigating incidents. For example, following last year’s report, ENISA is now drafting recommendations on power supply dependencies and national roaming for resilience.

ENISA publishes an annual report to provide industry and government bodies in the EU with data about significant incidents. The next annual report will be published in summer 2014, covering incidents that occurred in 2013.

We thank the regulators and the EC for a fruitful collaboration and we are looking forward to leveraging this kind of reporting to further improve the security and resilience of the electronic communication networks in the EU electronic communications sector and more generally for supervision of security in other critical sectors.

Table of Contents

1 Introduction

For the second time in the EU significant security incidents were reported to ENISA and the European Commission, under Article 13a of the Framework Directive (2009/140/EC), a new article introduced in the 2009 reform of the EU legal framework for electronic communications. In this document, ENISA analyses the 79 incident reports of severe outages of electronic communication networks or services that were submitted for 2012. This year's reports were also compared with last year's annual reporting. The Executive Summary of this report provides a snapshot of this analysis.

Note that in this document ENISA does *not* provide details from the individual incident reports. The analysis is only an aggregation in terms of averages and percentages across the EU. ENISA does not make any references here to specific countries or specific providers. The incidents are discussed in more detail in the Article 13a Expert Group.

This document is structured as follows. Section 2 and Section 3 briefly summarize Article 13a and the details of the technical implementation of Article 13a, as agreed in the Article 13a Expert Group by the different NRAs of the EU Member States. Section 4 analyses the incidents which were reported, and this paper concludes with some general conclusions (Section 5) which follow from the incidents. For the interested reader, the annex contains data about root causes and detailed causes per service as well as the detailed causes and impact for Circuit Switched Telephony and VoIP respectively.

2 Article 13a of the Framework Directive: 'Security and Integrity'

The reform of the EU legal framework for electronic communications, which was adopted in 2009 and was transposed by most EU countries around May 2011, adds Article 13a to the Framework Directive. Article 13a addresses the security and integrity[1] of public electronic communications networks and services. The legislation concerns National Regulatory Authorities (NRAs) and providers of public electronic communications networks and services (providers).

Article 13a states:

- Providers of public electronic communications networks and services should take measures to guarantee security and integrity of their networks.
- Providers must report to competent national authorities about significant breaches of security or integrity.
- National Regulatory Authorities should notify ENISA and national authorities abroad when necessary, for example in case of incidents with cross-border impact.
- Annually, National Regulatory Authorities should submit a summary report to ENISA and the European Commission (EC) about the incidents.

The incident reporting flows are shown in the diagram below. This document analyses the incidents that have been reported to ENISA and the EC (the black dashed arrow).

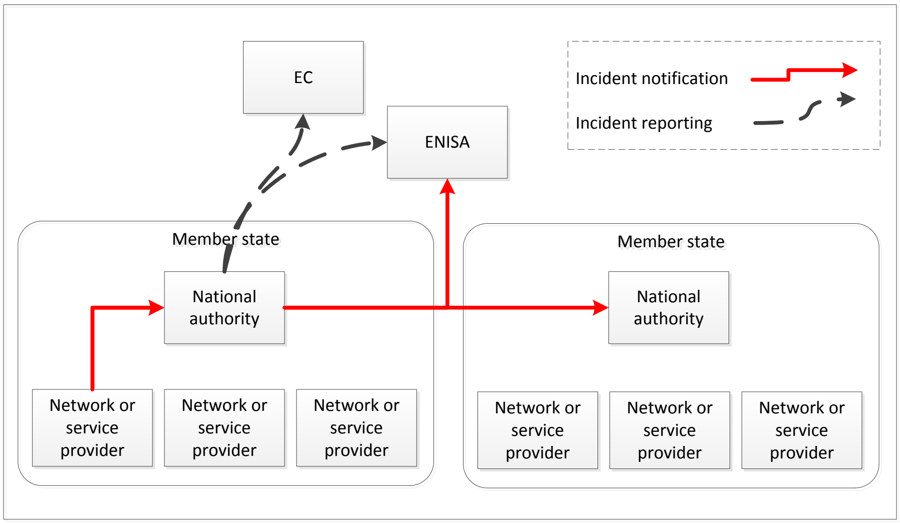

EC
ENISA
Incident notification
Incident reporting
Member state
National authority
Network or service provider
Network or service provider
Network or service provider
Member state
National authority
Network or service provider
Network or service provider
Network or service provider

Figure 1: Incident reporting in Article 13a.

[1] Here integrity means network integrity, which is often called availability or continuity in information security literature.

3 Article 13a Expert Group and Incident Reporting Procedure

In 2010, ENISA, Ministries and NRAs initiated a series of meetings (workshops, conference calls) to achieve a harmonised implementation of Article 13a of the Framework directive. In these meetings, a group of experts from NRAs, called the Article 13a Expert Group, reached agreement on two non-binding technical documents providing guidance to the NRAs in the EU Member States :

- Technical Guidelines for Incident Reporting and
- Technical Guidelines for Minimum Security Measures.

The Article 13a Expert Group continues to meet several times a year to discuss the implementation of Article 13a (for example, on how to supervise the electronic communications sector) and to share knowledge and exchange views about past incidents, and how to address them.

3.1 Technical Guidelines on Incident reporting

The last two years, NRAs have used version 1.0 of the Technical Guidelines on Incident Reporting. At the end of last year, in agreement with NRAs, ENISA amended and improved the reporting thresholds and the incident reporting template, to be used for the 2013 reporting. This was done in a separate document, describing the procedure for 2013 reporting.

From January 2013 the NRAs will be using version 2.0 of the Technical Guideline on Incident Reporting.

3.1.1 Services in scope

NRAs should report incidents affecting the following communication services and networks:

- Fixed telephony (e.g. PSTN, VoIP over DSL, Cable, Fiber, et cetera),
- Mobile telephony (e.g. GSM, UMTS, LTE, et cetera),
- Fixed Internet access (e.g. Dial up, DSL, Cable, Fiber, et cetera),
- Mobile Internet access (e.g. GSM, UMTS, LTE, et cetera)

NRAs may also report about incidents affecting other types of services.

3.1.2 Security incidents in scope

NRAs should report security incidents, which had a significant impact on the continuity of supply of electronic communications networks or services.

3.1.3 National user base

NRAs should provide estimates of the total number of users of each service in their country.

- For fixed telephony and Internet, NRAs should use the number of subscribers or access lines in their country.
- For mobile telephony, NRAs should use the number of active telephony SIM cards.
- For mobile Internet, NRAs should sum up[2]:
    1. The number of standard mobile subscriptions, which offer both telephony and Internet access, and which have been used for Internet access recently (e.g. in the past 3 months).
    2. The number of subscriptions dedicated for mobile Internet access, which are purchased separately, either standalone or on top of an existing voice subscription.

[2] Here we follow the definition agreed in the COCOM meetings.

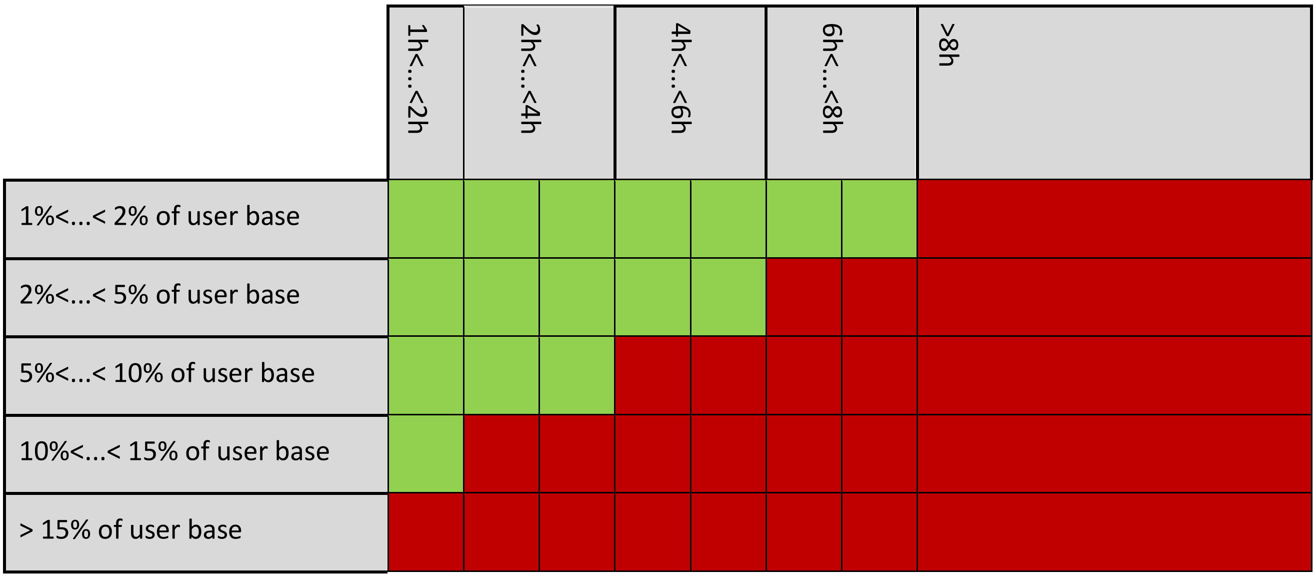
3.1.4 Thresholds

The threshold for annual summary reporting is based on the duration and the number of users of a service affected as a percentage of the national user base of the service.

NRAs should send an incident report, as part of the annual summary reporting, if the incident

- lasts more than an hour, and the percentage of users affected is more than 15%,
- lasts more than 2 hours, and the percentage of users affected is more than 10%,
- lasts more than 4 hours, and the percentage of users affected is more than 5%,
- lasts more than 6 hours, and the percentage of users affected is more than 2%, or if it
- lasts more than 8 hours, and the percentage of users affected is more than 1%.

The threshold should be understood 'per service'. In other words, if one incident involves impact on multiple services, then for one of the services the threshold should be passed. NRAs may also report incidents with an impact below the threshold.



	1h<...<2h	2h<...<4h		4h<...<6h		6h<...<8h		>8h
1%<...< 2% of user base	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟥
2%<...< 5% of user base	🟩	🟩	🟩	🟩	🟩	🟥	🟥	🟥
5%<...< 10% of user base	🟩	🟩	🟩	🟥	🟥	🟥	🟥	🟥
10%<...< 15% of user base	🟩	🟥	🟥	🟥	🟥	🟥	🟥	🟥
> 15% of user base	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥

Figure 2 *Threshold for annual summary reporting based on a combination of duration and the percentage of the national user base.*

3.1.5 Root cause categories

In the incident reports five categories of root causes have been distinguished.

- **Natural phenomena** – This category includes incidents caused by natural disasters. For instance storms, floods, heavy snowfall, earthquakes, and so on.
- **Human errors** - This category includes incidents caused by errors committed by employees of the provider.
- **Malicious attacks** - This category includes incidents caused by an attack, a cyber-attack or a cable theft e.g.
- **System failures** – This category includes incidents caused by a failure of hardware or software.
- **Third party failures** – This category includes incidents caused by a failure or incident at a third party.

3.1.6 Reporting procedure

In spring 2012 the European Commission agreed with the EU Member States (in meetings of the Communications Committee, COCOM) to do the first round of annual summary reporting on the 2011 incidents. The decision included a recommendation to use the reporting template agreed within the Article 13a Expert Group and published by ENISA. Following the COCOM meeting, ENISA implemented the technical procedure by deploying a basic electronic form based on the Article 13a guidelines for incident reporting. There was also an agreement that in the following years, annual reporting would be carried out by the end of February each year.

