Annual Incident Reports 2013

Analysis of Article 13a annual incident reports

September 2014

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

Christoffer Karsberg, Christina Skouloudi, Dr Marnix Dekker

Contact

To contact 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 no 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), NMHH (HU), ITSIRI (LV), OEC (PL), AKOS (SI), Teleoff (SK), OFCOM (CH), and HAKOM (HR).

Executive summary

Every year, 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), by the National Regulatory Authorities (NRAs) of the different EU Member States.

This report covers the incidents that occurred in 2013 and it gives an aggregated analysis of the incident reports about severe outages across the EU. This report does not include details about individual countries or providers. The main statistical data is as follows:

- **90 major incidents reported:** This year, in total 19 countries reported 90 significant incidents and 9 countries reported no significant incidents.
- **Mobile networks most affected:** Approximately half of the major incidents had an impact on mobile Internet and mobile telephony.
- **Mobile network outages affect many users:** Incidents affecting mobile Internet or mobile telephony affected most users (around 1.4 million users and 700 000 users respectively per incident). This is consistent with the high penetration rates of mobile telephony and Internet.
- **Impact on emergency calls**: A fifth of the major incidents had an impact on the emergency calls (aka 112 access).
- **System failures are the most common root cause:** Most major incidents were caused by "System failures" (61 % of the incidents).
    - Looking more in detail at this root cause category, the most common detailed causes were "software bugs", "hardware failures" and "software misconfigurations".
    - The assets most often affected were switches (e.g. mobile switching and routers) and base stations and controllers.
- **System failures affect the most user connections:** Incidents categorized with the root cause system failure, affected around 1.5 million user connections on average per incident.
    - Looking more in detail, the detailed causes affecting most user connections were "software misconfiguration", "software bugs", and "power surges".
- **Natural phenomena and malicious actions cause long lasting incidents:** Incidents caused by natural phenomena (heavy snowfall, storms, etc.) and malicious actions (arson, cable theft, etc.) lasted on average more than 50 hours.
- **Natural phenomena and system failures have most impact:** Multiplying number of user connection and duration, one obtains a measure for total impact, or 'total user hours lost'. Natural phenomena had on average most impact, followed by system failures.
    - Looking more in detail, Power cuts, heavy snowfall, cable cuts and storms, respectively, impacted most user hours.
- **Base stations and switches were most affected:** Overall, base stations, switches and mobile switching were the assets most affected by incidents.

ENISA, together with the EC and NRAs in the EU Member States, will discuss specific incidents in more detail within the Article 13a Expert Group. Where needed, ENISA may publish technical guidance about mitigating specific types of incidents. This year, for example, following the 2012 incidents, ENISA has been working on recommendations for providers about how to manage security requirements for vendors and outsourcing partners they use for their core operations.

The next annual report will be published in summer 2015, for the 2014 incidents.

Table of Contents

1 Introduction

This is the third iteration of this report, which summarises significant security incidents reported to ENISA and the European Commission (EC), 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. This year ENISA and the EC received 90 incident reports from NRAs, about severe outages in the EU's electronic communication networks or services which occurred in 2013. This report provides an aggregate analysis of these 90 incidents.

Please note that in this document we do *not* provide details from the individual incident reports. The analysis is only an aggregation in terms of averages and percentages across the EU, and it does not contain references to specific countries or specific providers. Individual incidents are discussed in more detail with the NRAs 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 from 2013 which were reported to ENISA and the EC and provides examples of incidents. The Executive Summary (at the start of this document) provides a snapshot of this analysis and the conclusions.

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 *notify* competent national authorities about breaches of security or loss of integrity that have had significant impact on the operation of networks or services.
- 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 about the incidents.

These incident reporting flows (incident notification and annual reporting) are shown in the diagram below. This document analyses the incidents from 2013 that have been reported to ENISA and the EC (the black dashed arrow).

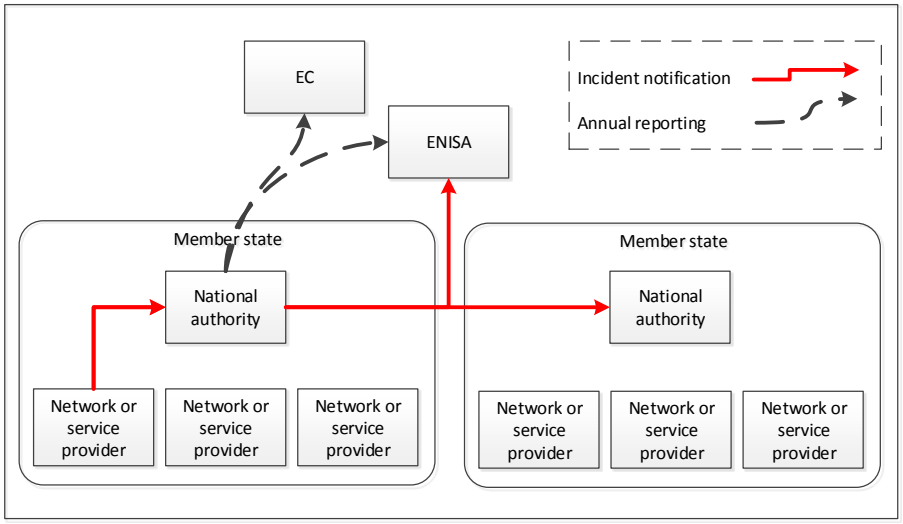

Figure 1: Incident reporting in Article 13a.

[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 develop the technical guidelines and 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 Incident reporting procedure

In spring 2012, the 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 coming years, annual reporting would be carried out by the end of February each year.

In autumn 2012, ENISA developed an online incident reporting tool (called CIRAS), which replaces the electronic forms exchanged by email. CIRAS allows NRAs to exert greater control over the data reported and provides the NRAs with better access to data about incidents reported across the EU.

We briefly explain the main features of the incident reporting procedure, as described in the technical guideline which was developed in collaboration with the NRAs.

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, Fibre, etc.),
- Mobile telephony (e.g. GSM, UMTS, LTE, etc.),
- Fixed Internet access (e.g. DSL, Fibre, Cable, etc.),
- Mobile Internet access (e.g. GPRS/EDGE, UMTS, LTE, etc.)

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.

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

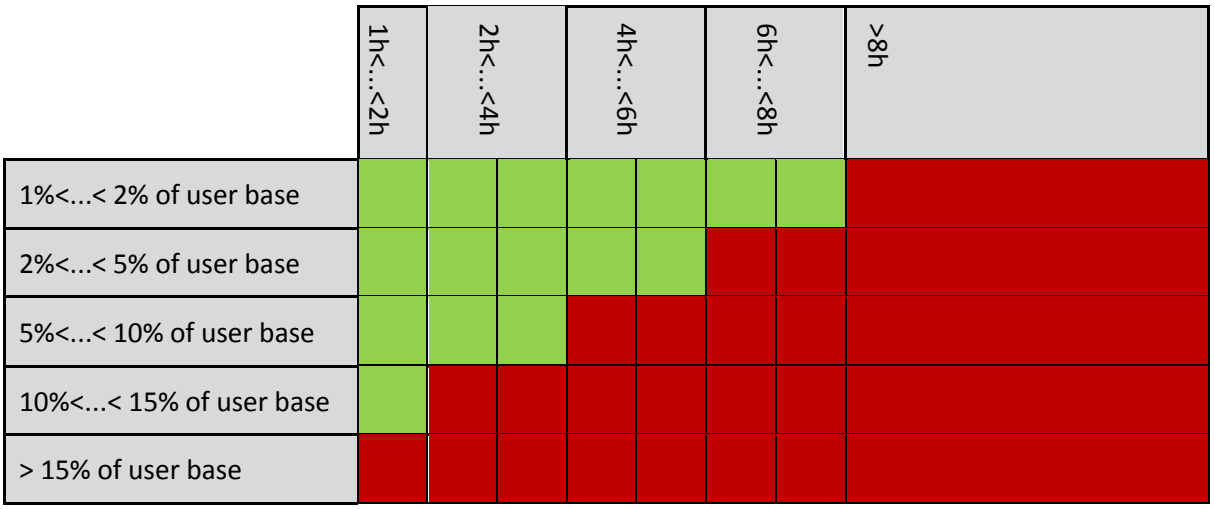

Figure 2 ***Threshold for annual summary reporting based on a combination of duration and the percentage of the national user base.***

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 in order to trigger the reporting mechanism. NRAs may also report incidents with impact graded below the threshold.

For 2013, we introduced a new optional threshold for annual summary reporting, based on absolute impact, in order to allow NRAs in large Member States to include larger incidents but that would not exceed the relative thresholds. NRAs may optionally include incidents when the product of duration and number of user connections affected exceeds 180 million user minutes, or 3 million user hours. For next year's reporting, about the 2014 incidents, this absolute threshold has been lowered and becomes mandatory.

[2] Reference is made to the definition agreed in the COCOM meetings.

3.1.5 Root cause categories

In the incident reports four categories of root causes have been distinguished plus one category that is used in conjunction with one of the other four categories.

- **Natural phenomena** – This category includes incidents caused by severe weather, earthquakes, floods, pandemic diseases, wildfires, wildlife, and so on.
- **Human errors** - This category includes incidents caused by errors committed by employees of the provider or outside the provider, during the operation of equipment or facilities, the use of tools, the execution of procedures, etc. E.g. an excavator cutting off a cable.
- **Malicious attacks** - This category includes incidents caused by a deliberate act by someone or some organisation, e.g. a cyber-attack or a cable theft.
- **System failures** – This category includes incidents caused by failures of a system, for example hardware failures, software failures or flaws in manuals, procedures or policies.
- **Third party failures** – This category includes incidents caused by a failure or incident at a third party. This category is used in conjunctions with one of the other root cause categories.

4 Analysis of the incidents

In total, all 28 EU Member States participated in this process. Of these, 18 countries and one EFTA Member State reported in total 90 significant incidents, 9 countries reported there were no significant incidents and one country had not implemented incident reporting yet.

The two pie charts to the right show the situation the previous two years. In the rest of this report we show, besides the data about the 2013 incidents, figures and diagrams from the previous two years, to allow the reader to make a comparison.

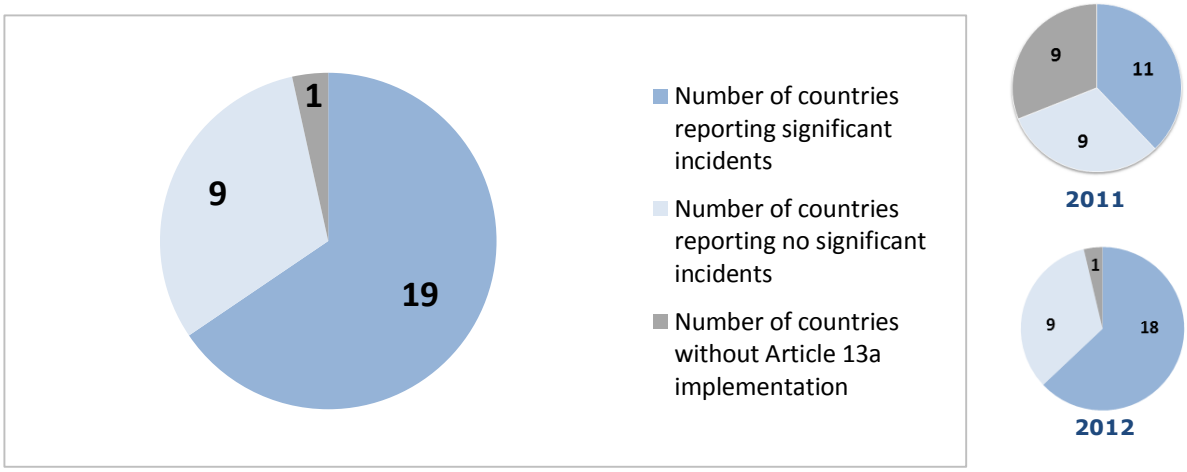

Figure 3: Countries involved in the annual summary reporting over 2013.

In this section the

In this section, the 90 reported incidents are aggregated and analysed. First, the impact per service is analysed (in Section 4.1), then the impact per root cause category is analysed (Section 4.2), and in Section 4.3 detailed causes are examined. In Section 4.3 impact as a product of user connections affected and duration of the incidents is analysed and in Section 4.5 the components or assets affected by the incidents are considered. Throughout the text we provide anonymized descriptions (in blue italic) of actual large-scale incidents which occurred in 2013.

