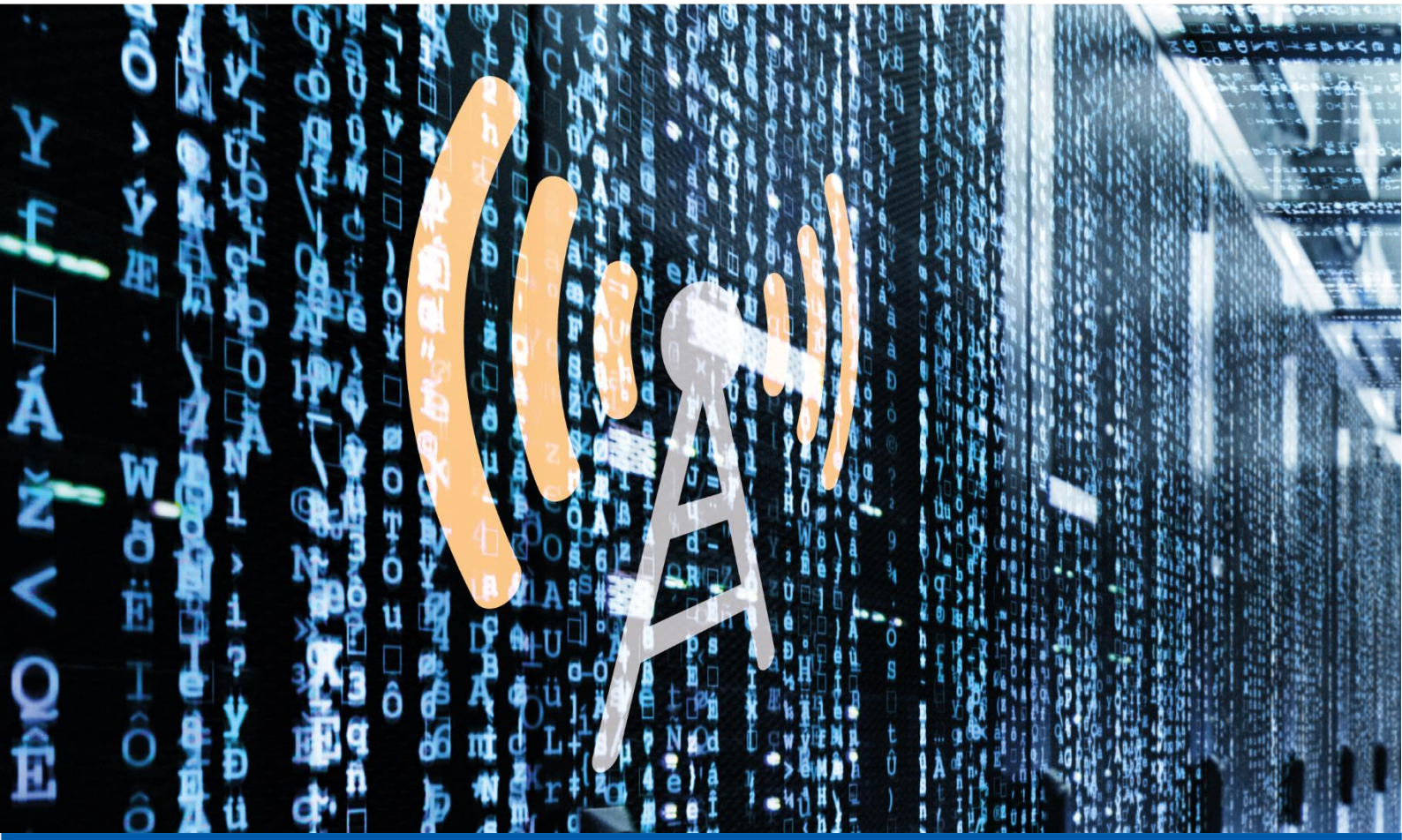
enisa

EUROPEAN UNION AGENCY
FOR CYBERSECURITY



TELECOM SERVICES SECURITY INCIDENTS 2019

Annual Analysis Report

JULY 2020

ABOUT ENISA

The mission of the European Union Agency for Cybersecurity (ENISA) is to achieve a high common level of cybersecurity across the Union, by actively supporting Member States, Union institutions, bodies, offices and agencies in improving cybersecurity. We contribute to policy development and implementation, support capacity building and preparedness, facilitate operational cooperation at Union level, enhance the trustworthiness of ICT products, services and processes by rolling out cybersecurity certification schemes, enable knowledge sharing, research, innovation and awareness building, whilst developing cross-border communities. Our goal is to strengthen trust in the connected economy, boost resilience of the Union's infrastructure and services and keep our society cyber secure. More information about ENISA and its work can be found www.enisa.europa.eu.