In the automn of 2012 ENISA developed an online incident reporting tool (called CIRAS), which replaces the electronic forms exchanged by email. The goal of CIRAS is to allow NRAs more control over the data reported and to improve the collection and aggregation of incident reports.

4 Analysis of the incidents

In total, all 28 EU Member States participated in this process. 18 countries reported in total 79 significant incidents, 9 countries reported there were no significant incidents and 1 country hadn't implemented incident reporting yet.

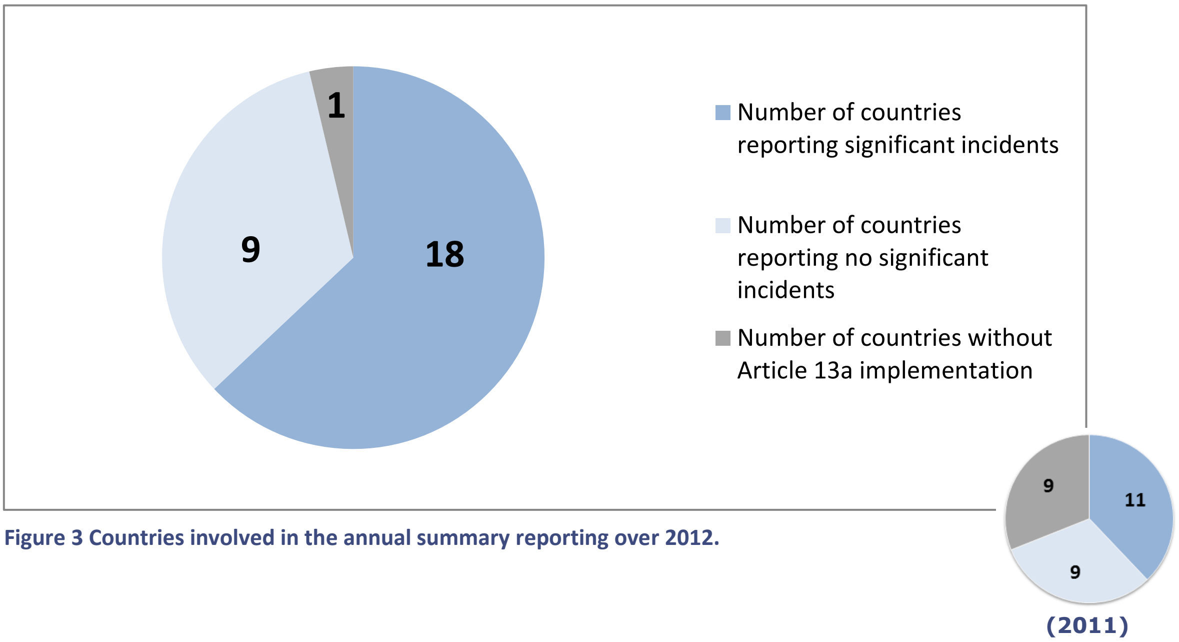


Figure 3 Countries involved in the annual summary reporting over 2012.

In this section the 79 reported incidents are aggregated and analysed. First, some examples of incidents are given (in Section 4.1), then the impact per service is analysed (in Section 4.2), then the impact per root cause category is analysed (Section 4.3), and in Section 4.4 detailed causes are examined. In Section 4.5 impact as a product of user connections affected and duration of the incidents is analysed and in Section 4.6 the components or assets affected by the incidents are considered.

At this point there is a need to stress that statistical conclusions based on these numbers should be drawn with care. The smaller incidents are not reported at an EU level and this means that the view is biased towards the larger incidents. Another remark is that the reporting to ENISA has only been carried out for two years, and this is not enough to draw conclusions on trends. However, where there are data from 2011, diagrams are displayed as a comparison.

4.1 Examples of incidents

In this section, we give some anonymized examples of inccidents, to give an idea of the different incidents that have been reported over the last two years.

4.1.1 Overload caused VoIP outage (hours, thousands, system failure)

In the shift from a temporary to a permanent network solution, voice over IP service were lost for 400 000 users. Basically the IMS[3] *became overloaded as a result of too many simultaneous registrations of customer devices. The provider had to limit registrations and was handling full traffic again after 14 hours.*

[3] IMS = IP Multimedia Core Network Subsystem, a functional architecture designed to enable providers to deliver a wide range of real-time, packet-based services.

4.1.2 Faulty upgrade halted IP-base traffic (hours, millions, human error)

An upgrade in a core router went seriously wrong, and caused a drop of all IP based traffic for the provider causing many services to go down, including the emergency number 112. This incident led to an outage of 17 hours affecting 3 million users. The provider downgraded to make the network stable. The post incident action was to change the routines for upgrades including new procedures for suppliers and integrators.

4.1.3 Cable theft causing fibre optic cable break (hours, thousands, malicious attack)

A fiber optic cable was cut off due to a cable theft attempt. The incident affected 70 000 fixed telephony users and 90 000 fixed Internet users for 10 hours. During repairs a temporary path was established.

4.1.4 DDoS attacks on DNS affected mobile Internet (hours, millions, malicious attack)

A series of Distributed Denial of Service attacks targeted a provider's domain name service. Up to 2,5 million mobile Internet users were affected during 1-2 hours. The attacking IP-addresses were tracked and blocked, the load balancing units were restarted and the traffic could be recovered. As post-incident actions additional DNS servers were installed, configuration changes were made on firewalls and hardware was expanded to withstand similar attacks.

4.1.5 Big storm affecting power supply causing large scale outage (days, millions, natural disaster)

A severe storm hit several countries. The storm had a major impact on the power grid infrastructure and to a limited extent also on mobile network equipment (like mobile base stations). The prolonged power cuts eventually caused many mobile base stations to run out of power. As a result around a million users were without mobile communication services for 24 hours, and in some cases up to two weeks.

4.1.6 Configuration error (hours, millions, configuration error)

An employee of a fixed telephony provider made a configuration error. The error prevented fixed telephony users to make outgoing international phone calls to Western European countries for 4 hours. The incident was resolved after a reconfiguration and a reboot.

4.1.7 Vandalism by former employee affected DSL (days, thousands, malicious attack)

A former employee of a provider deliberately set fire to a switching system, which was used for providing fixed Internet service to around 10.000 subscribers. The incident was resolved by replacing the switch. Around 36 hours later the fixed Internet service was working again.

4.1.8 Faulty software update affected mobile telephony (hours, thousands, software failure)

A provider applied a regular software update at a Home Location Register (HLR) which turned out to be faulty. The failure at the HLR impacted mobile telephony and Internet services. The incident affected about half of the provider's customers and lasted around 8 hours.

4.1.9 Submarine cable cut from anchorage (hours, thousands, third party)

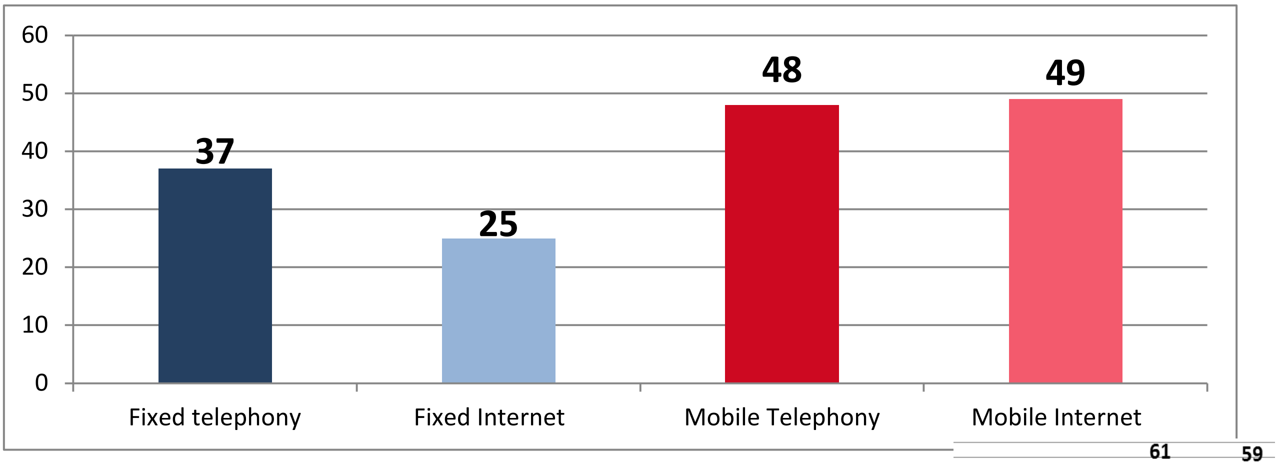
A ship's anchoring damaged one *of four submarine cables connecting two islands. Contingency plans were triggered quickly, which meant that only a smaller number of users were affected.*

4.2 Impact

This section focusses on the impact of the incidents on the electronic communication services.

4.2.1 Incidents per service

Figure 4 shows which percentage of incidents affected which services. Most incidents have an impact on two or more services (which is why the percentages in the chart add up to 152%).



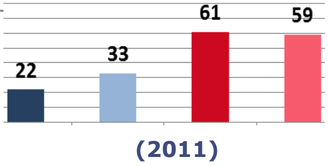


Figure 4 Incidents per service (percentage)

Most incidents (around 48%) affected mobile telephony or mobile Internet. This would suggest that mobile services are more at risk of large-scale outages. We drew a similar conclusion last year.

4.2.2 Number of users affected per incident per service

Figure 5 shows the average number of users affected, per incident, per service (in 1000s).

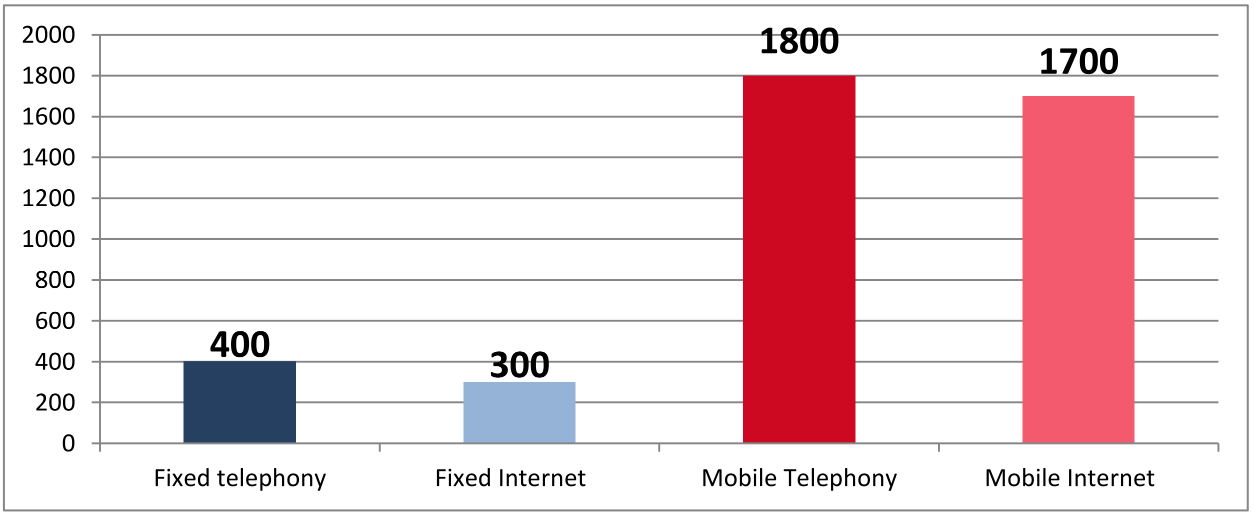
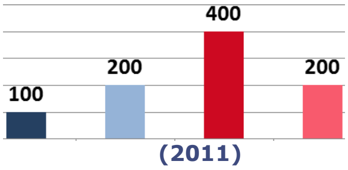


Figure 5 Average number of users affected per incident per service (1000s).