Note about statistical conclusions: Readers should be cautious when drawing conclusions from the statistics in this report. In particular, they should take into account that:

1. The scope of reporting major security incidents is restricted to incidents with an impact on the *continuity* of public electronic communication services and networks. There are many other types of incidents with an impact on security of services and networks which are not in scope of annual reporting. For example, if attackers would wiretap undersea cables without causing any outages, then such a security incident would not be included in the annual reporting.
2. We are still in the early phases of implementation of Article 13a. There are still changes and improvements in the way national and EU reporting is being implemented. Statistical conclusions about multi-annual trends should therefore *be drawn with care*.
3. The scope of reporting includes only major, or *significant,* incidents scoring above the agreed thresholds. Smaller incidents are not reported at an EU level and this means that the view is skewed towards the larger incidents.

4.1 Impact of incidents

We focus first on the impact of incidents on the electronic communications networks and services.

4.1.1 Impact per service

Approximately half of the reported incidents affected mobile internet or mobile telephony, as was the case in 2012 and in 2013.

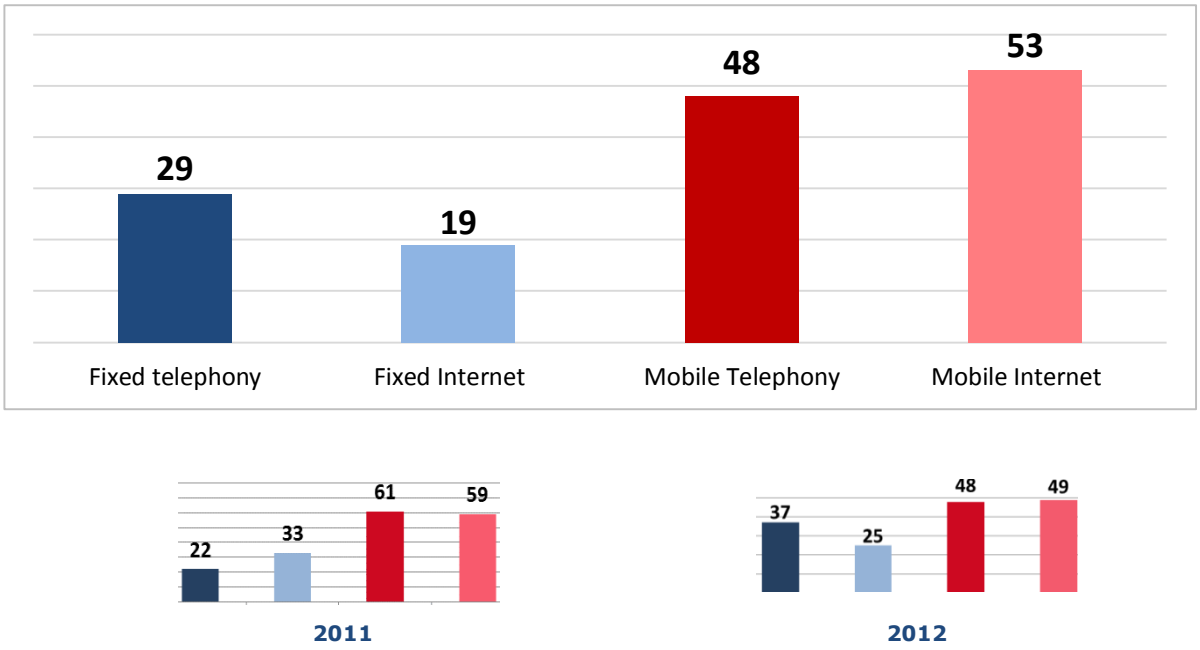

Figure 4: Incidents per service (percentage)

Most incidents have an impact on two or more services (which is why the percentages in the chart add up to 149 %). National thresholds for reporting are per service and a percentage of the total national user base for that service. So this would suggest that mobile services are more at risk of large outages than fixed services.

Faulty network update caused mobile telephony and mobile Internet to fail (duration: hours, connections: millions, cause: system failure): *A planned network upgrade was done at night for mobile phone call services. After the upgrade, customers' call and data services failed. Because the change was made to call and not data services, the cause of the failure was difficult to locate. The problem occurred to users under one Radio Network Controller (RNC), but not all of them, which rendered locating the cause even harder.*

4.1.2 Number of user connections affected

Mobile Internet outages affected on average 1.4 million user connections per incident. Incidents with an impact on mobile telephony affected on average 700 000 user connections.

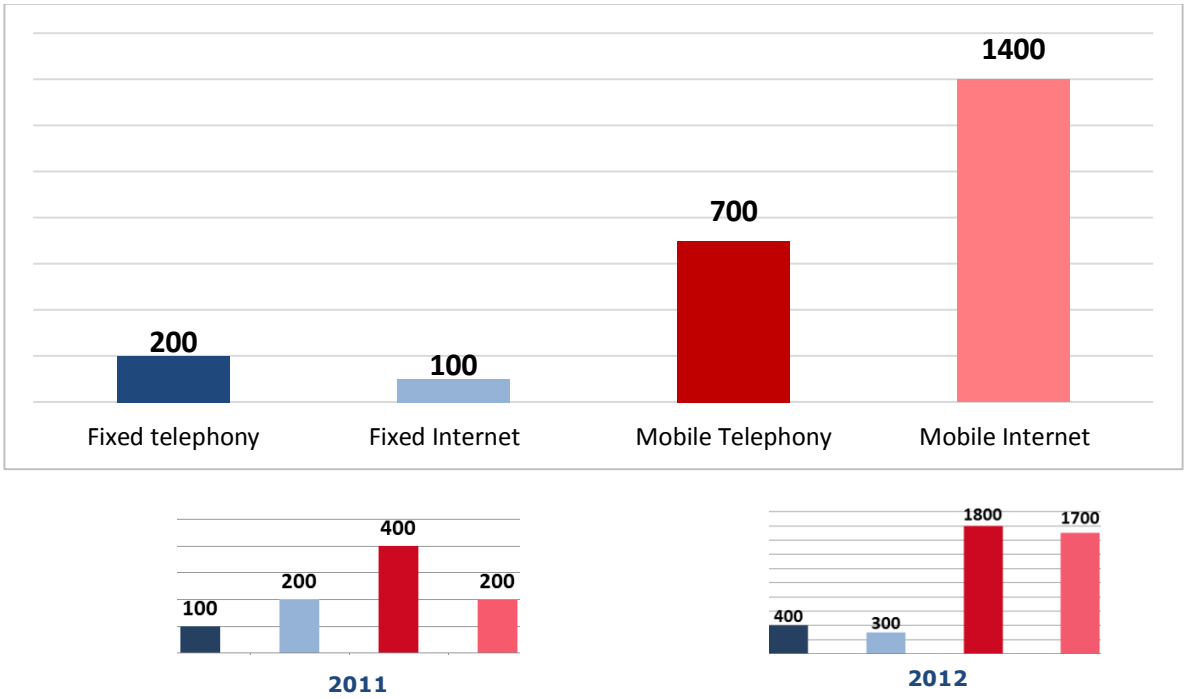

Figure 5: Average number of user connections affected per incident per service (1000s).

The difference between fixed and mobile may partly be due to the fact that some of the impacted components, we call them assets, in the mobile networks, were more centrally located parts of the networks as compared to the failed assets for fixed services, thus affecting more user connections per incident.

EU averages shown here are not representative of the size of incidents nationally. The averages in these diagrams include both small and large countries. Nationally, the average size of incidents can be very different, depending on the size of the population and/or the national network topology.

4.1.3 Percentage of the national user base affected

Mobile Internet outages impacted about 9 % of the national user base for mobile Internet user connections on average, a significant portion of the national user base. Each year there has been a drop in failed user connections for all services, but it should be noted that a larger share of smaller incidents have been reported year by year. All three years, mobile Internet has been reported to suffer the most impact in terms of affected user connections compared to the other services.

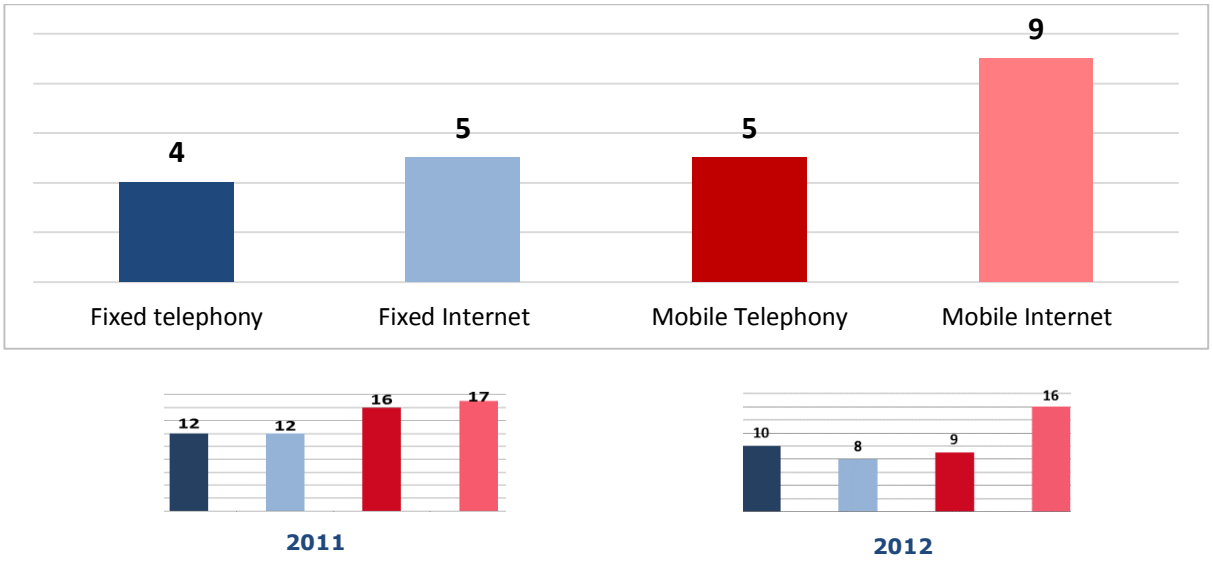

Figure 6: Percentage of national user base affected on average per incident per service.

Faulty upgrade in router caused mobile Internet to fail (duration: hours, connections: thousands, cause: system failure): *Disruption of connection of mobile data sessions was caused by a failed upgrade of hardware and software in a router.*

4.1.4 Impact on emergency services

One fifth of the incidents involved an impact on emergency calls - i.e. the possibility for users to contact emergency call-centres using the emergency number 112. Compared to previous years this figure is at its lowest.

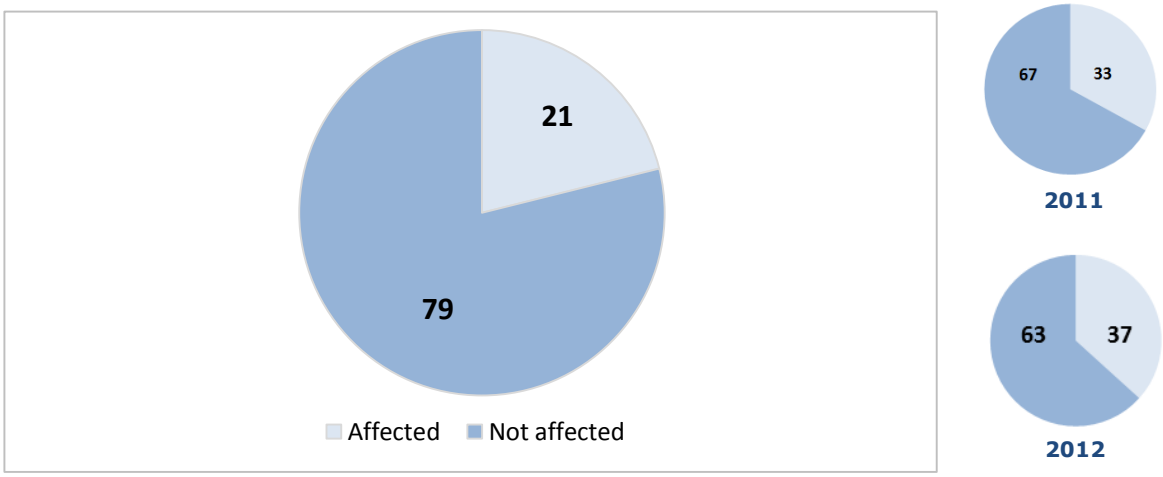

Figure 7: Impact on emergency calls.

4.1.5 Impact on interconnections

In 4 % of the incidents there was an impact on interconnections between other providers. This is the lowest figure since annual summary reporting started.