CONTACT

For technical queries about this paper, please email resilience@enisa.europa.eu
For media enquires about this paper, please email press@enisa.europa.eu

AUTHORS

Georgia Bafoutsou, Aggelos Koukounas, Marnix Dekker - ENISA

ACKNOWLEDGEMENTS

We are grateful for the review and input received from the experts in the ENISA Article 13a Expert Group which comprises national telecom regulatory authorities (NRAs) from in the EU and EEA, EFTA and EU candidate countries.

LEGAL NOTICE

COPYRIGHT NOTICE

Catalogue number: TP-AD-20-001-EN-N
ISBN: 978-92-9204-350-6
DOI: 10.2824/491113

TABLE OF CONTENTS

EXECUTIVE SUMMARY

In 2019, half of the total user hours lost were due to system failures.

In 2019, human errors were more frequent, an increase of 50% compared to 2018

In the EU, telecom operators notify significant security incidents to the National Regulatory authority (NRA) in their country. At the start of every calendar year, the national authorities for telecom security send a summary about these incidents to ENISA. This document, the Annual Report Telecom Security Incidents 2019, covers the incidents reported by the authorities for the calendar year 2019 and it gives an anonymised, aggregated EU-wide overview of telecom security incidents.

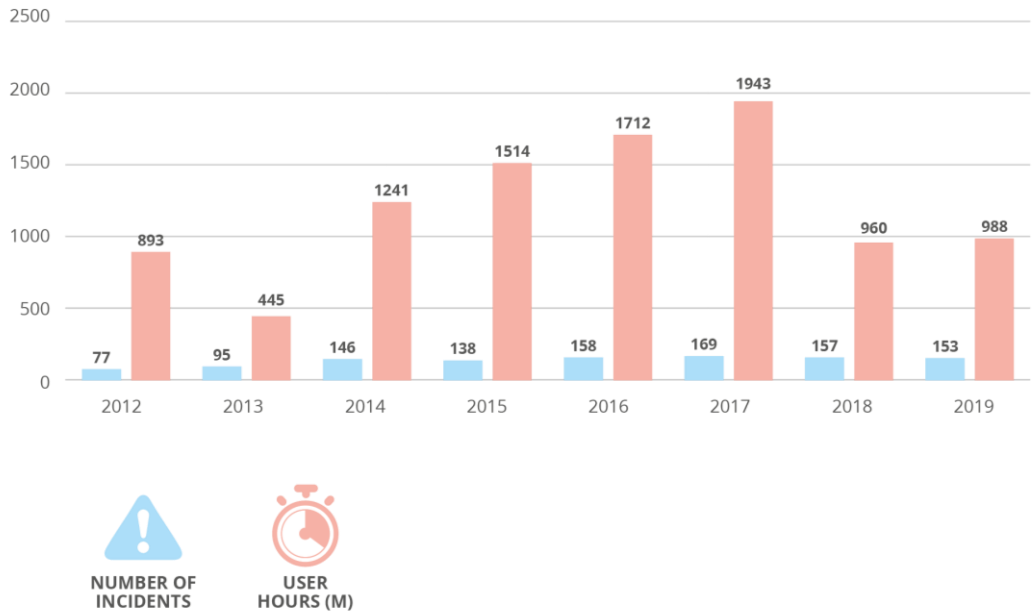
Security incident reporting has been part of the EU's telecom regulatory framework since the 2009 reform of the telecom package: Article 13a of the Framework directive (2009/140/EC) came into force in 2011. The incident reporting in Article 13a focuses on security incidents with significant impact on the operation of services, i.e. outages of the electronic communication networks and/or services.

Statistics annual summary reporting 2019

The 2019 annual summary reporting contains reports about 153 incidents submitted by national authorities from the 26 EU Member States and 2 EFTA countries. The total user hours lost, multiplying for each incident the number of users and the number of hours was 988.12 Million User Hours, i.e. roughly 0.026% of the total user hours in a year[1].