Incidents affecting mobile telephony and mobile Internet involve on average 1,8 million users. This is partly due to the fact that mobile telephony has more customers (on average 110% of the population for mobile telephony, compared to 50% for fixed telephony). Note that the EU averages in this calculation are not always representative for the sizes of incidents that could occur nationally regarding users affected, because of differences in national network topologies. Also, since the thresholds for reporting to ENISA and the EC are based on the percentage of national users affected, smaller outages are underrepresented in the EU averages.

4.2.3 Percentage of the national user base affected

Figure 6 shows the percentage of the national user base affected, on average per incident, per service.

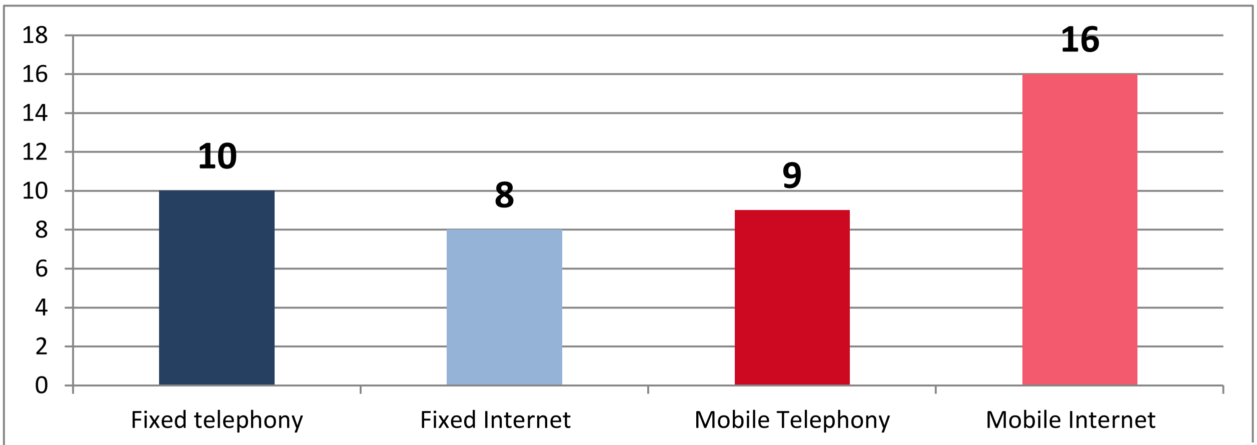
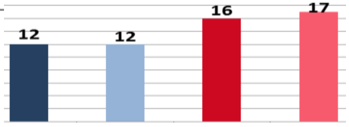


Figure 6 Number of users affected per incident per service (percentage).



(2011)

On average, incidents affecting mobile internet affect 16% of the users. This is more than the percentages for the mobile telephony and the fixed communication services. This would suggest that, not only mobile Internet services are more vulnerable, but also that a larger portion of the users is affected in the incidents that were reported.

4.2.4 Impact on emergency services and interconnections

In figures 7 and 8 we show the impact on emergency services and interconnections respectively.

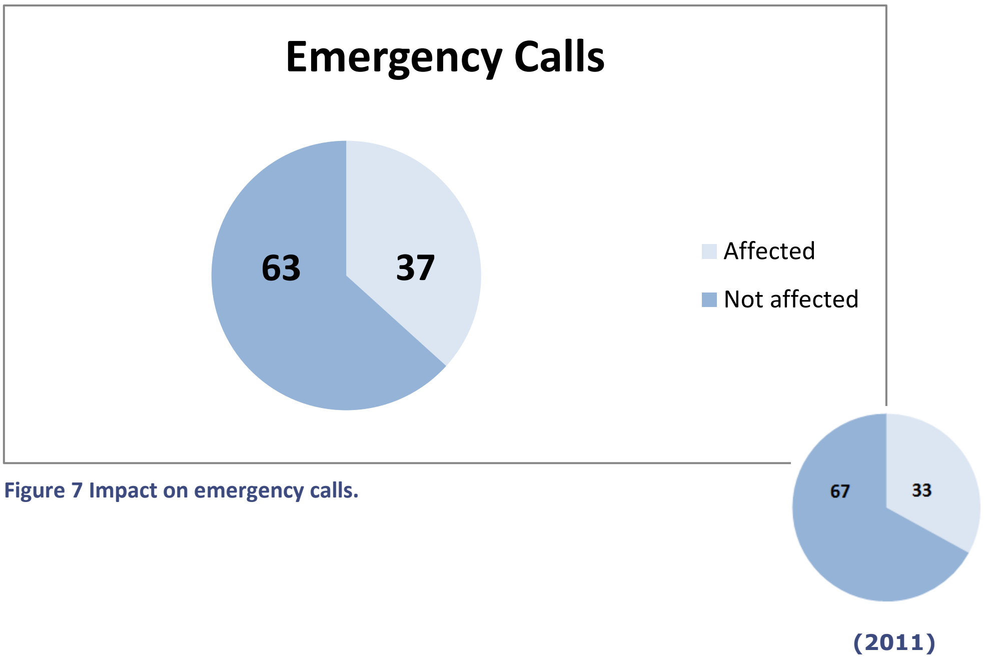


Figure 7 Impact on emergency calls.

In 37 % of the incidents there was impact on emergency calls - i.e. the possibility for users to contact emergency call-centres using the emergency number 112.

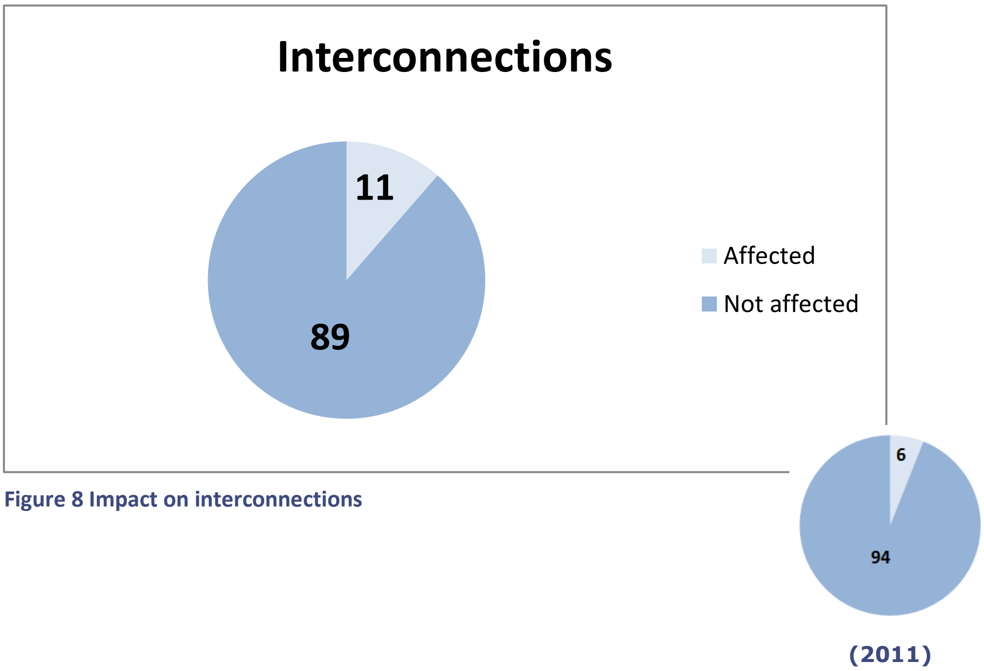


Figure 8 Impact on interconnections

In 11 % of the incidents there was an impact on interconnections to other providers.

4.3 Root cause categories

This section shows the impact of incidents, per root cause category.

4.3.1 Incidents per root cause category

Figure 9 shows the percentage of incidents per root cause category.

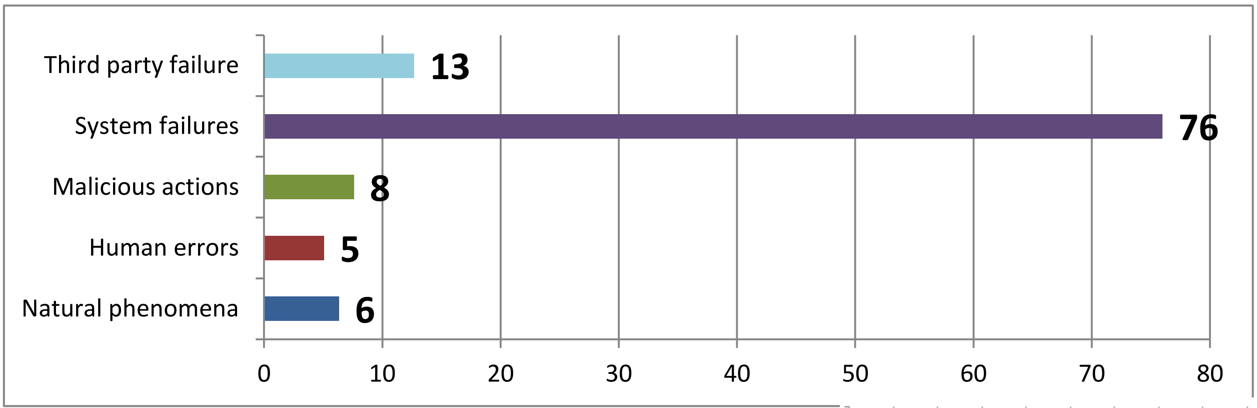
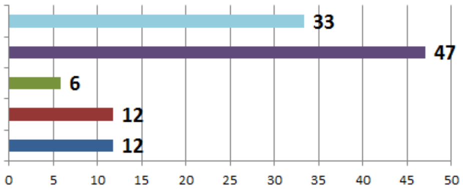


Figure 9 Incidents per root cause category (percentage).



(2011)

Most of the incidents fall in the rootcause category ‘System failures’ (76%). Note that the numbers add up to more than 100% because for a few incidents multiple root cause categories were indicated.

4.3.2 Average duration of incidents per root cause category

Figure 10 shows the average duration of incident per root case category.

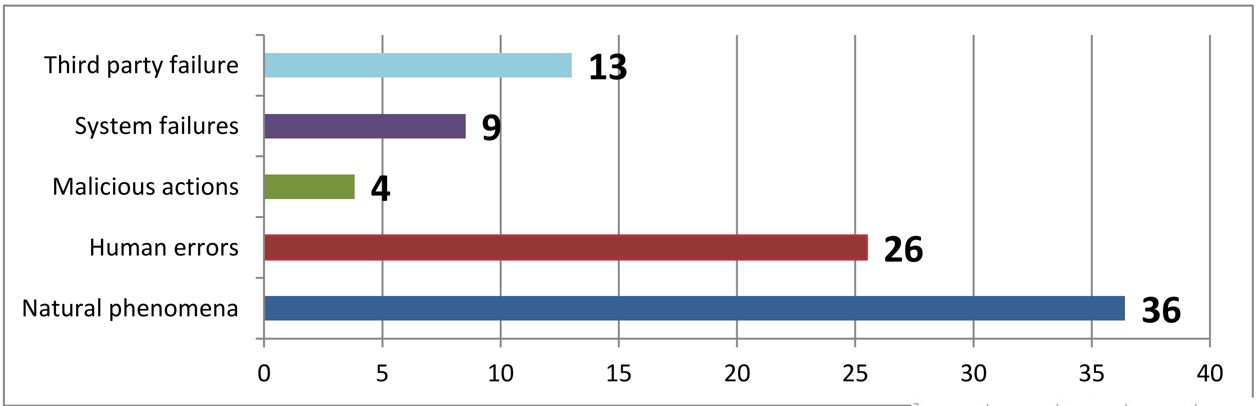
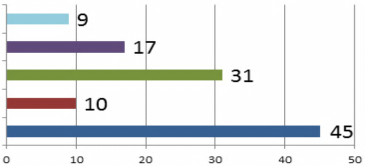


Figure 10 Average duration of incidents per root cause category (hours).