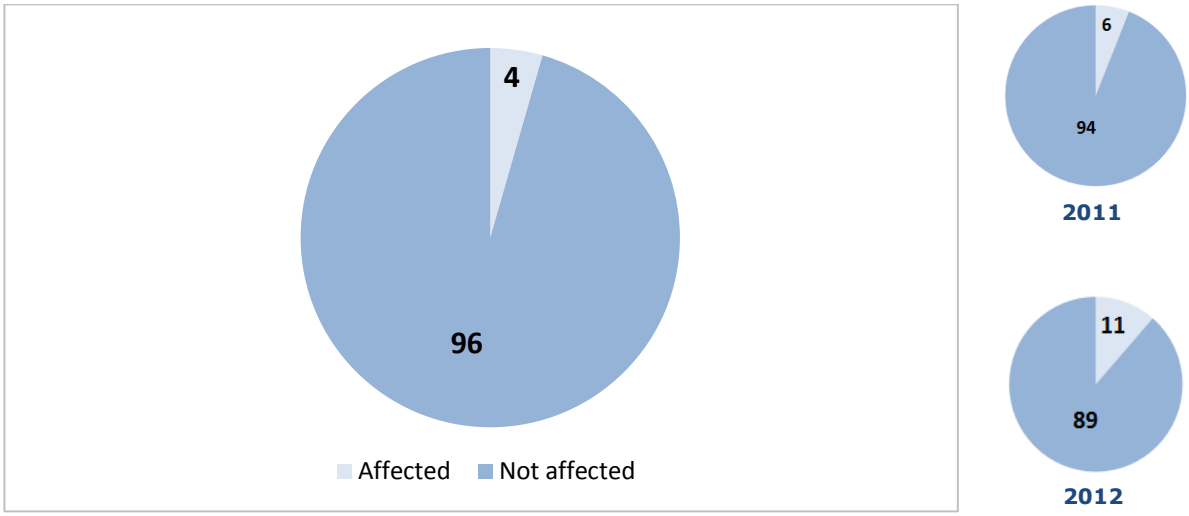

Figure 8: Impact on interconnections

4.2 Root cause categories

Now we look at the main root cause categories of reported incidents. Root cause categories are very broad categories for incidents.

4.2.1 Incidents per root cause category

In 2013 about 61 % of the incidents were 'System failures', 19 % caused by 'human errors'. Only 6 % was categorized as 'malicious actions'.

Over the last 3 years the root cause category 'System failures' has been the most common root cause category.

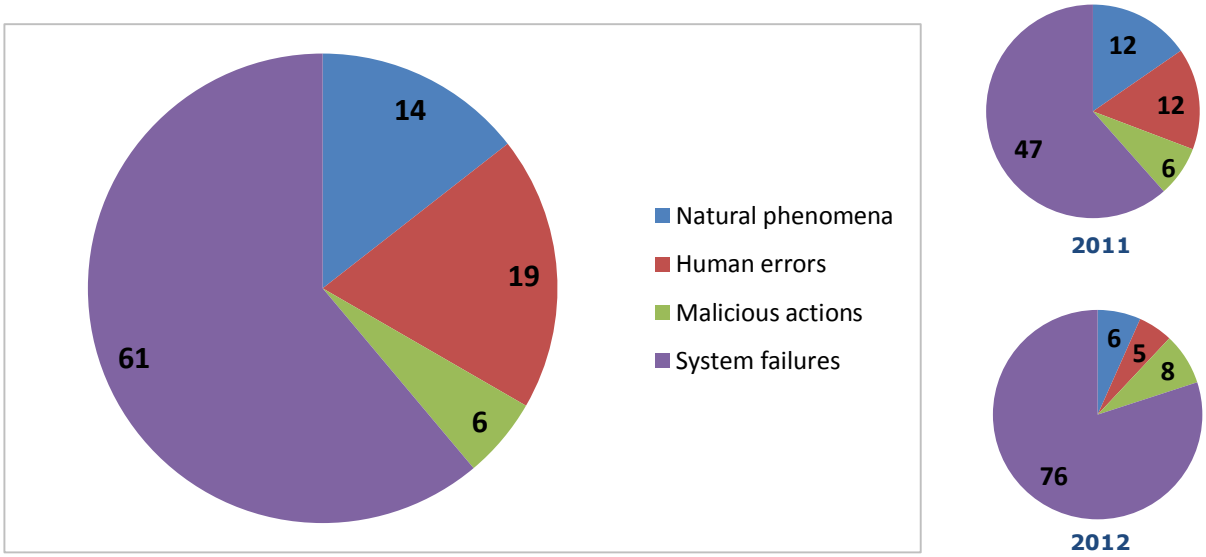

Figure 9: Incidents per root cause category (percentage).

Hardware failure caused interruptions to mobile Internet services (duration: hours, connections: thousands, cause: system failure): *A hardware failure on the transmission node (router) caused the interruption of all data traffic between the Gateway GPRS Support Node (GGSN) and gateway router. All mobile users who during the time of failure tried to access the Internet were affected.*

4.2.2 Third party failures

About 11 % of the incidents reported were categorized as 'third party failures' (see Figure 10).

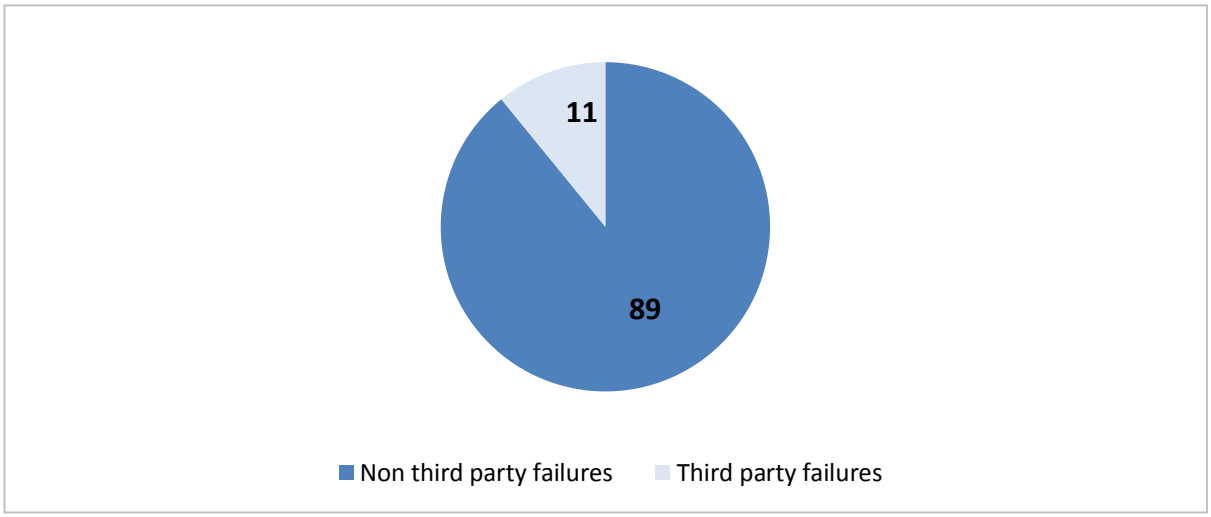

Figure 10: Third party failures and non-third party failures of all incidents (percentages).

We analyse these third party failures in more detail and show the corresponding root cause category in these cases (see Figure 11). Third party failures have similar root causes as incidents which are not categorized as third party failures.

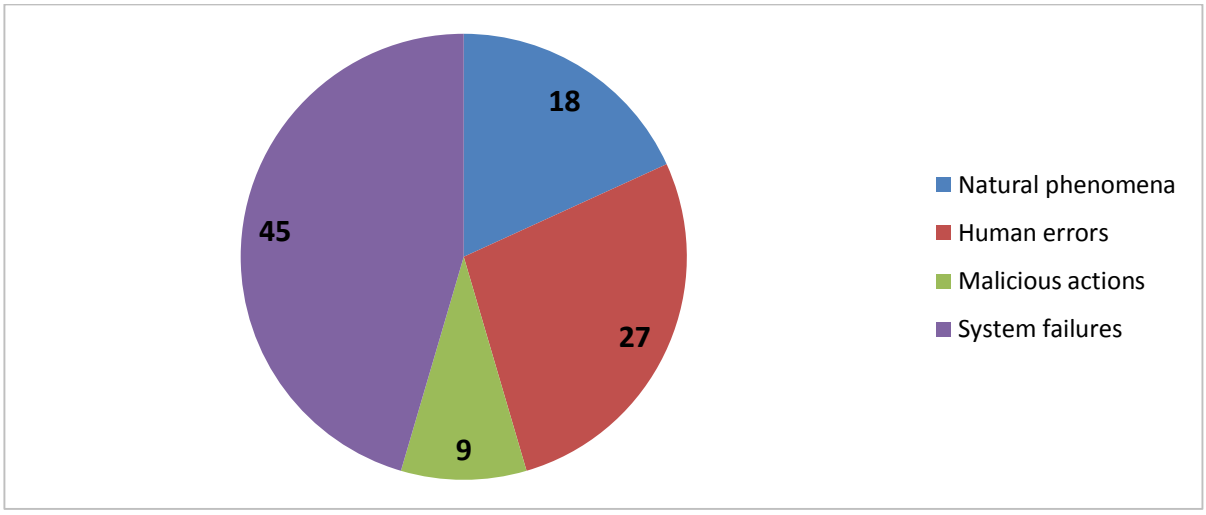

Figure 11: Third party root causes (percentage).

Cable cut caused mobile outage (duration: hours, connections: thousands, cause: third party and human error): *Mobile telephony and mobile Internet services were disrupted for thousands of users for several hours when another operator was installing a cable and cut a cable of the former operator. At the same time as the fault was located, the redundant connection also failed. The interface unit of the redundant connection was reset, which returned the services for customers. The cable cut was fixed and the traffic was rerouted back to the original route.*

4.2.3 Root cause categories per service

Here we look at the root causes for each of the four services separately: fixed telephony, fixed Internet access, mobile telephony and mobile Internet access.

In 2013, 38 % of the incidents with an impact on fixed telephony were caused by natural phenomena. About 58 % of the incidents with an impact on mobile telephony were categorized as 'System failures'. Only 12 % of the mobile outages were caused by human error.

In the four diagrams below we also compare with previous years. Bear in mind that this year we show the fifth category, third party failure, separately (section 4.2.2).

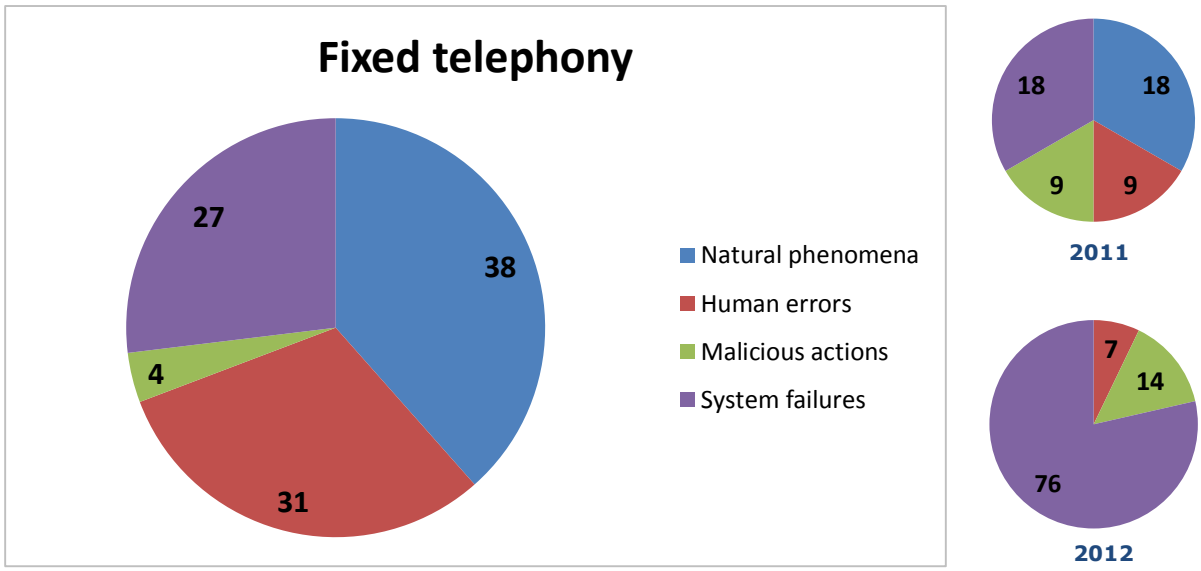

Figure 12: Root cause categories for fixed telephony (percentage).