It should be noted that the current incident reporting is not the full telecom security picture, because it only covers the largest incidents that cause the big outages.

Figure 1: Number of incidents and million user hours lost per year



[1] Using a basis of 500M (EU citizens) times 365 (days) times 24 (hours). User hours is a metric we use throughout this report to quantify the impact of an incident, multiplying the number of subscribers/connections affected, with the duration in hours. For example, 1M User Hours means 1M users were affected for one hour, or 2M users for half an hour, etc.

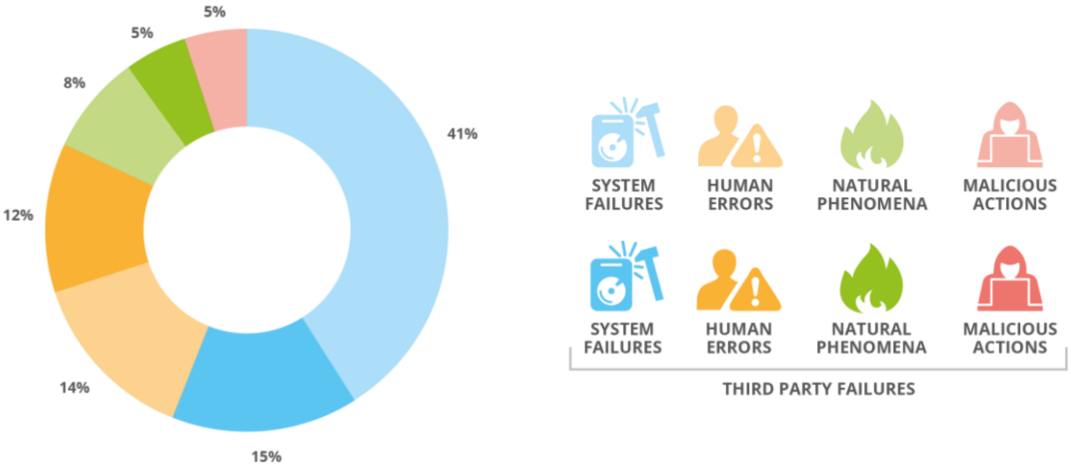
Key takeaways from the 2019 incidents

- **System failures dominate in terms of impact:** they represent almost half of the total user hours lost (479 million user hours). They are also the most frequent root cause of incidents: 56% of the total. Over the last 4 years, both the frequency and overall impact of system failures have been trending down significantly.

- **Incidents caused by human errors have risen:** More than a quarter (26%) of total incidents have human errors as a root cause. Human errors have increased with 50% compared to the previous year.

- **Third-party failures show a great increase:** Almost a third of the incidents were also flagged as third-party failures (31%), i.e. incidents which originated in third party, say a utility company, a contractor, a supplier, etc. This number tripled compared to 2018, when it was just 9%.

Figure 2: Root Causes and Third party failures – 2019



- **Power cuts are the second most common detailed cause:** Overall, independent from the underlying root cause, power cuts are either a primary or a secondary cause in over a fifth of the major incidents.

- **Natural phenomena have a major impact:** Natural phenomena account for a third of the total user hours lost, which brings them in the second place in terms of impact.