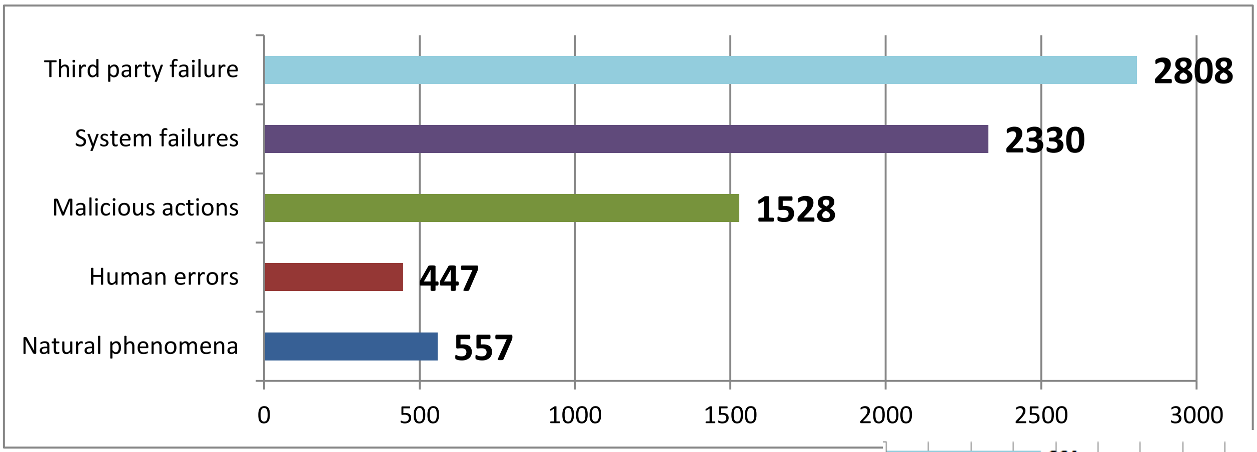


(2011)

Natural phenomena need the longest recovery time compared with the other root cause categories: an average of 36 hours. Also incidents in the root cause category 'Human Error' needed long recovery time, 26 hours in average.

4.3.3 Average number of user connections affected per root cause category

Figure 11 shows the average number of affected user connections in each incident for a certain root cause category. Note that a single user could have access to multiple services, so in certain incidents the affected users are counted multiple times. For this reason we count the number of user connections affected per service.



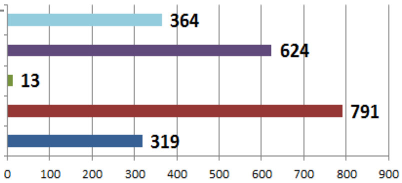


Figure 11 Average number of user connections affected per incident per root cause

(2011)

Although incidents caused by natural phenomena lasted longest (36 hours on average), the number of user connections in these cases was relatively limited (on average 560.000 connections) compared to other root cause categories. The incidents caused by third party failures affected most connections (around 2.8 Million), and they lasted fairly long (on average 13 hours). A high proportion of these incidents (60%) were caused by failures related to power supply. It is difficult to draw conclusions on why the number of affected connections was so high this year. There were some incidents that generated a very high number of affected user connections, mainly five incidents on mobile networks that affected a range of 4 million to 50 million user connections.

4.4 Detailed causes

In this section, instead of looking at the five root cause categories, we examine initial causes and subsequent causes triggering the incident. For example, when a storm led to a power cut which leads to a network outage, then for this incident both power cut and storm are counted as detailed causes. We call them: “detailed causes”.

4.4.1 Detailed causes

Figure 12 shows the detailed causes of incidents.

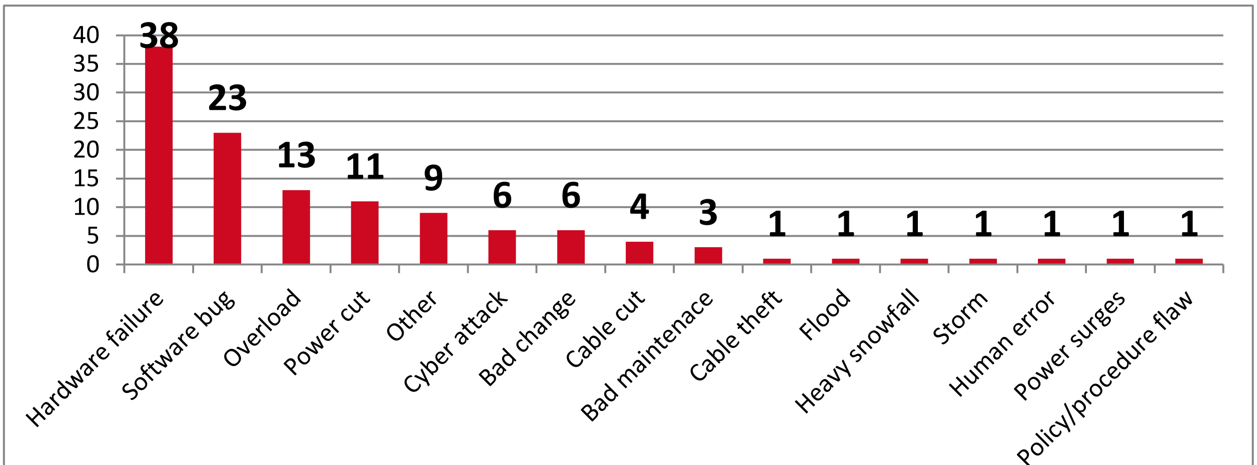
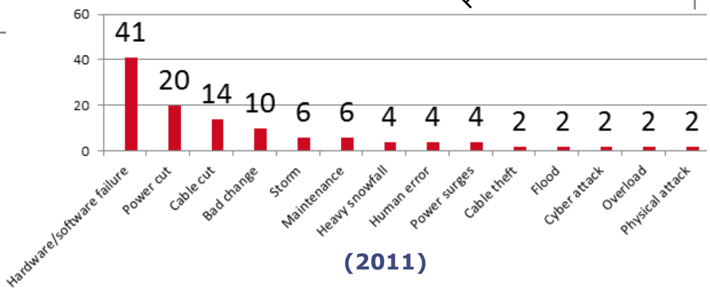


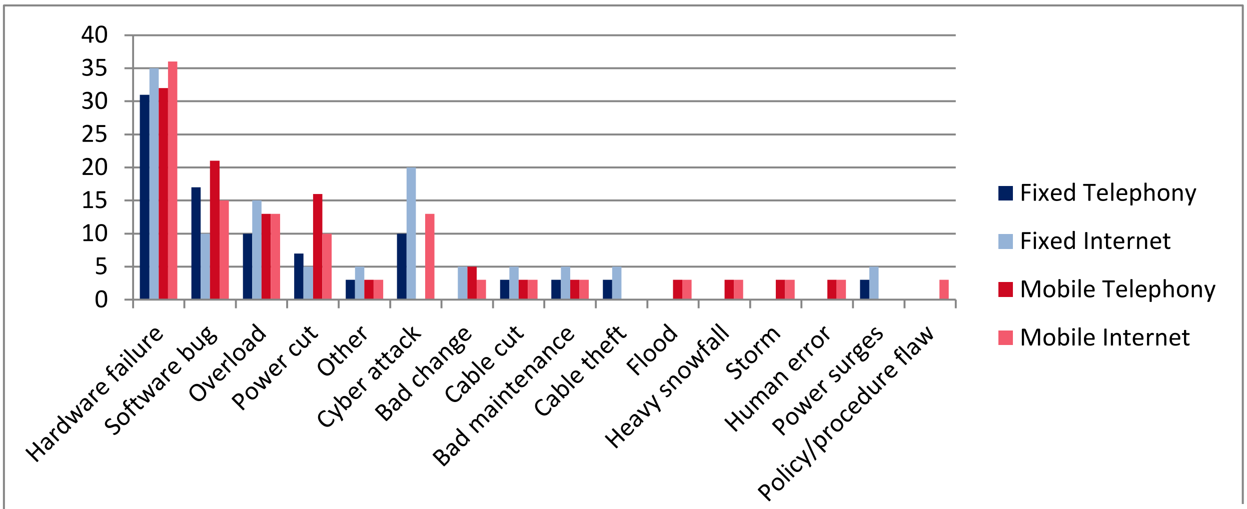
Figure 12 Detailed causes of reported incidents



Hardware failure was the most common cause, followed by software bugs.

4.4.2 Detailed causes per service

Figure 13 shows the causes of incidents per service.



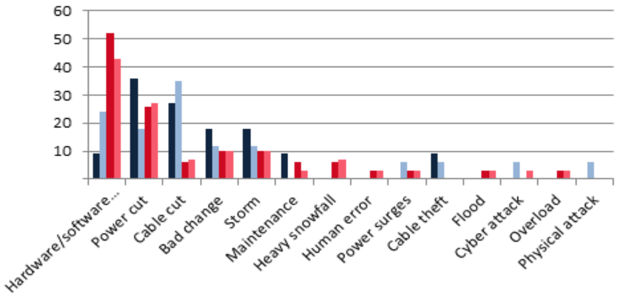


Figure 13 Detailed causes per service

(2011)

For incidents in all four services, hardware failure was the most common cause. The second most common cause for fixed telephony was software bug. Half of those incidents affected VoIP. For fixed Internet, cyber attack was the second most common cause. For mobile telephony and mobile internet the second most common cause was a software bug.

4.4.3 Average duration of incidents and number of user connections affected per detailed cause

Figure 14 shows the average duration of the incidents, per detailed cause[4].

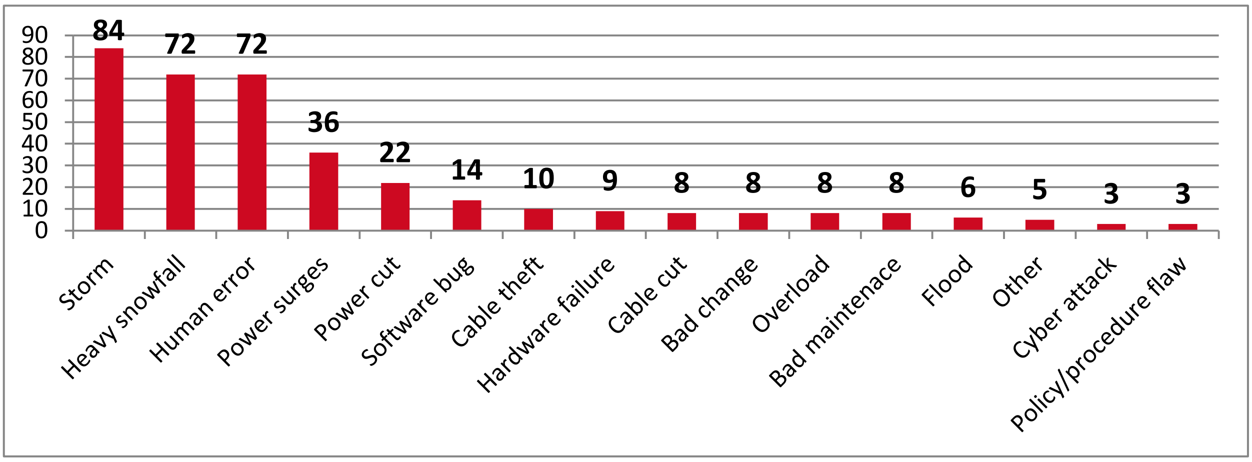


Figure 14 Average duration of incidents per detailed causes (hours).