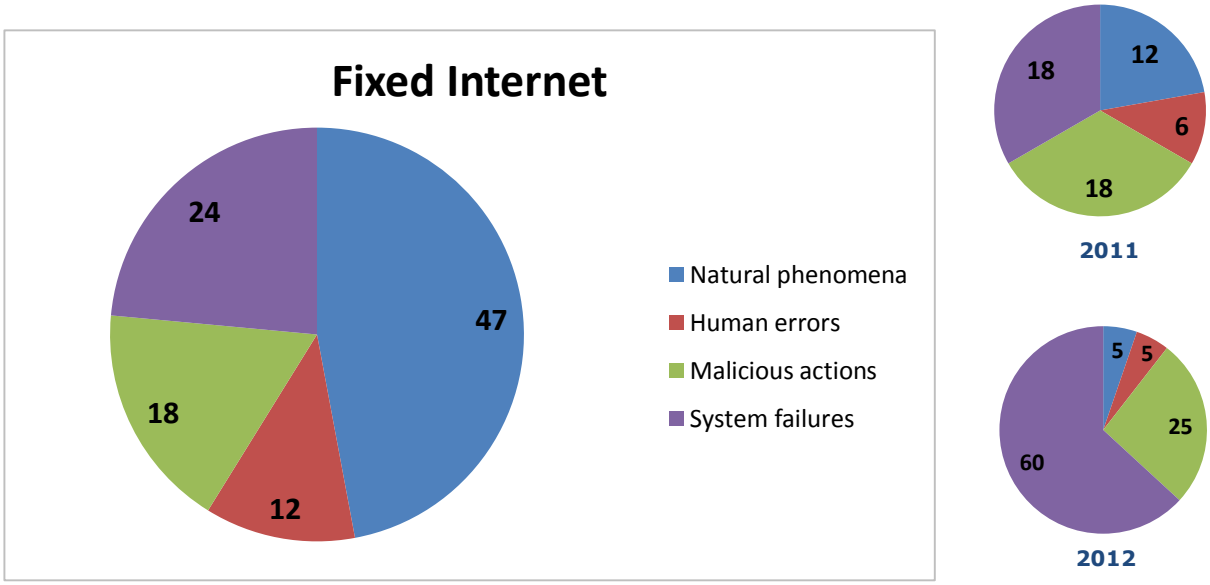

Figure 13: Root cause categories for fixed Internet (percentage).

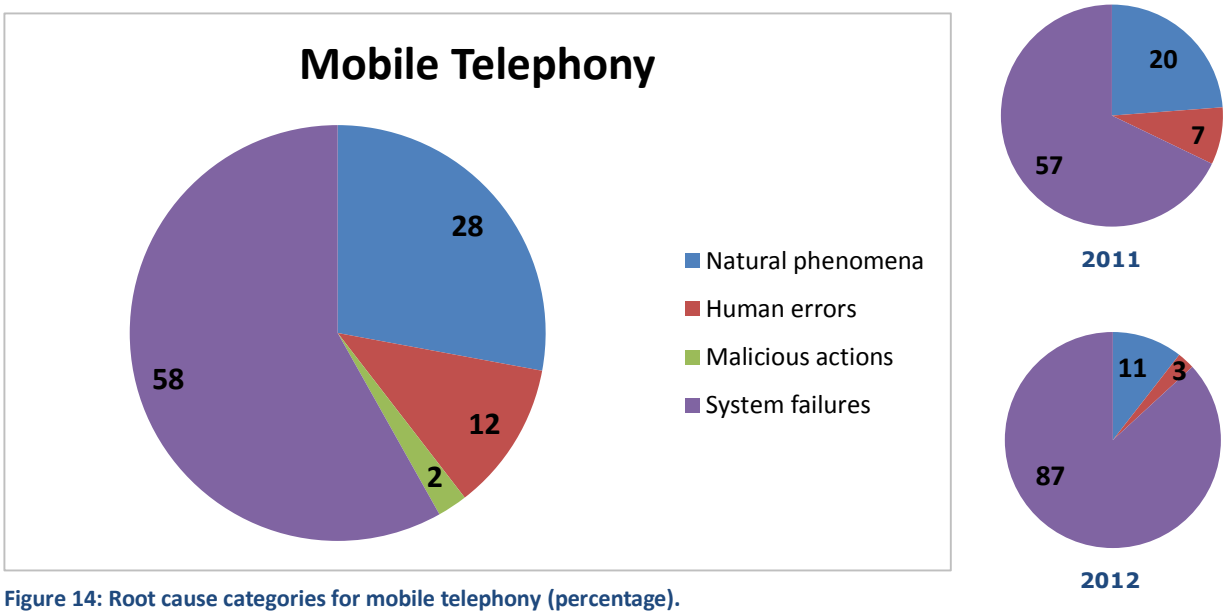

Figure 14: Root cause categories for mobile telephony (percentage).

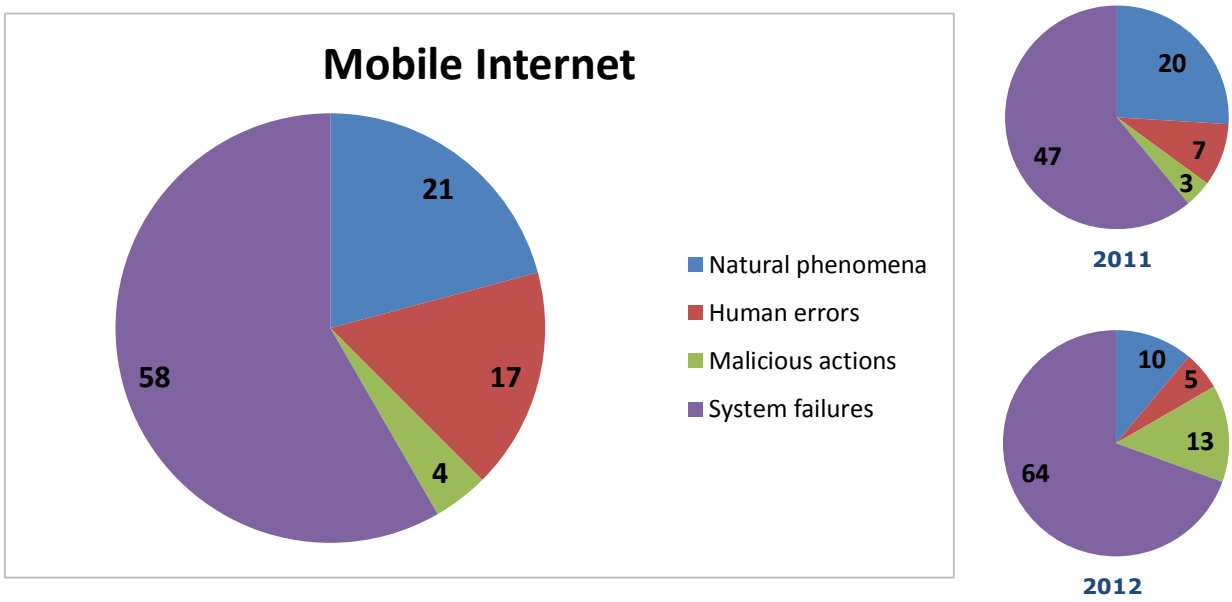

Figure 15: Root cause categories for mobile Internet (percentage).

4.2.4 Average duration of incidents per root cause category

Incidents caused by natural phenomena had a long recovery time on average per incident (54 hours). This year the average incident duration for malicious actions was also high (53 hours). It should be mentioned, however, that the figure was skewed by one particular incident which took very long to resolve (164 hours). Overall natural phenomena caused the longest outages for all three years.

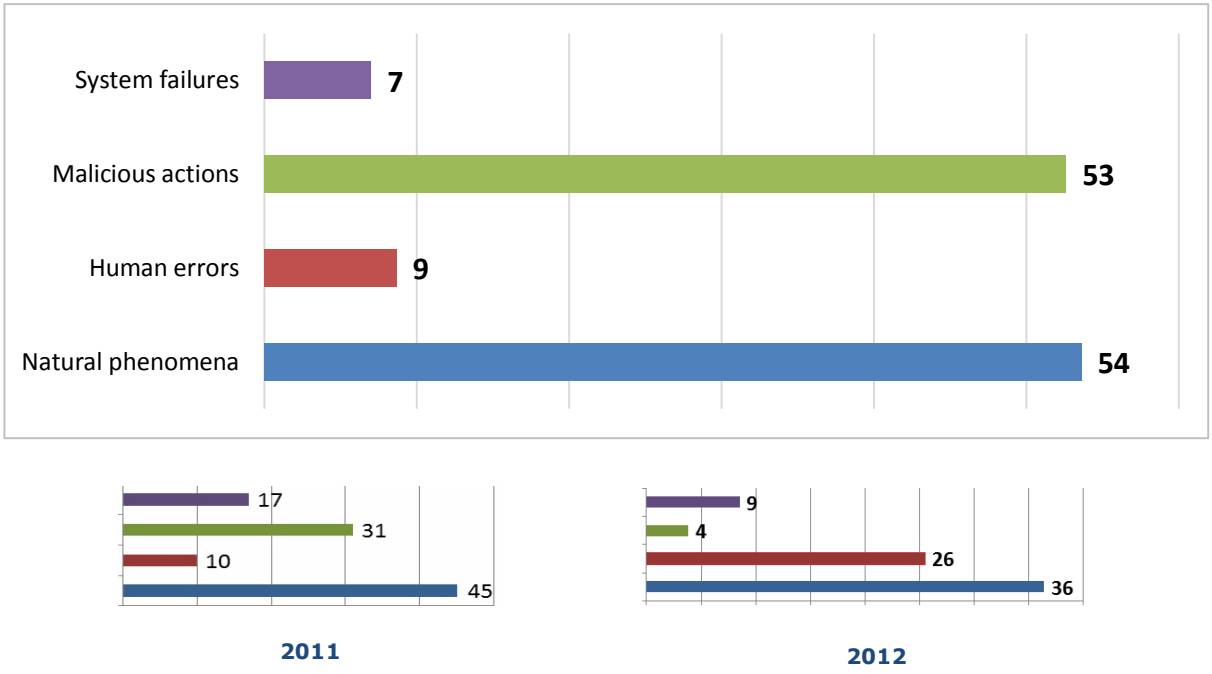

Figure 16: Average duration of incidents per root cause category (hours).

DDoS attack on DNS servers causing Internet unavailability (duration: days, connections: thousands, cause: malicious action): *The DNS of some Internet service providers were DDoS attacked causing Internet access to be practically unavailable for 150 000 users for 2 hours.*

Theft attempt caused cable cut to carrier network (duration: days, connections: thousands, cause: malicious action): *An attempted theft of copper resulted in the cutting of 12 cables, each containing over 100 fibres. The incident occurred on the same street as the Point of Presence (PoP) site for the national carrier network resulting in a failure of all resilient service options.*

Storm shut down Power supply causing mobile networks to fail (duration: days, connection: thousands, cause: natural phenomena and third party failure): *A storm hit the country damaging trees, affecting the power grid and all mobile networks within the storm area. The impact was limited to urban areas but its effect was more long lasting in rural areas. The base stations ran out of battery and were left without power. Also some fixed lines were affected.*

4.2.5 Average number of user connections affected per root cause category

We now show the number of user connections affected per incident for each of the different root cause categories. We are showing *user connections* affected and not *users affected*, because a single consumer often has access to multiple services, for example fixed telephony and mobile telephony,

which may all fail in the same incident. So the number of user connections impacted is often a multiple of the number of users impacted.

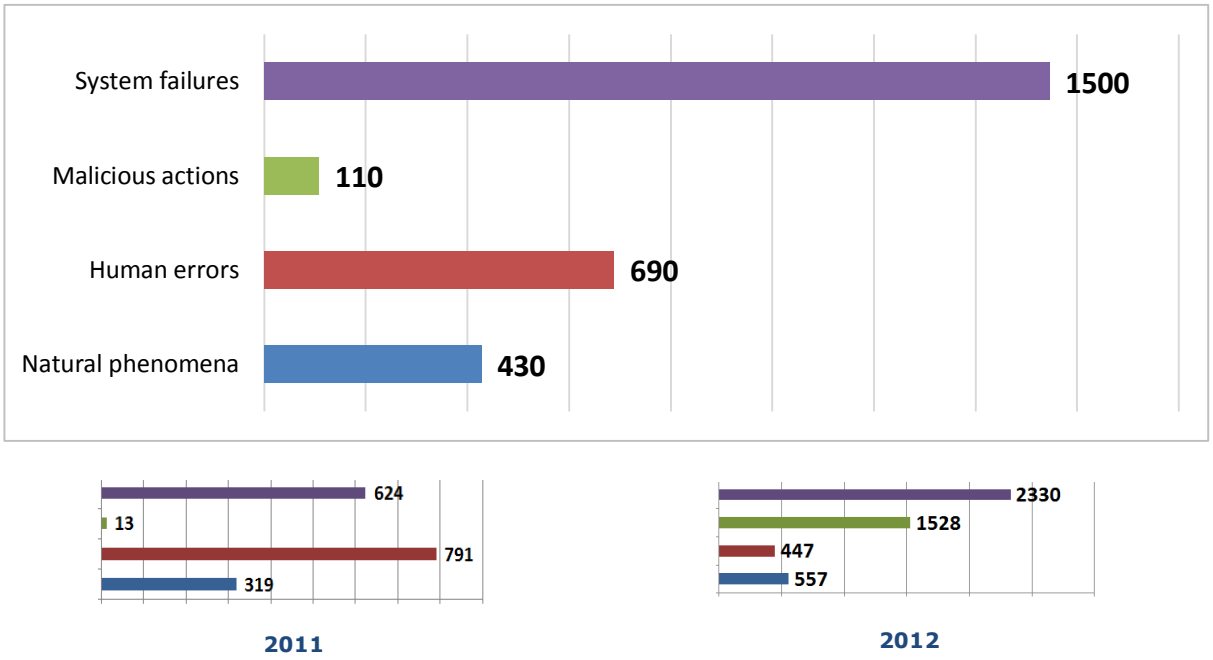

Figure 17: Average number of user connections affected per incident per root cause (1000s)

System failures affected most user connections; on average over 1.5 million user connections per incident.