Incidents caused by bad weather, mainly storms and heavy snowfall, had the longest duration.

Figure 15 shows the average number of user connections affected, per detailed cause.

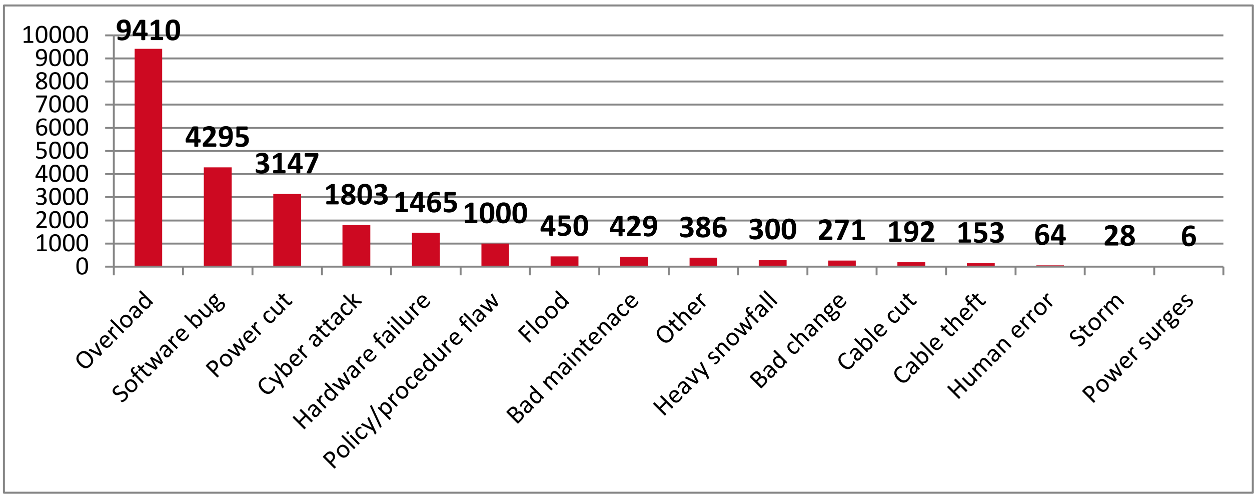


Figure 15 Average number of user connections affected per incident per detailed cause (1000s).

Overload was the cause affecting by far most user connections, more than 9 million connections on average per incident. In second and third place came software bugs with 4 million affected connections and power cuts with 3 million connections.

[4] Note that ENISA does not have comparable data from the 2011 incidents.

4.5 Impact in user hours

This year we also show the impact of the incidents in terms of the product of connections affected and the duration of the incident: We abbreviated this as "user-hours lost".

4.5.1 User hours lost per root cause category

Figure 16 shows the average impact in user-hours from incidents per root cause category.

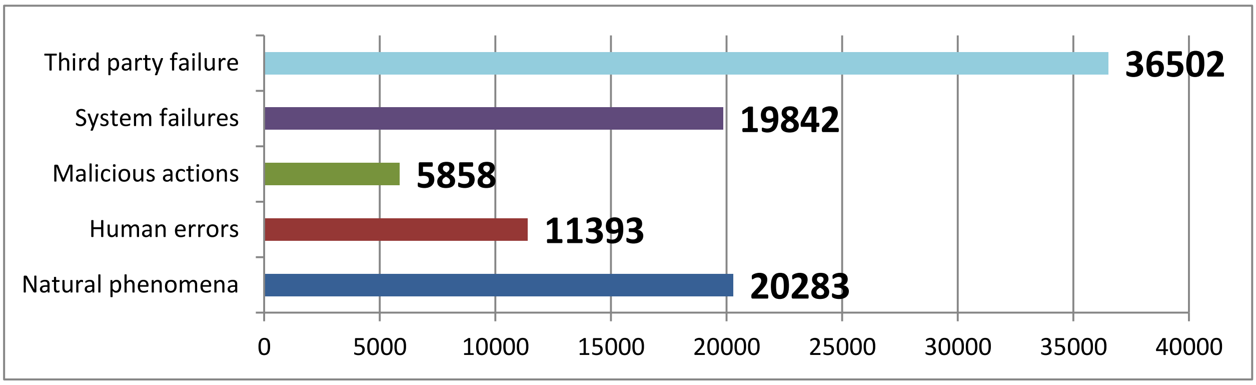


Figure 16 Average user-hours lost per incident per root cause category.

The root cause category third party failure had most impact in terms of user-hours lost followed by natural phenomena.

4.5.2 User-hours lost per detailed cause

Figure 17 shows the impact from the detailed causes in user-hours.

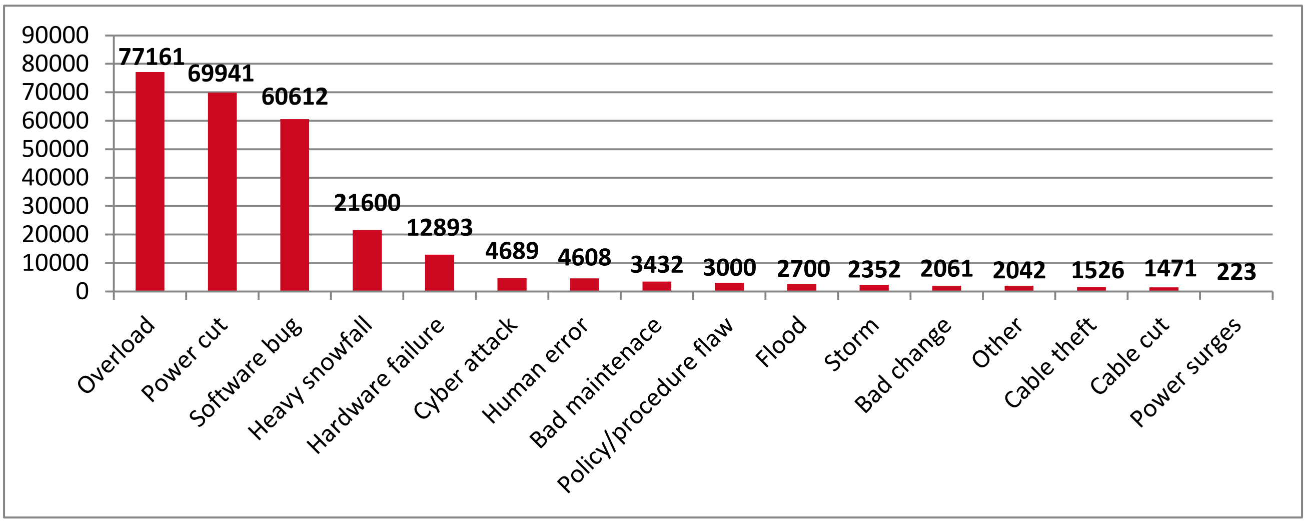


Figure 17 Average impact in user/hours of incidents per detailed cause.

Overload is the detailed cause that has most impact in terms of user hours lost, followed by power cuts followed and software bugs.

4.6 Assets affected

This year we also detail which components or assets of the electronic communications networks were affected by the incidents.

4.6.1 Assets affected overall

Figure 18 shows overall what assets were affected by the incidents.

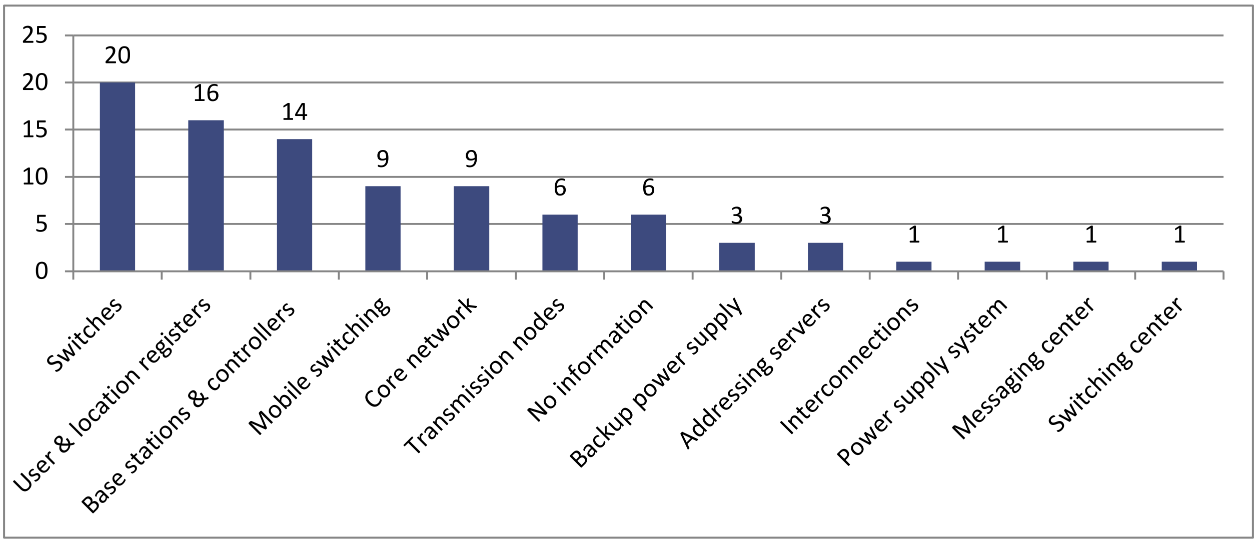


Figure 18 Assets affected by the incidents (percentages).

Switches were the assets most affected, followed by user and location and mobile network base stations.

4.6.2 Affected assets by system failures

System failures is the most common root cause category. In Figure 19 we show which assets were affected in these incidents.

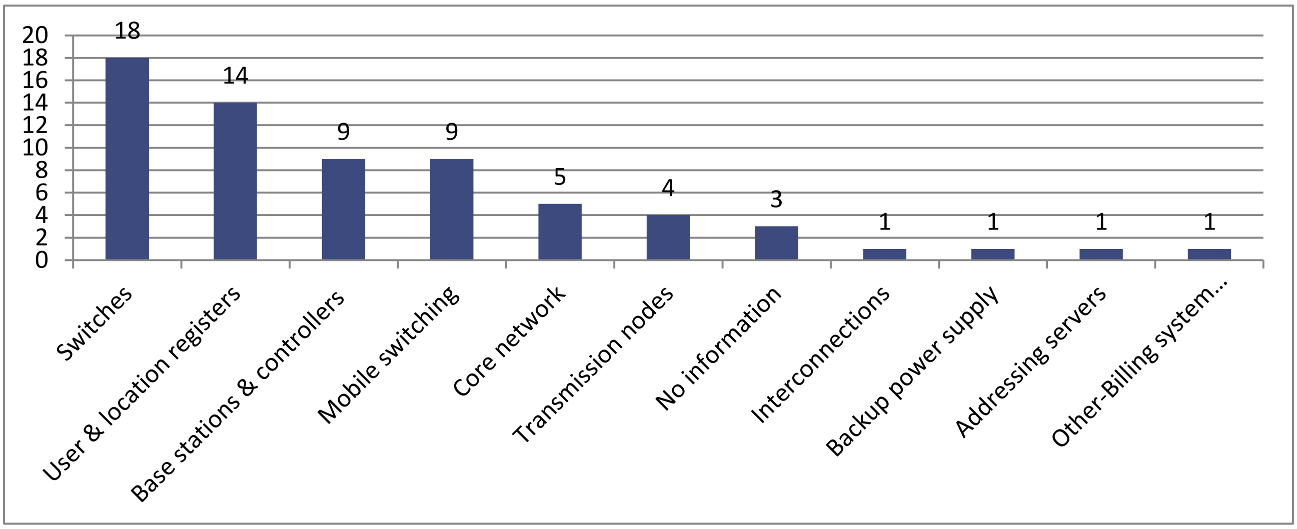


Figure 19 Assets affected in case of system failures (percentages).

System failures most often affected switches, user and location registers and base stations.

5 Conclusions

In this document ENISA summarized how the incident reporting scheme, mandated by Article 13a of the Framework Directive (2009/140/EC), was implemented across the EU and analysed the incident reports. ENISA and the EC received as part of the second round of reporting: 79 reports about major incidents that occurred in 2012.

From the 79 significant incidents reported to ENISA and the EC, the following conclusions can be drawn.

- **Mobile networks most affected:** Most incidents affected mobile telephony or mobile Internet (about 50 % of the incidents respectively).
- **Mobile network outages affect many users:** Incidents affecting mobile telephony or mobile Internet affected most users (around 1,8 million users per incident). This is consistent with the high penetration rate of mobile telephony and mobile Internet.
- **Emergency Service are affected by incidents**: In 37 % of the incidents there was impact on emergency calls using the emergency number 112.
- **System failures are the most common root cause:** Most incidents were caused by root causes in the category “System failures” (75 % of the incidents). This was the most common root cause category also for each of the four services (fixed and mobile telephony and fixed and mobile Internet). In the category “System failures”, hardware failures were the most common cause, followed by software bugs. The assets most often affected by system failures were switches (e.g. routers and local exchange points) and home location registers.
- **Third party failures and overload affect many users:** Incidents categorized with the root cause third party failures, mostly power supply failures, affected around 2.8 Million user connections on average. Incidents involving the detailed cause overload affected around 9.4 million user connections on average.
- **Natural phenomena cause long lasting incidents:** Incidents caused by natural phenomena (mainly storms and heavy snowfall) lasted around 36 hours on average.
- **Overload and power failures have most impact:** Incidents caused by overload followed by power failures respectively had most impact in terms of number of users times duration.
- **Switches and home location registers most affected by incidents:** Overall, switches and home location registers were the network components most affected by incidents.

ENISA, in the context of the Article 13a Expert Group, will discuss specific incidents in more detail with the NRAs, and if needed, discuss and agree on mitigating measures.

ENISA would like to take this opportunity to thank the NRAs, the European Member States and the European Commission for the fruitful collaboration, which has allowed for an efficient and rapid implementation of the incident reporting process. We believe that this process (Article 13a) is a good example for supervision of cyber security in other sectors. In fact, the proposal for a cyber security directive, rececntly proposed by the EC, explicitly mentions that the Framework directive was used as a model, and Article 14 of that proposal is very similar to Article 13a. ENISA is looking forward to leveraging this kind of reporting to assist the EU Commission and the Member States in further improving the security and resilience of the electronic communication networks in the EU.

References

Related ENISA papers

- The Article 13a WG technical guidelines on incident reporting and on minimum security measures: https://resilience.enisa.europa.eu/article-13
- ENISA's report about the 2011 incidents, reported under Article 13a: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/annual-reports/annual-incident-reports-2011
- ENISA's whitepaper on cyber incident reporting in the EU shows Article 13a and how it compares to some other security articles mandating incident reporting and security measures: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/cyber-incident-reporting-in-the-eu
- For the interested reader, ENISA's 2009 paper on incident reporting shows an overview of the situation in the EU 4 years ago.

EU legislation

- Article 13a of the Framework directive of the EU legislative framework on electronic communications: http://ec.europa.eu/information_society/policy/ecomm/doc/140framework.pdf
- The electronic communications regulatory framework (incorporating the telecom reform): http://ec.europa.eu/information_society/policy/ecomm/doc/library/regframeforec_dec2009.pdf
- An overview of the main elements of the 2009 reform: http://ec.europa.eu/information_society/policy/ecomm/tomorrow/reform/index_en.htm
- In 2013 the European Commission issued a European Cyber Security Strategy and proposed a directive on Cyber Security. Article 14 of the proposed directive is similar to Article 13a, requiring operators to take appropriate security measures and to report significant incidents.

Annex A: Incident causes split out per service

This section shows the root cause categories and causs split out per service.

A.1 Root cause categories per service (percentage)

Figures 20, 21, 22 and 23 show the root cause categories of incidents split out per service. The diagrams show that for each service most incidents had a root cause in the category ‘system failures.

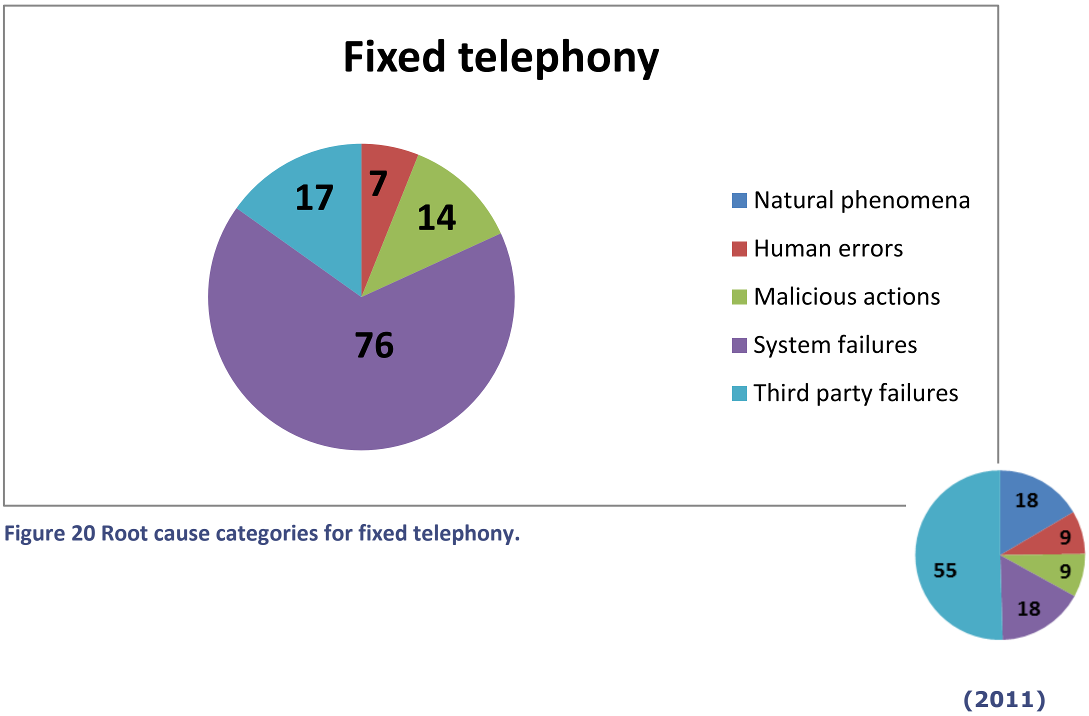


Figure 20 Root cause categories for fixed telephony.

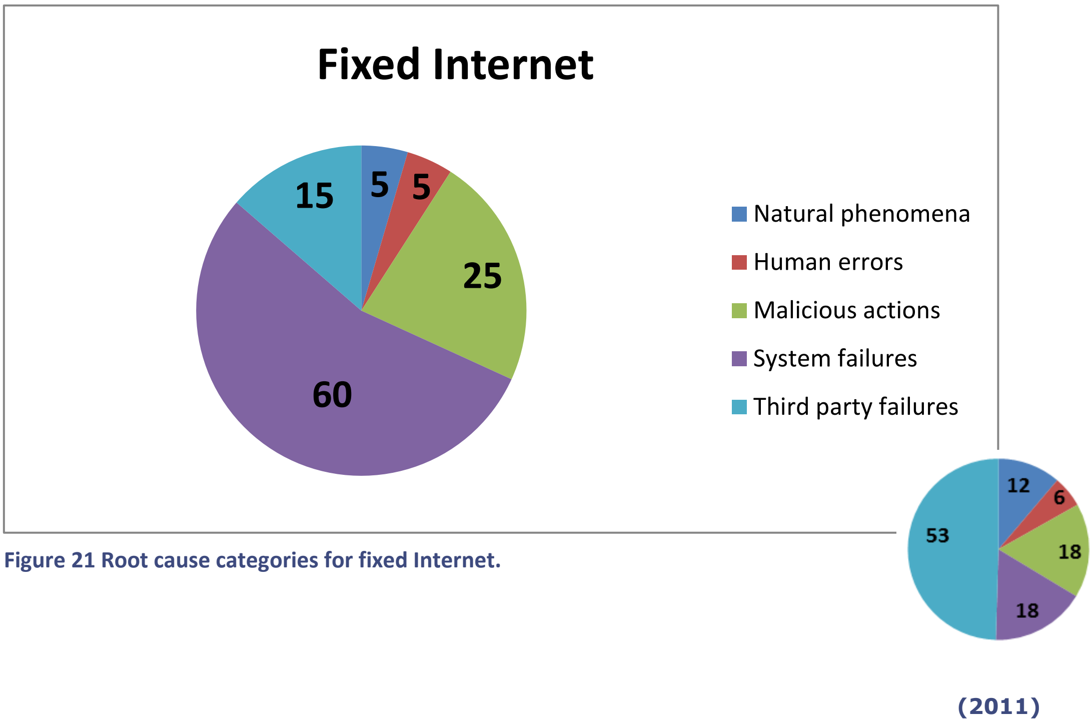


Figure 21 Root cause categories for fixed Internet.