Comparing with the analysis of the duration, this means that incidents caused by malicious actions lasted very long (over 50 hours) but the number of user connections impacted in these incidents was relatively limited (on around 100 000 user connections).

4.2.6 User hours lost per root cause category

Last year we started to look at the impact in terms of user hours lost. Taking into account both the number of user connections affected and the duration of the incident yields a measure for the total impact of an incident. We call it 'user hours lost'. Natural phenomena had most impact in terms of user hours lost. This suggests that this is the category of outages which affects most users most of the time. At the same time, it is important to remember that these numbers are only representative of large scale incidents, because small incidents remain below the thresholds.

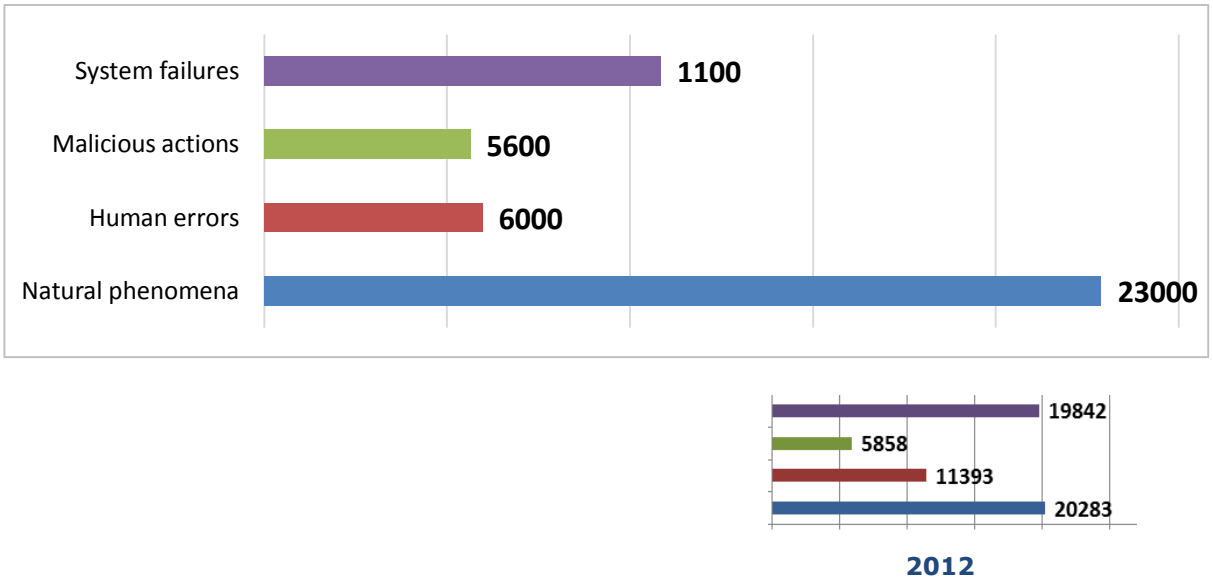

Figure 18: Average user hours lost per incident per root cause category.

Severe storm affecting power supply and mobile networks causing large scale mobile outage (duration: days, connections: thousands, cause: natural phenomena and third party failure): *A deep low-pressure with storms and hurricane winds caused power outages, damaged transmission lines to mobile sites and damaged access networks. Hundreds of GSM and LTE sites and thousands of UMTS sites were affected, with some lasting longer than 72 hours.*

4.3 Detailed causes

Root cause categories are rather broad. In this section we look at the detailed causes of incidents. The detailed causes give a better overview of what are technically the causes of incidents.

To explain the difference between root cause categories and detailed causes: Take for example an incident in which a storm leads to a power cut which leads to an outage. For this incident both storm and power cut are detailed causes.

4.3.1 Detailed causes of all incidents

In 2013, the most common causes of incidents were 'software bug' and 'hardware failure'. This was also the case for the previous two years. Also 'power cut' was among the top four causes during all three years. For the 2013 reporting, we added 'software misconfiguration' as a cause, which turned out to be a significant cause of incidents[3].

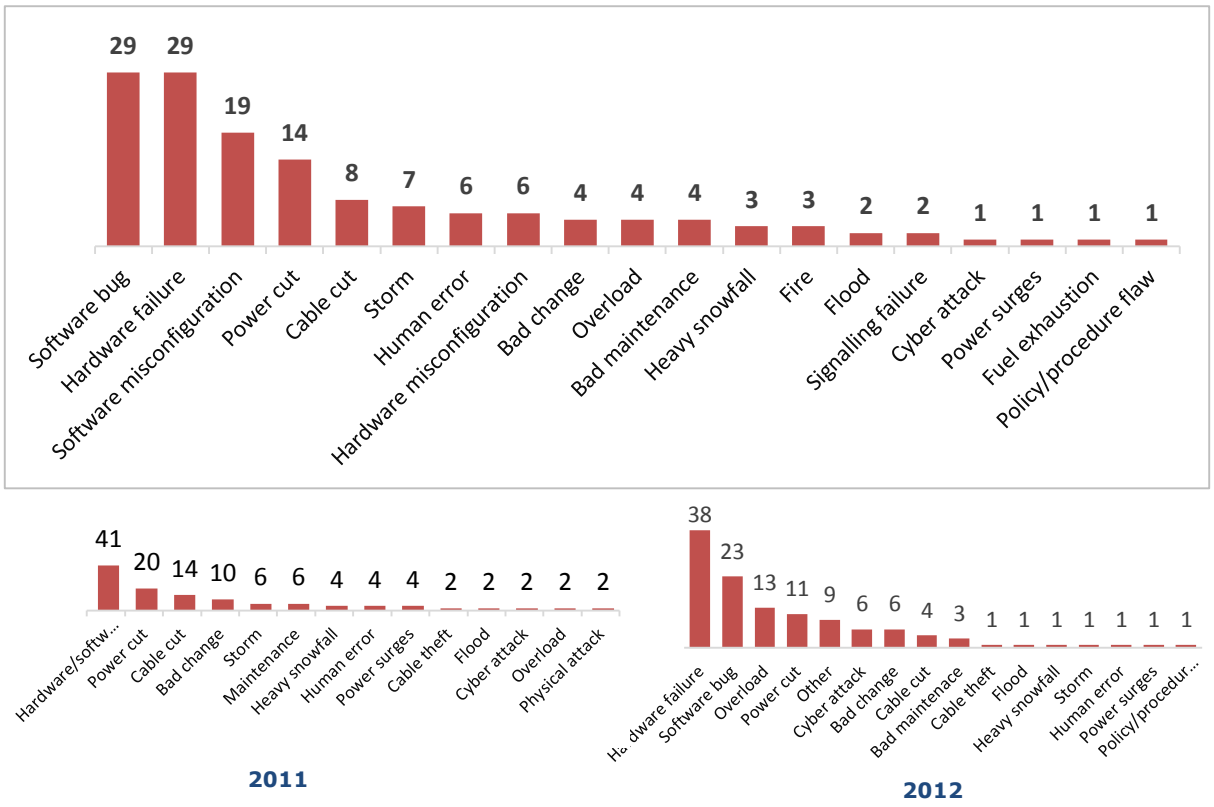

Figure 19: Detailed causes of reported incidents (percentage)

Outage for mobile Internet users caused by hard disc failure (duration: hours, connections: thousands, cause: hardware failure): *A hard disc failure occurred on one of the Serving GPRS Support Nodes (SGSN) when swapping over to a backup image on a redundant disc. All connectivity was lost to the SGSN leaving hundreds of thousands subscribers without mobile Internet access for eight hours.*

[3] The list of causes has been fine-tuned if compared with past editions of this Report. For example, the cause hardware/software failure (2011) was split in 2012, and the causes software misconfiguration, hardware misconfiguration, fire and wildfire were added for the 2013 reporting.

4.3.2 Detailed causes per service

Now we split up the data about detailed causes for each of the four services (fixed telephony, fixed Internet, mobile telephony and mobile Internet) - see figures 20, 21, 22 and 23 below. Many incidents with an impact on fixed telephony and fixed Internet were caused by power cuts, and many incidents with an impact on mobile Internet and mobile telephony were caused by hardware failures and software bugs but also power cuts was a significant cause of failure.

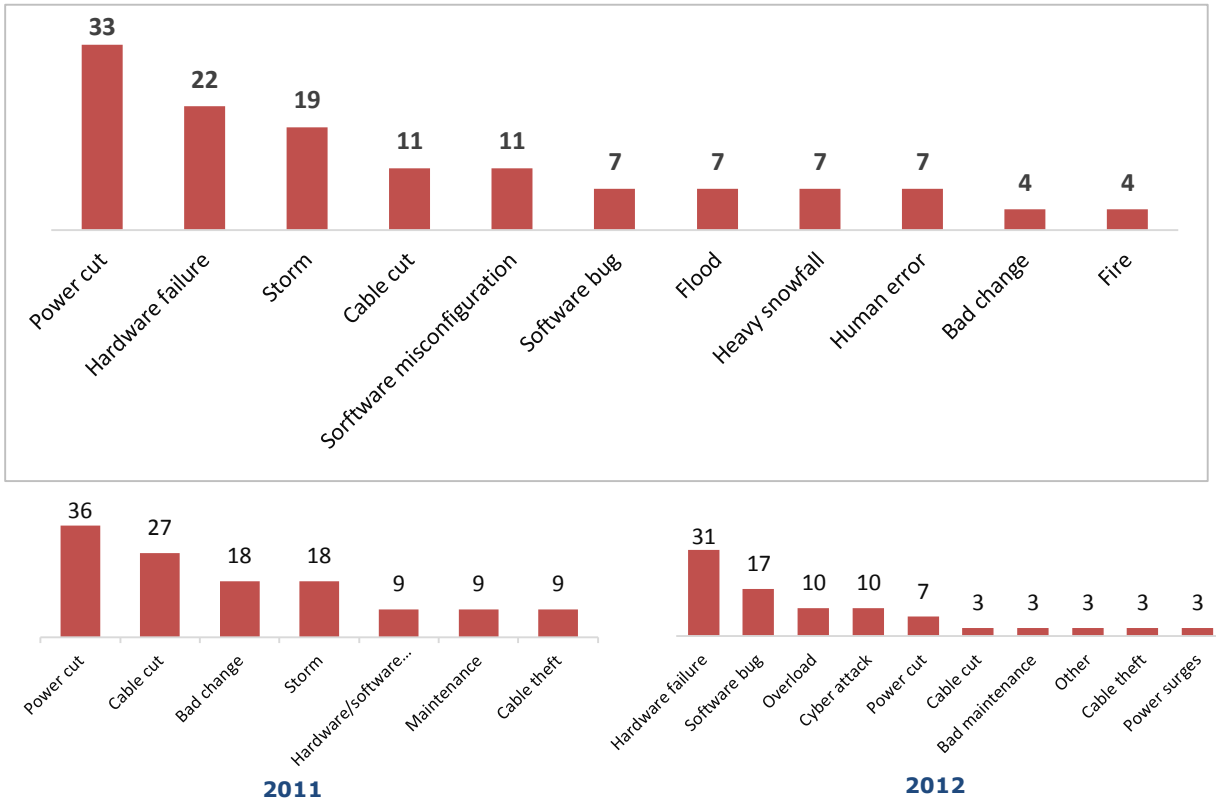

Figure 20: Detailed causes for fixed telephony (percentage).

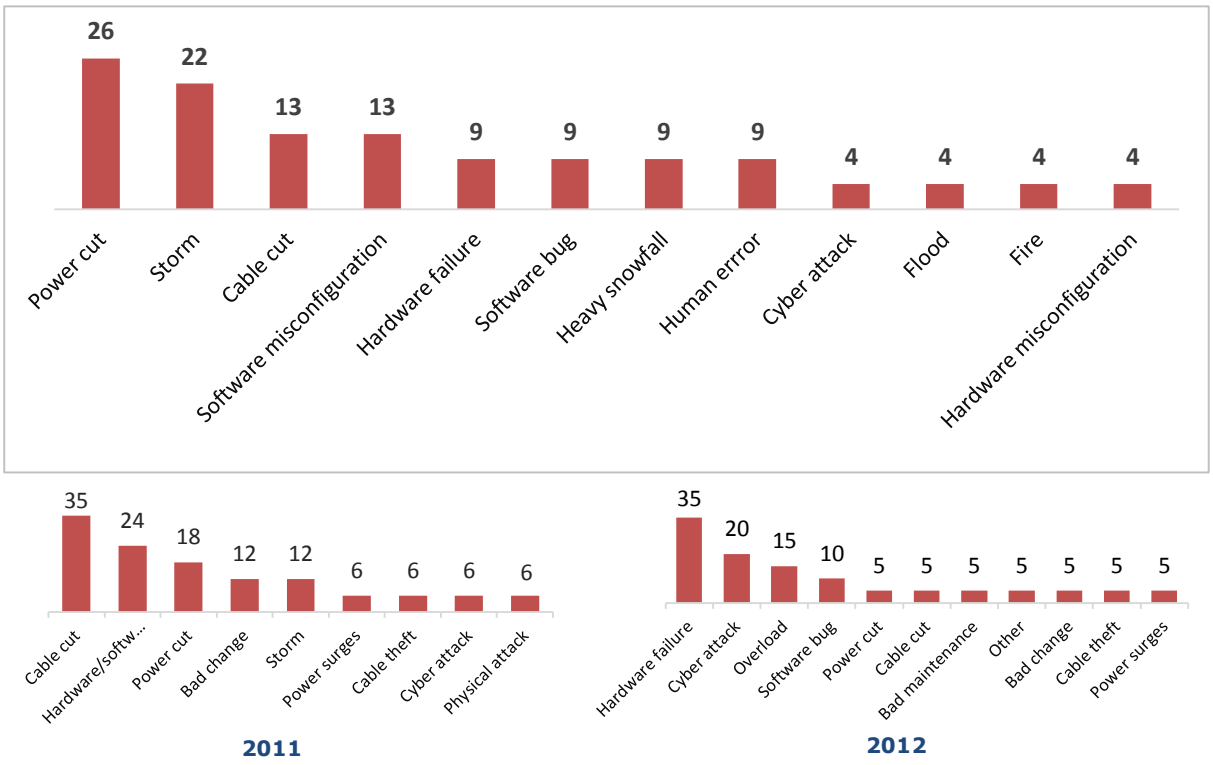

Figure 21: Detailed causes for fixed Internet (percentage).

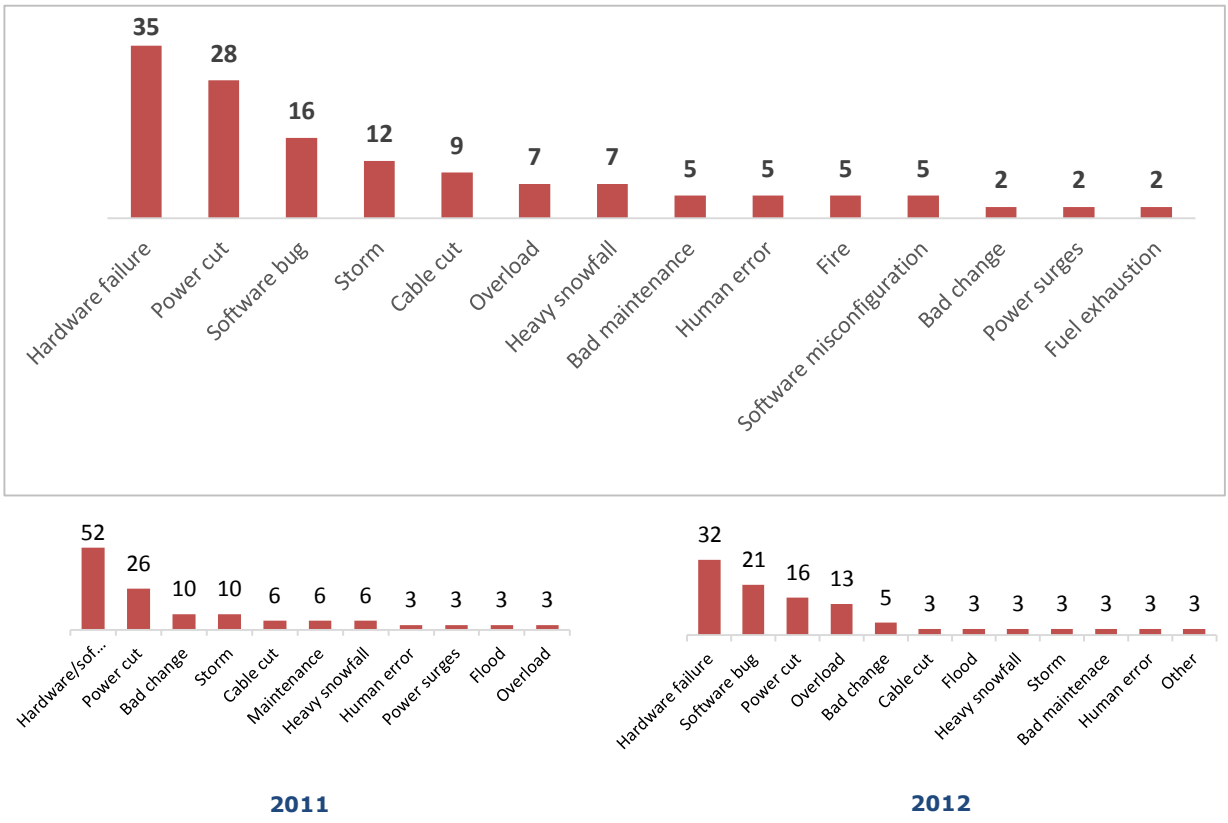

Figure 22: Detailed causes for mobile telephony (percentage).

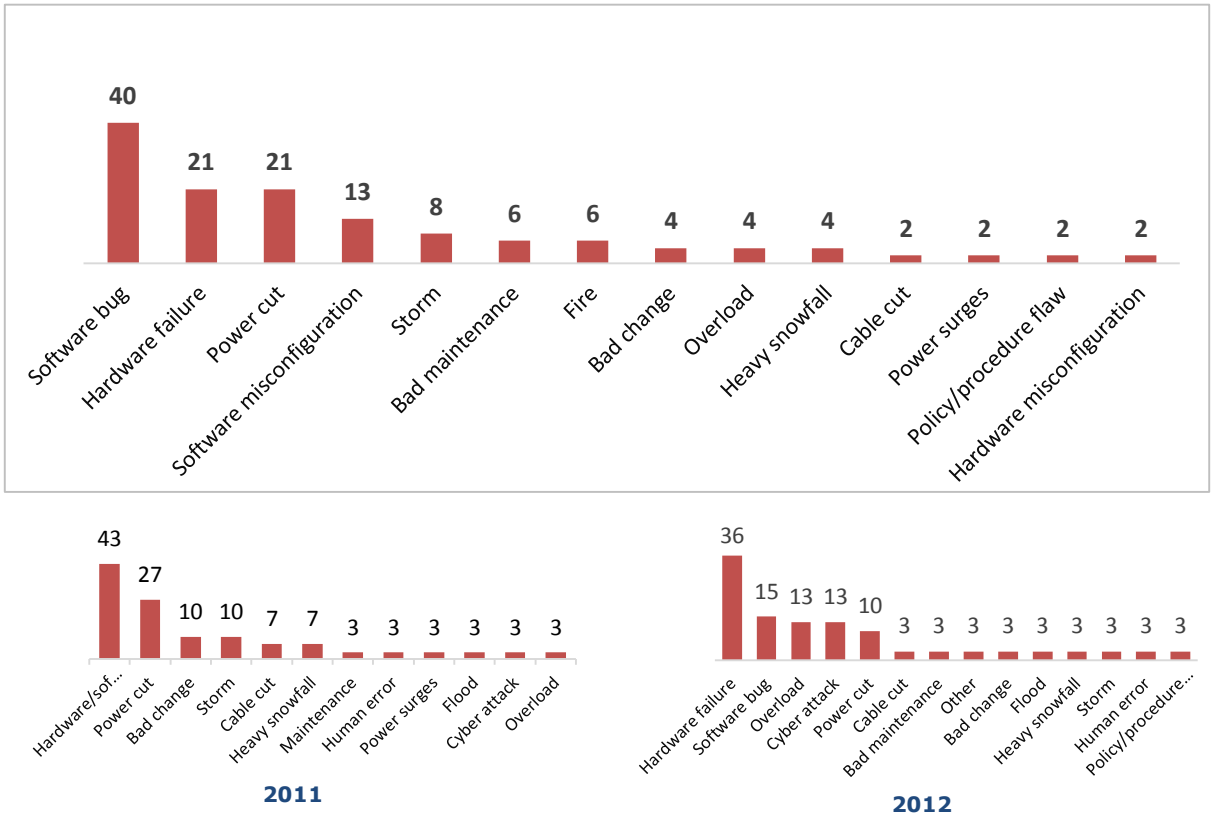

Figure 23: Detailed causes for mobile Internet (percentage).

4.3.3 Average duration of incidents per detailed cause

Last year we started to look at average duration of incidents, user connections affected and impact in terms of duration times the user connections affected for the detailed causes.

Incidents caused by Fire and Heavy Snowfall had the longest duration (86 and 62 hours respectively) followed by power cuts (53 hours) and Storms (47 hours).

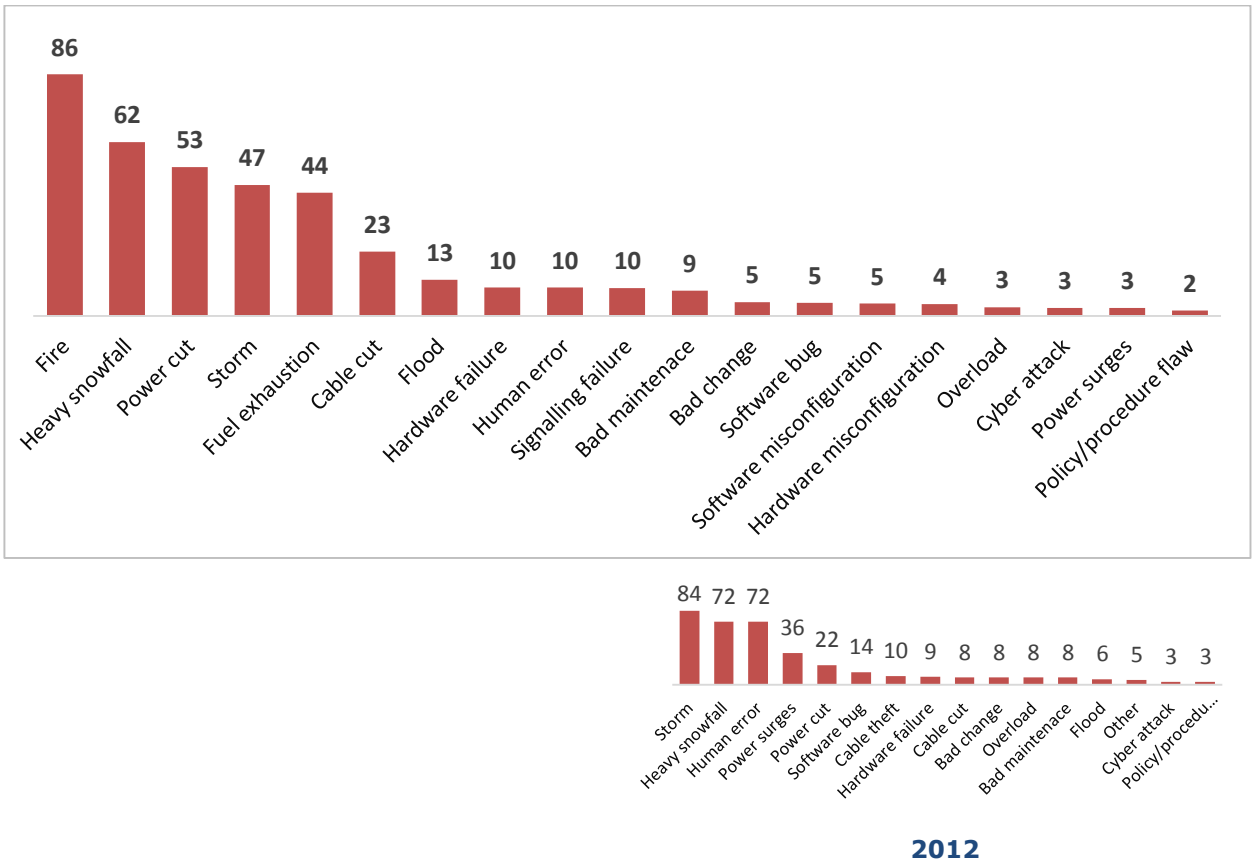

Figure 24: Average duration of incidents per detailed cause (hours).