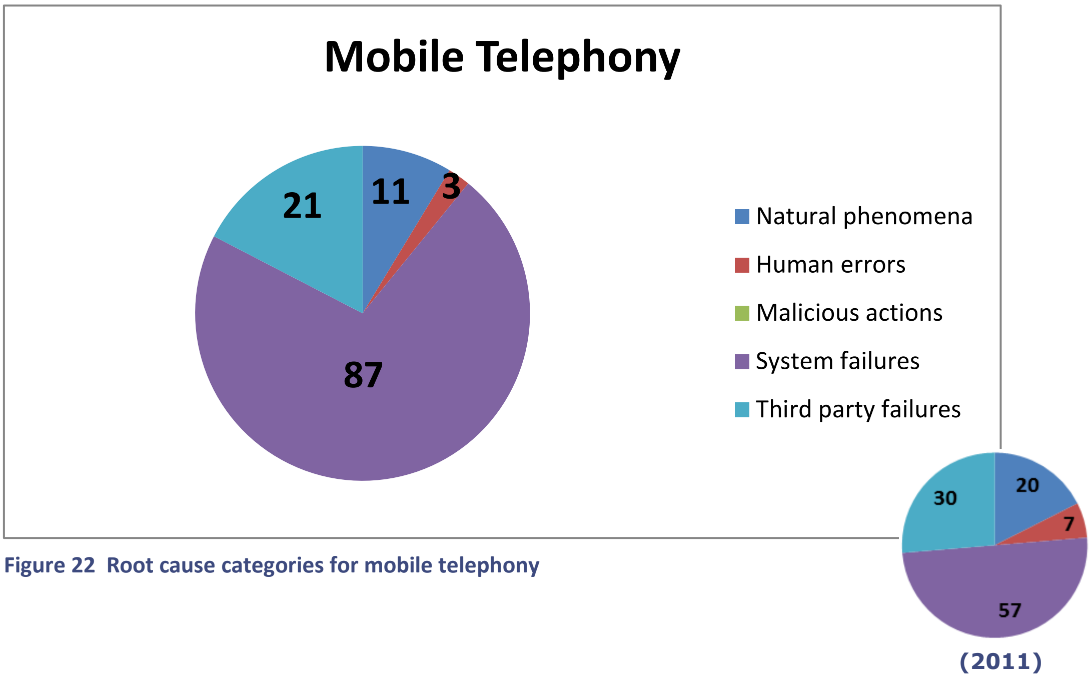


Figure 22 Root cause categories for mobile telephony

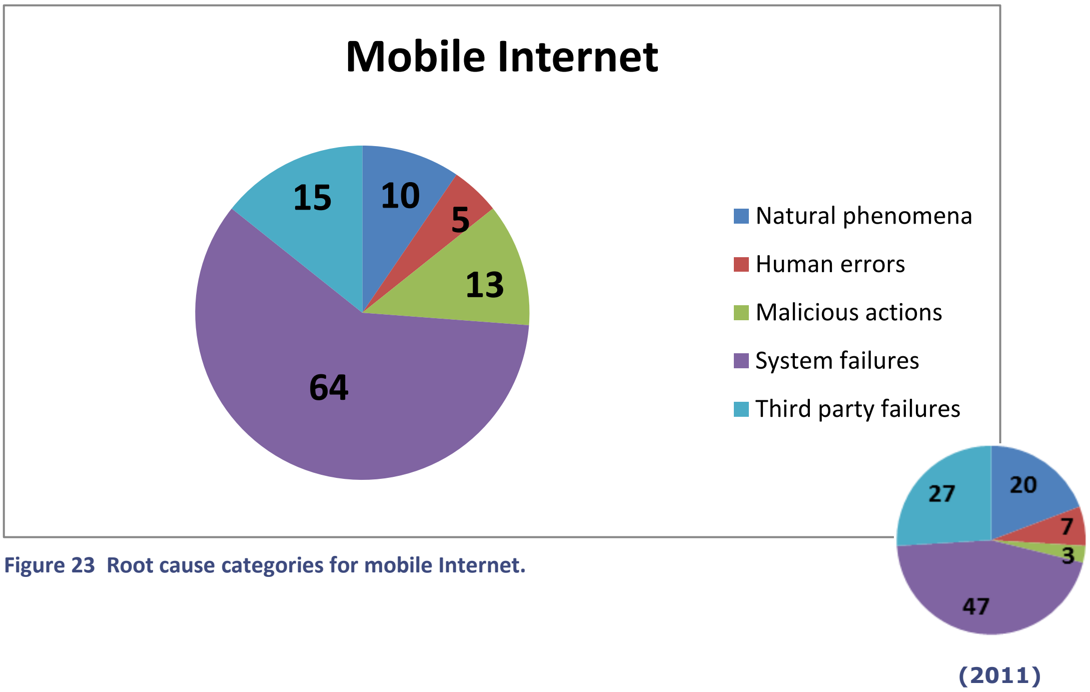


Figure 23 Root cause categories for mobile Internet.

A.2 Detailed causes per service

In Figure 24, 25, 26, 27 we show the detailed causes, split out per service.

The data shows that for all services, except fixed Internet, most incidents were caused by hardware failures followed by software bugs. For fixed Internet most incidents were caused by hardware failures followed by cyber attacks.

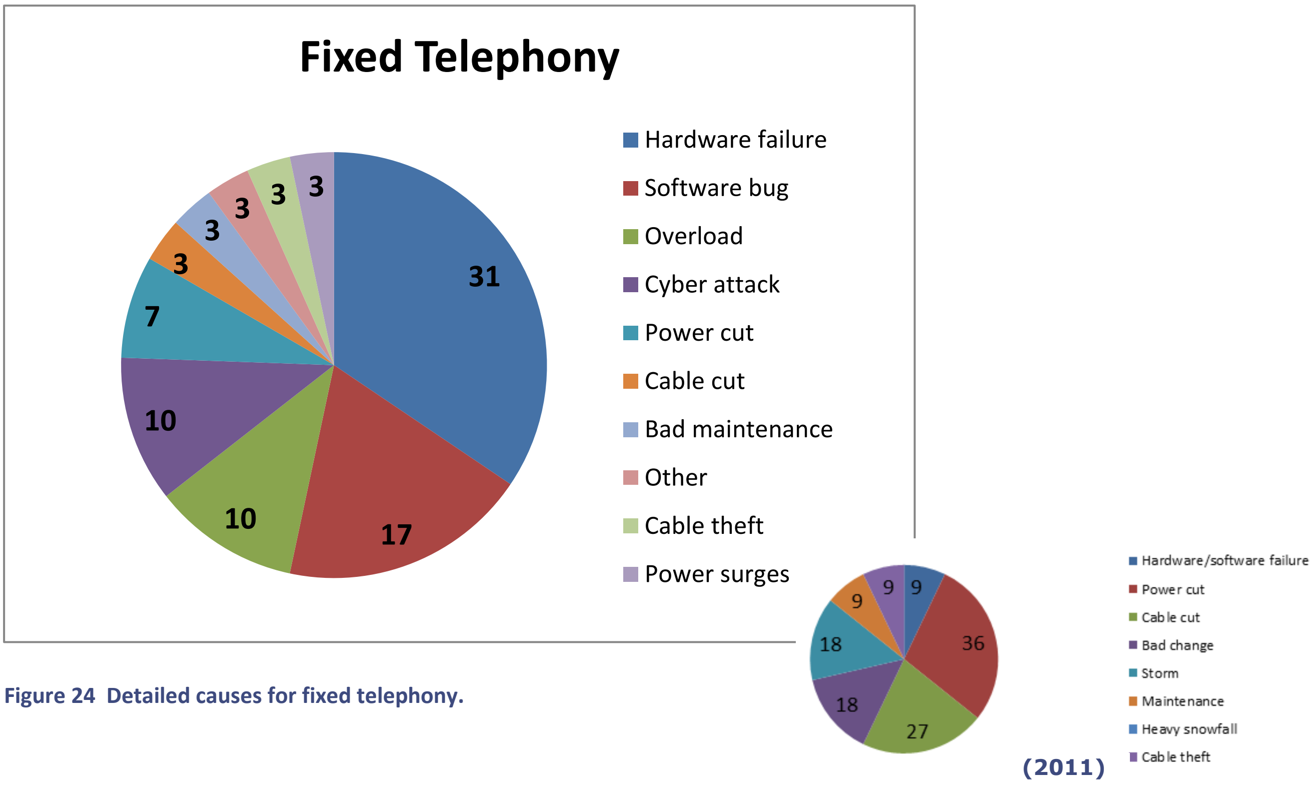


Figure 24 Detailed causes for fixed telephony.

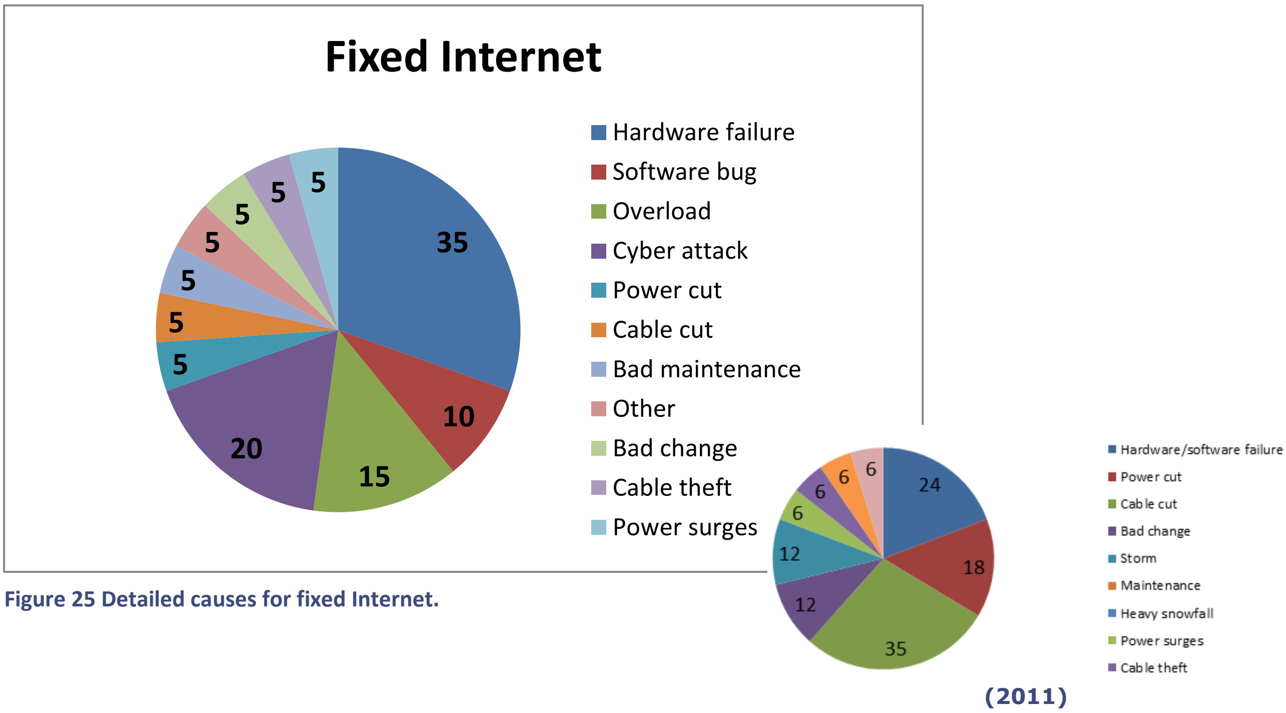
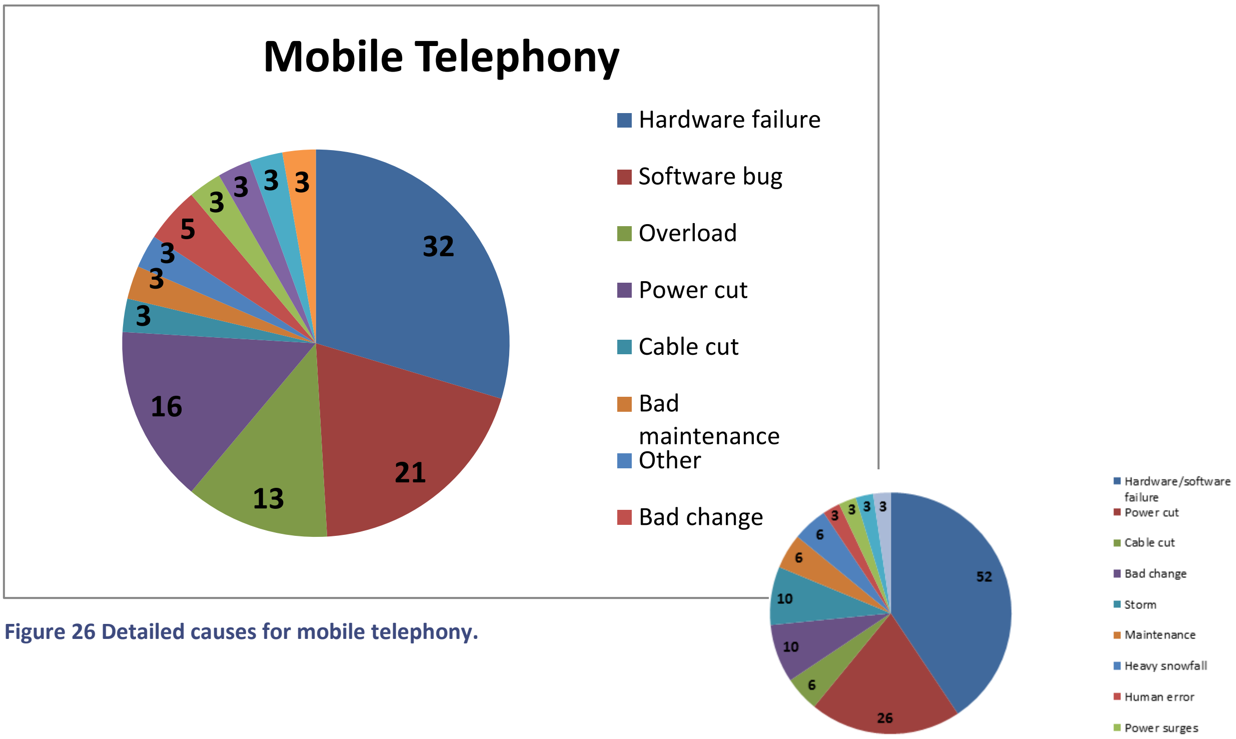