Snowstorms caused mobile service outages (durations: days, connections: thousands, cause: heavy snowfall): *The weather conditions were unusually bad for five days causing outages to mobile communications in 50 villages and smaller towns. 150 2G base stations and 50 3G stations all in all went down.*

4.3.4 Average number of user connections affected per detailed cause

Software bugs were the cause affecting most user connections (more than 2.4 million connections on average per incident) followed by power surges and bad maintenance with 2 million and 1.2 million affected connections respectively.

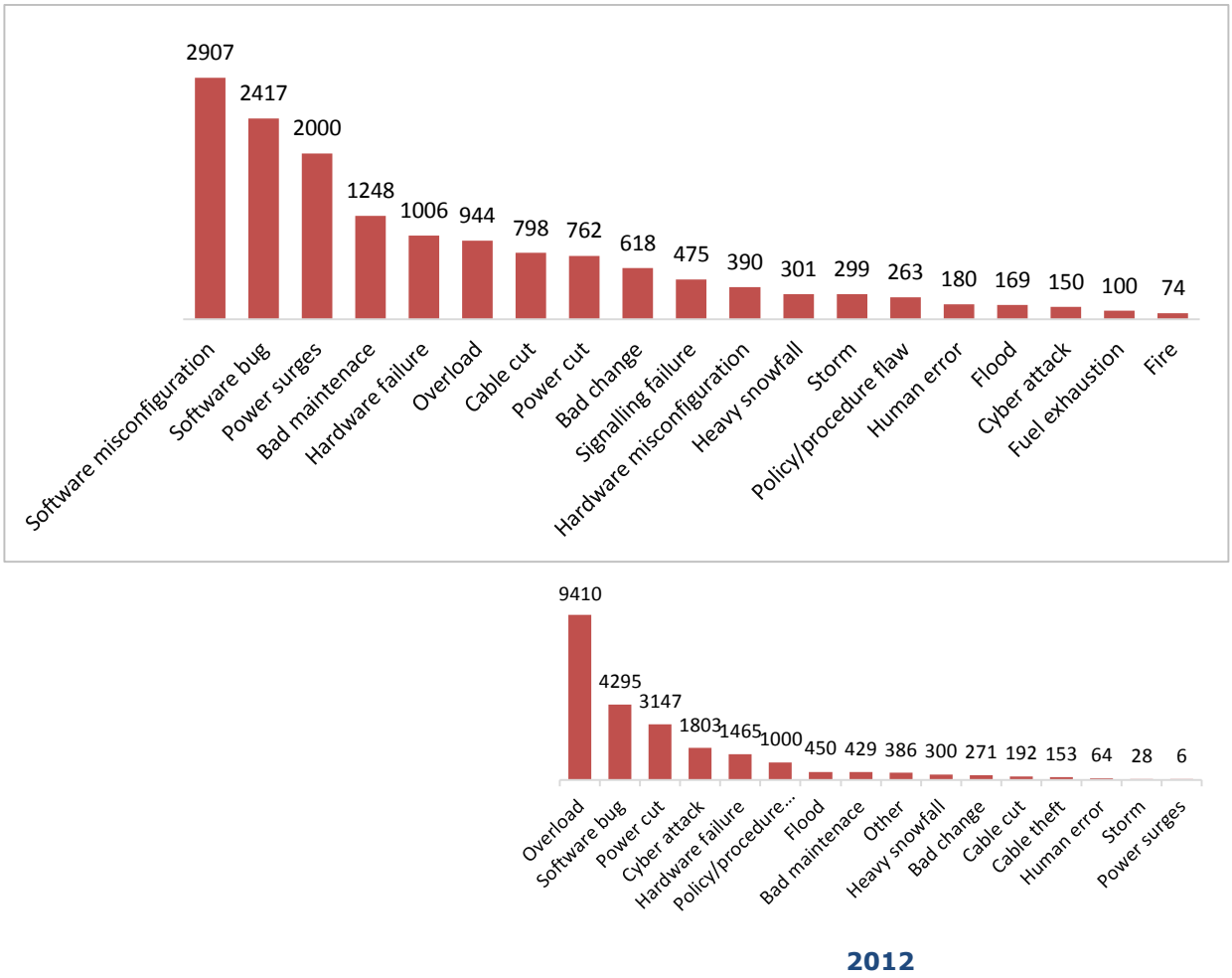

Figure 25: Average number of user connections affected per incident per detailed cause (1000s).

Software bug caused outage for millions of mobile Internet users nationally (duration: hours, connections: millions, cause: software bug): *Mobile data transmission services failed for three million users for several hours caused by the database for tariff management running out of memory space. Due to a software bug, no memory storage alerts were submitted and the services provided by the database could not be automatically restarted.*

4.3.5 User hours lost per detailed cause

Power cuts are the detailed cause that had most impact in terms of user hours lost, followed by heavy snowfall and cable cut. Also in 2012 Power cuts had high impact. Cyber-attacks did not have any significant impact on electronic communications during 2013.

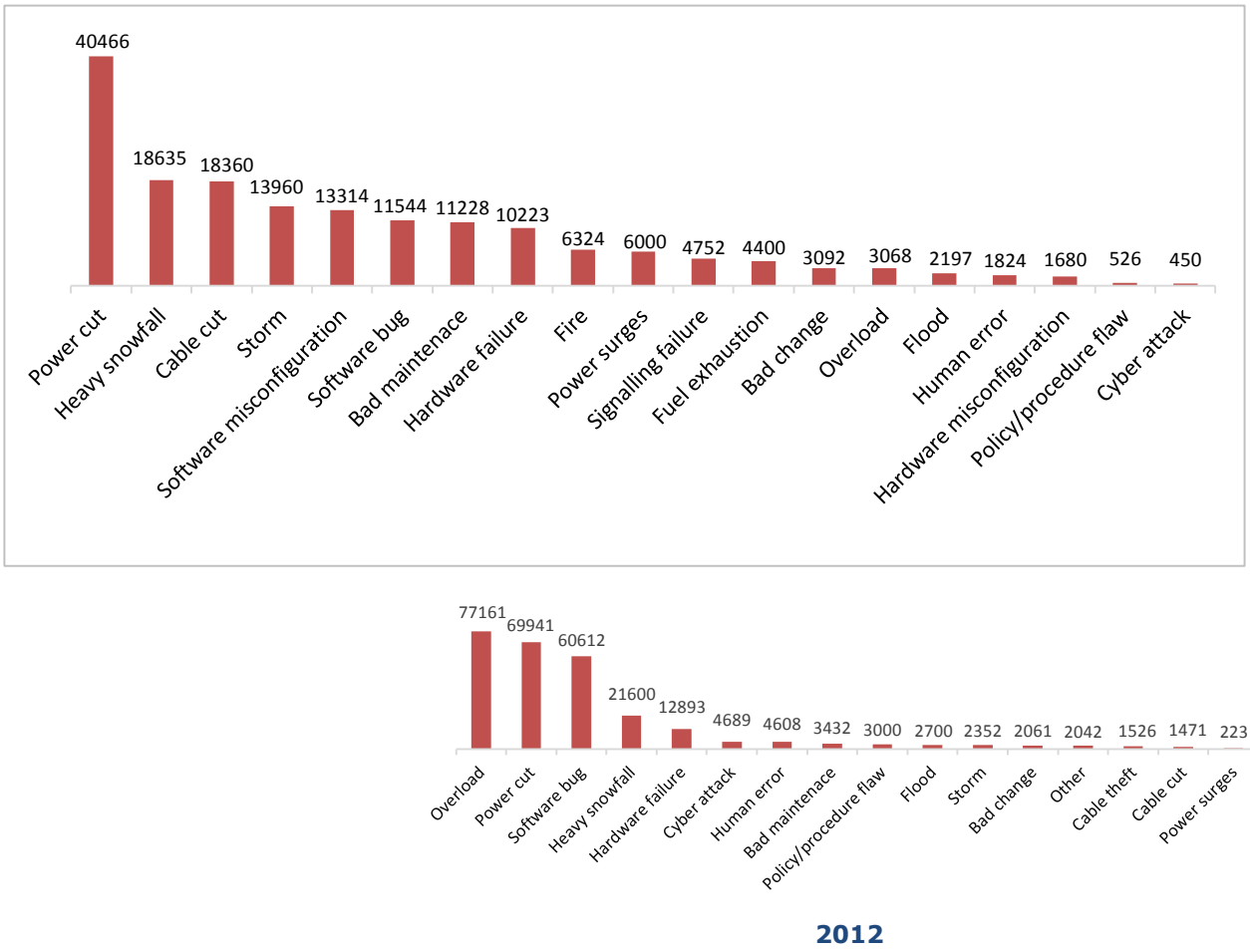

Figure 26: Average user hours lost per incident per detailed cause.

Power failure caused service failure for virtual mobile operator (duration: hours, connections: thousands, cause: power failure):
Loss of primary and secondary power to the data centre of a Mobile Virtual Network Operator caused a loss of voice and data connections. After reinstating the primary circuit breaker, power was restored and subsequent actions returned the equipment to full service.

4.4 Assets affected

For the second year we received reports from NRAs about which components or assets of the electronic communications networks were affected by the incidents. This provides some more information about the nature of the outages and what assets of the infrastructure that were primarily involved in them.

4.4.1 Assets affected overall

Base stations and controllers were the assets most affected, followed by Switches. Also in 2012 Base stations and Switches were in the top three in terms of assets affected.

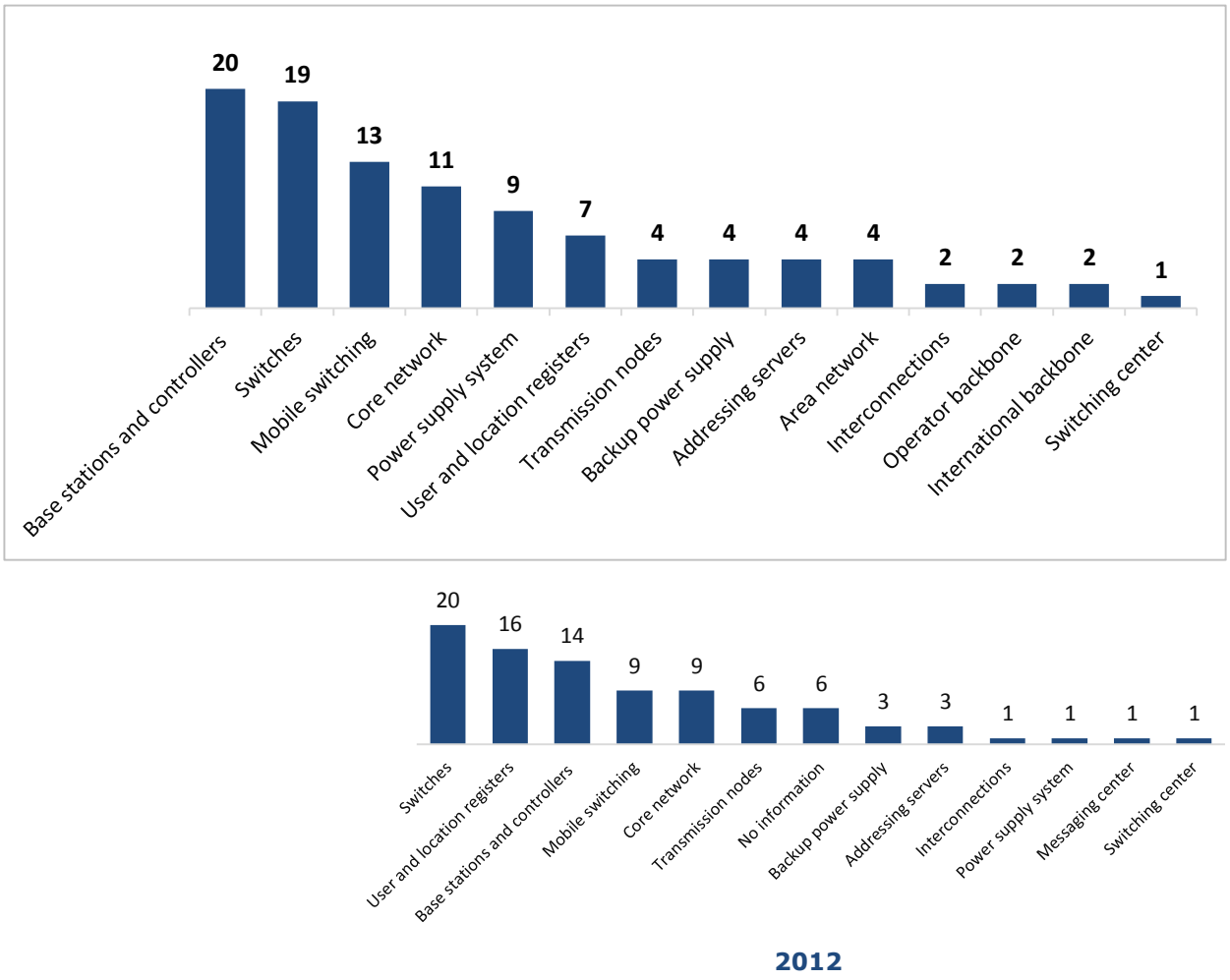

Figure 27: Assets affected by the incidents (percentage).