Figure 25 Detailed causes for fixed Internet.



(2011)

Figure 26 Detailed causes for mobile telephony.

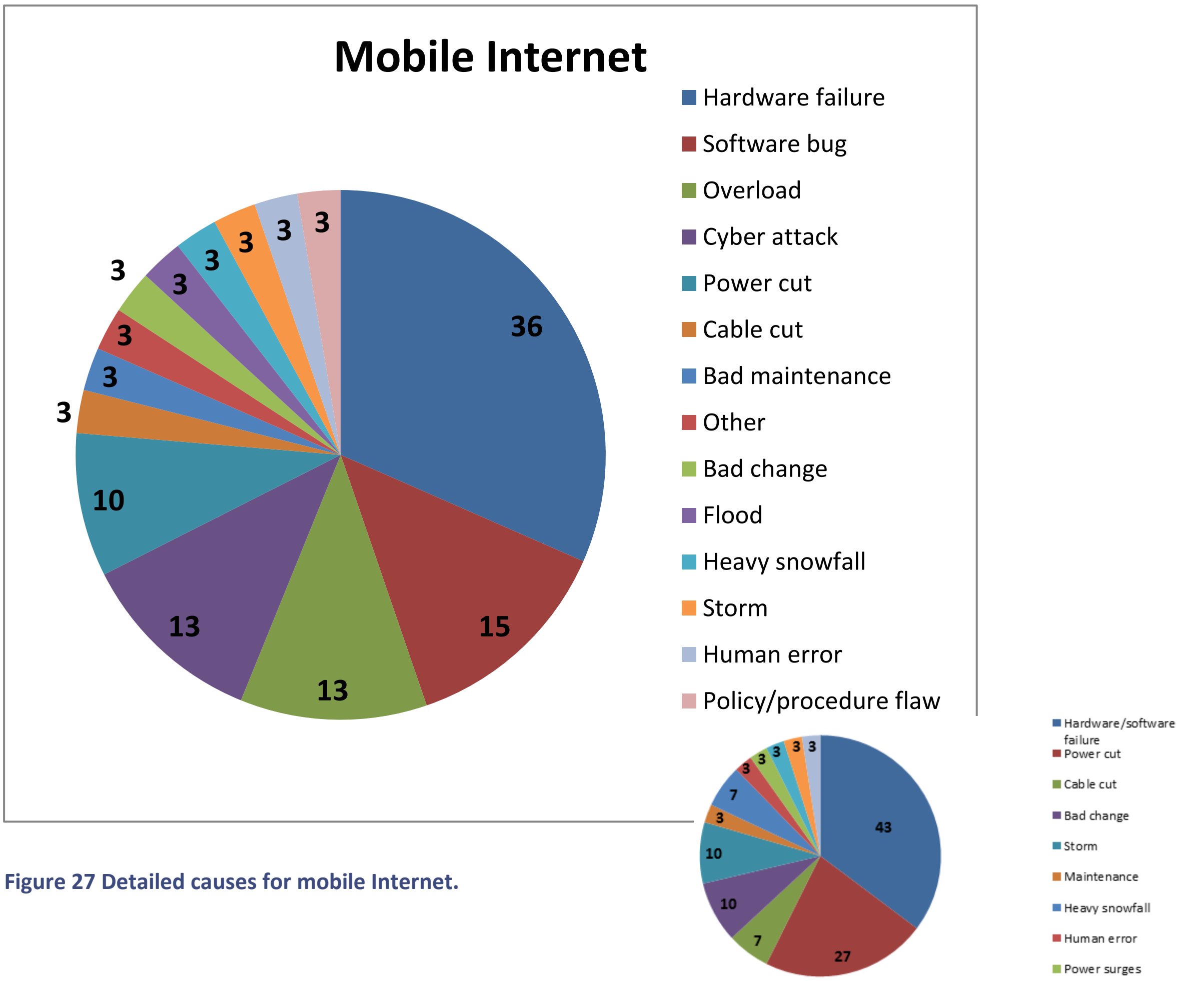


Figure 27 Detailed causes for mobile Internet.

(2011)

Annex B: VoIP versus PSTN

In this section fixed telephony is split in traditional circuit switched fixed telephony (PSTN) and fixed IP based telephony (VoIP).

Figure 28 shows the detailed causes, for PSTN and VoIP services.

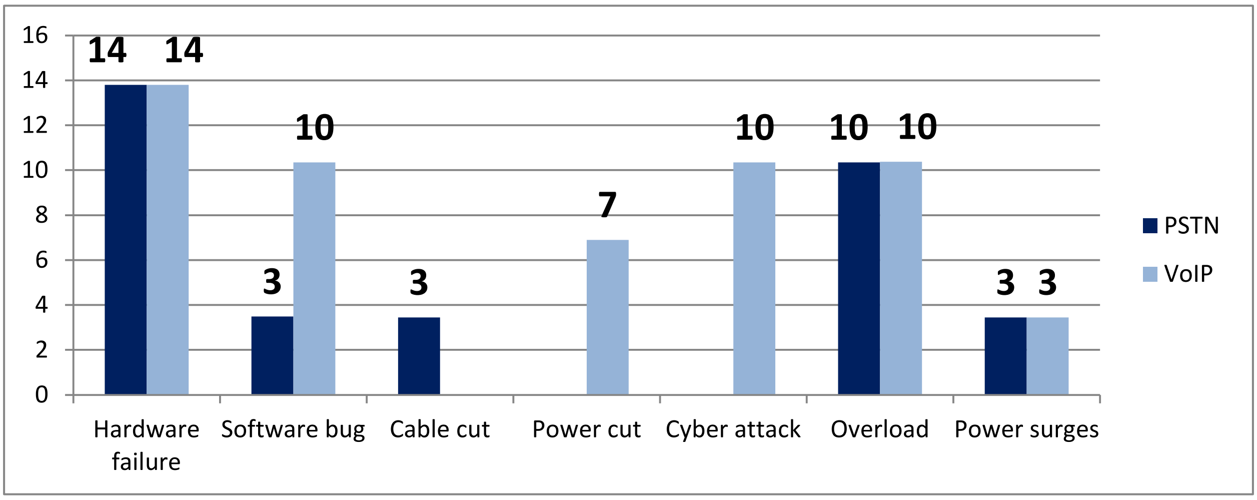


Figure 28 Detailed causes for incidents affecting PSTN and VoIP (percentage).

Both PSTN and VoIP were mostly affected by hardware failures. VoIP was more affected by software bugs, power cuts and cyber attacks, wereas PSTN was more affected by cable cuts.

Figure 29 shows the impact per detailed cause in user hours, for PSTN an VoIP services.

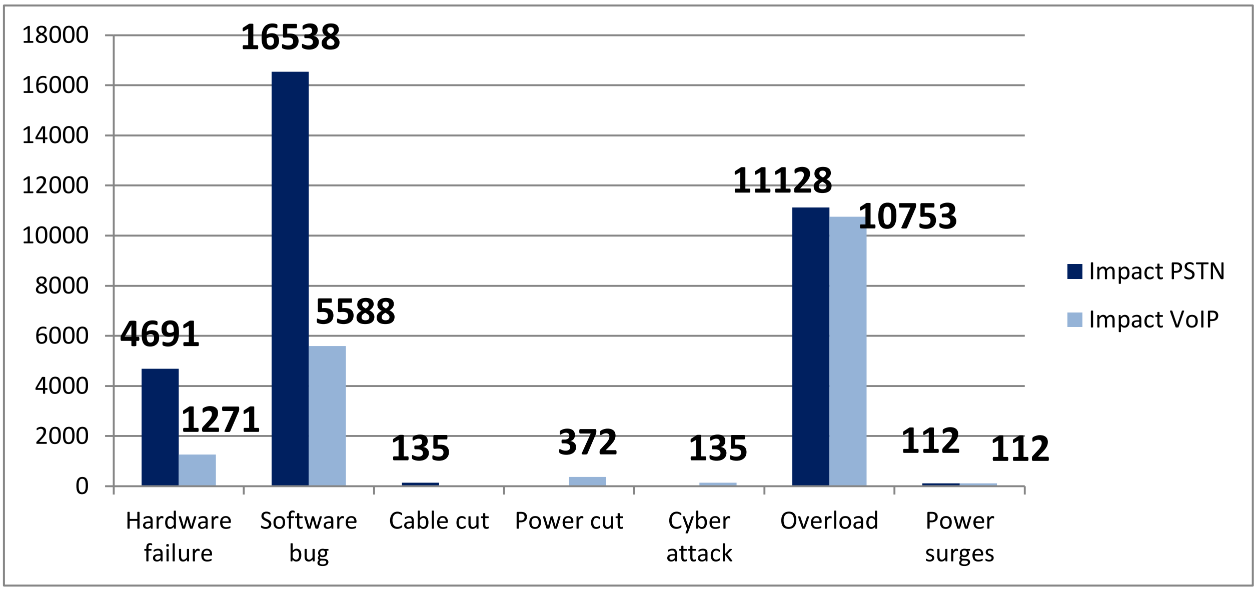


Figure 29 Impact in users hours of incidents per detailed cause, for PSTN and VoIP.

For PSTN, the detailed cause with most impact, in terms of user hours, was software bugs, followed by overload. For VoIP the impact of overload was highest, followed by software bugs.

European Union Agency for Network and Information Security (ENISA)
Annual Incident Reports 2012,
Analysis of Article 13a incident reports

ISBN 978-92-9204-066-6
doi: 10.2824/15669
Catalogue Number: TP-03-13-439-EN-N

ISBN Number
978-92-9204-066-6
Catalogue number
TP-03-13-439-EN-N

ENISA
European Union Agency for Network and Information Security
Science and Technology Park of Crete (ITE)
Vassilika Vouton, 700 13, Heraklion, Greece

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

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