Power cuts due to bad weather shut down mobile base stations (duration: days, connections: thousands, causes: power cut): *A severe storm caused long lasting power cuts leading to mobile communication base stations shutting down. Also communication cables had physical breaks. Over 200 2G and 100 3G base stations became non-operational for about four days.*

4.4.2 Affected assets in system failures

System failure was the most common root cause category for all incidents in 2013. In these system failures the most often affected assets were the Mobile Switching Centres (MSC), the switches and routers, and the base stations.

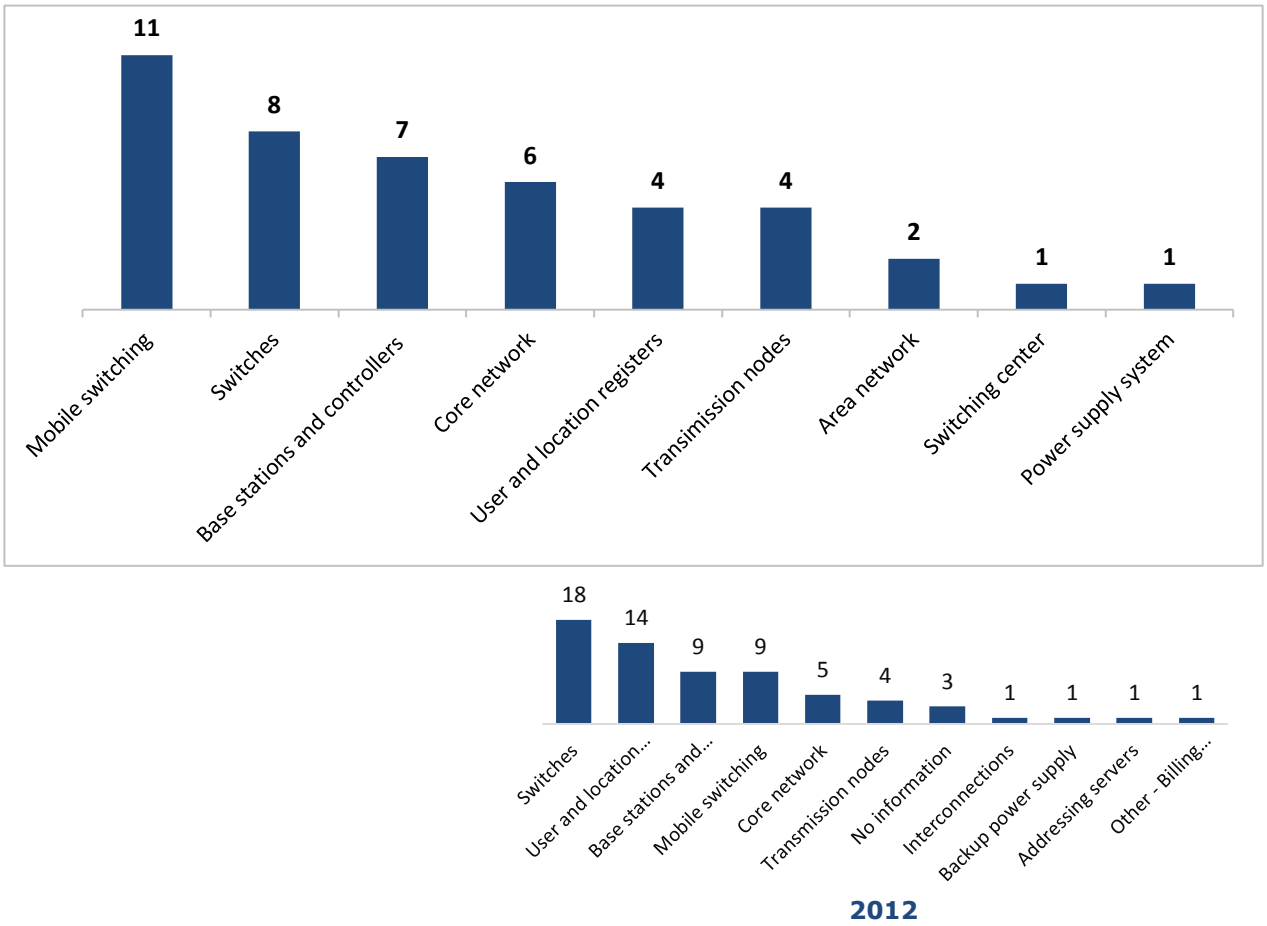

Figure 28: Assets affected by system failures (percentages).

Switching server failure caused mobile outage (duration: hours, connections: thousands, cause: system failure): *Due to a failure in a switching server, mobile communications (2G and 3G) became unavailable in a large part of the country.*

4.4.3 VoIP versus PSTN

We also split the service fixed telephony into traditional circuit switched fixed telephony (PSTN) and fixed IP based telephony (VoIP) to see what are the common detailed causes. Both PSTN and VoIP were mostly affected by storms. PSTN was also affected by hardware failure, and on third place power cuts and flood, whereas VoIP was evenly affected by hardware failure, software bugs, bad change and flooding. Figure 29 shows the overall picture of the causes, for incidents affecting PSTN and VoIP services.

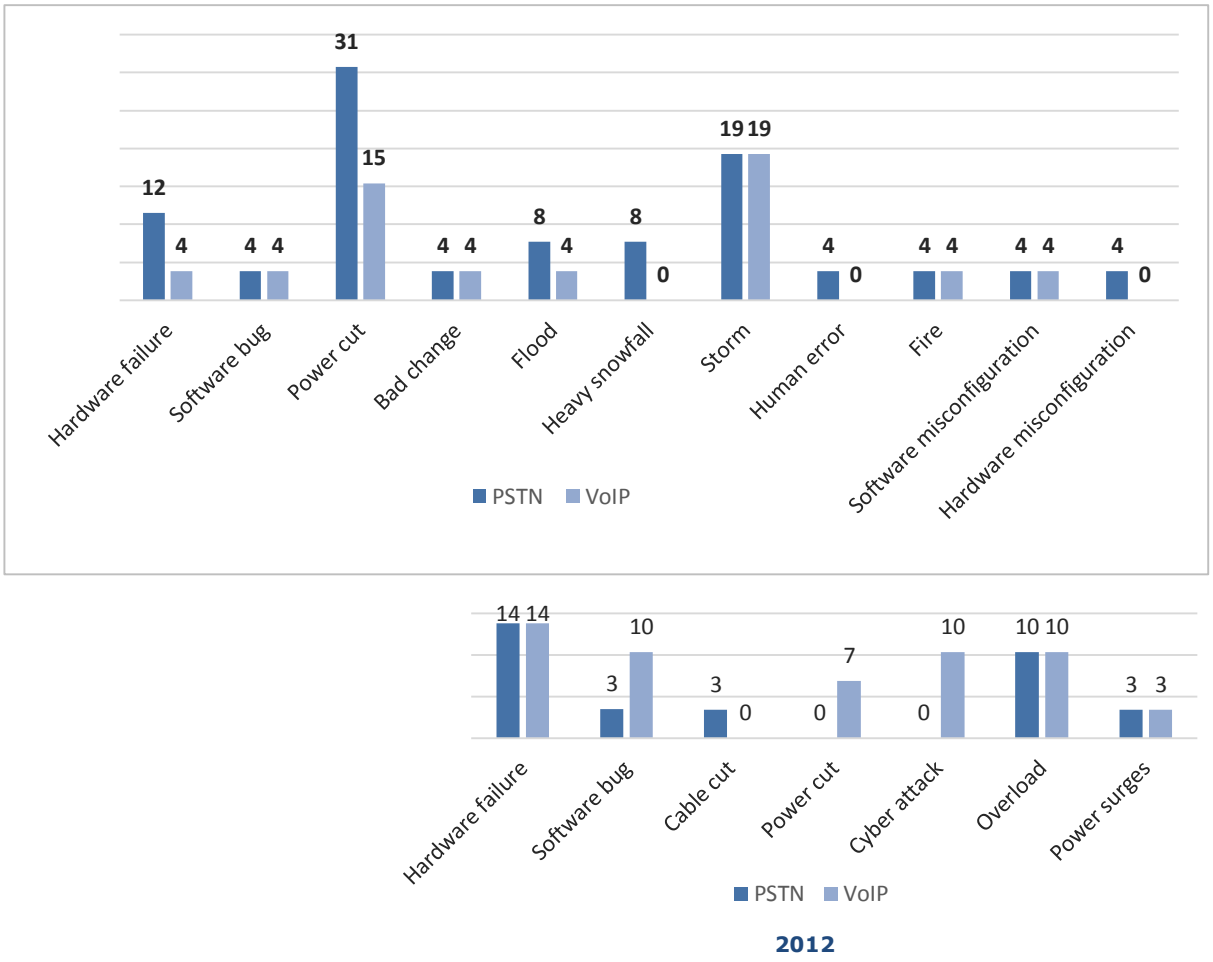

Figure 29: Detailed causes for incidents affecting PSTN and VoIP (percentage).

5 Conclusions

In this Report 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 incident reports from 2013. ENISA and the Commission received as part of the third round of reporting from the National Regulatory Authorities 90 reports about major incidents that occurred in 2013.

From the 90 significant incidents reported to ENISA and the European Commission, the following conclusions can be drawn.

- **Mobile networks most affected:** Most incidents affected mobile Internet followed by mobile telephony (53 % and 48 % respectively).
- **Mobile network outages affect many users:** Incidents affecting mobile Internet or mobile telephony affected most users (around 1.4 million users and 700 000 users respectively per incident). This is consistent with the high penetration rate of mobile telephony and mobile Internet.
- **Emergency Services are affected by incidents**: In 21 % 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 (61 % of the incidents). This was the most common root cause category for mobile networks. In the category system failures, software bugs and hardware failures were the most common causes. The assets most often affected by system failures were switches (e.g. mobile switching and routers) and base stations and controllers.
- **System failures affect many users:** Incidents categorized with the root cause system failures, affected around 1.5 million user connections on average per incident. Incidents involving the detailed cause software bug affected around 2.5 million connections on average per incident.
- **Natural phenomena and malicious actions cause long lasting incidents:** Incidents caused by natural phenomena (mainly storms and heavy snowfalls) and malicious actions lasted on average 54 and 53 hours respectively.
- **Power cuts and heavy snowfall have most impact:** Incidents caused by power cuts followed by heavy snowfall respectively had most impact in terms of number of user connections affected multiplied by the duration of the incident.
- **Base stations and Switches most affected by incidents:** Overall, base stations, switches and mobile switching were the network components most affected by incidents.

Based on the annual summary reporting of 2011 and 2012 incidents, ENISA analysed in 2013 the dependencies in the electronic communications sector on power supply and issued recommendations regarding the sector's ability to withstand and act efficiently after power cuts. ENISA also studied in 2013 national roaming for increased resilience in mobile networks. This year, based on the annual summary reporting of 2012 and 2013 incidents, ENISA is issuing recommendations for providers about how to manage security requirements for vendors and outsourcing partners they use for their core operations. Based on the 2012 and 2013 summary reporting ENISA is also studying national initiatives to reduce the number of under-ground cable breaks caused by mistakes.

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, Ministries and the European Commission for a fruitful collaboration and we look forward to leveraging this kind of reporting to further improve the security and resilience of the electronic communications sector in the EU and more generally for supervision of security also in other critical sectors. The next annual report will be published in summer 2015, for the 2014 incidents.

References

Related ENISA papers

- The Article 13a EG technical guidelines on incident reporting and on security measures: https://resilience.enisa.europa.eu/article-13
- ENISA's reports about the 2011 and 2012 incidents, reported under Article 13a: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/annual-reports
- ENISA's study 2013 on Power Supply Dependencies in the Electronic Communications Sector: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/power-supply-dependencies
- ENISA's study 2013 on National Roaming for Resilience: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/national-roaming-for-resilience
- 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 5 years ago: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/good-practice-guide-on-incident-reporting/good-practice-guide-on-incident-reporting-1

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.

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