Figure 3: Share of user hours lost for each root cause category in 2019

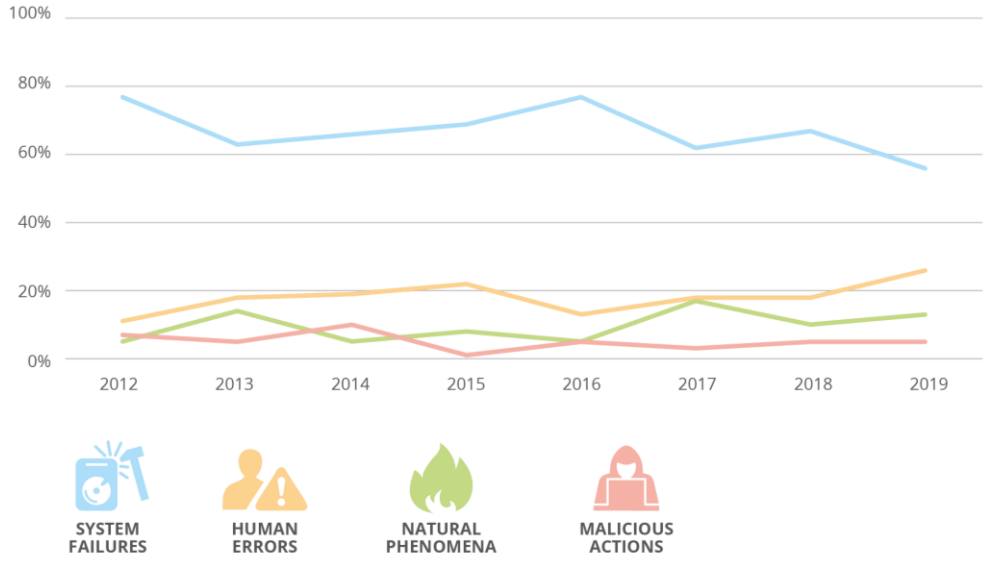
ENISA offers an online visual tool for analysing the incidents. It can be used to dive into other aspects and detailed causes. See:

https://www.enisa.europa.eu/topics/incident-reporting/cybersecurity-incident-report-and-analysis-system-visual-analysis/visual-tool

Multiannual trends over 8 years of reporting

Every year, the incident data points to important issues and trends. Apart from the national initiatives, the EU telecom security authorities also collaborate with ENISA on an EU level to analyse and work on specific issues.

Figure 4: Root cause categories Telecom security incidents in the EU - reported over 2012-2019



- **Total number of incidents reported is stabilizing at around 160:** Over the period 2014-2019, there is a consistent number of incidents reported which is stabilizing at around 160 incidents per year.
- **Sharp drop of the average impact of incidents:** Until 2017, there was a gradual increase of total user hours lost per year. But in 2018 we see a sharp drop in the total user hours lost compared to previous years. This trend continues in 2019.
- **Share of incidents caused by human errors is trending up:** The percentage of incidents caused by Human errors in regards with the total number of incidents has been trending up since 2016 and now in 2019 they account for 21% of the total number of incidents.
- **System failures continue to be the most frequent cause of incidents, but their average size is trending down:** Every year system failures have been the most common root cause category. Although, since 2016 the average size of these incidents is decreasing, between 2018 and 2019 we observe a slight increase in lost user hours due to system failures, and a corresponding decrease to hours lost due to natural phenomena.
- **Frequency and impact of malicious actions stable:** Over the reporting period the frequency of malicious actions is stable (approximately accounting for 5% of incidents per year). Their impact in terms of user hours is stable also.

We refer the reader to the body of this paper for more details.

Outlook

Security incident reporting has is a hallmark of EU cybersecurity legislation and it is an important enabler for cybersecurity supervision and policy making, at national and EU level. Since 2016 security incident reporting is also mandatory for trust service providers in the EU, under Article 19 of the EIDAS regulation. In 2018, under the NIS Directive (NISD), security incident reporting became mandatory for Operators of Essential Services in the EU and for Digital Service Providers, under Article 14 and Article 16 of the NIS directive.

By the end of 2020, the European Electronic Communications Code (EECC) will come into effect across the EU. Under Article 40 of the EECC the incident reporting requirements have a broader scope, including not only outages, but also breaches of confidentiality, for instance. Also, there are more services in scope of the EECC, including not only traditional telecom operators, but also for example over-the-top providers of communications services.

In 2020, the annual reporting guideline will be updated to include new thresholds for annual summary reporting to ENISA combining quantitative and qualitative parameters and also the notification of security incidents affecting not only the services of fixed and mobile internet and telephony, but also the number-based interpersonal communications services and/or number independent interpersonal communications services (OTT communications services).

ENISA has been working with national authorities and experts from the private sector to prepare the ground for the above mentioned changes.

ENISA is also working with the NIS Cooperation group to find and exploit synergies between the different pieces of EU legislation, particularly when it comes to incident reporting and cross-border supervision.

We look forward to continuing our close collaboration with the EU member states, the national telecom authorities and experts from the telecom sector from across Europe to implement security incident reporting efficiently and effectively.

1. INTRODUCTION

Electronic communication providers in the EU have to notify security incidents with a significant impact on the continuity of electronic communication services, to the national telecom regulatory authorities (NRAs) in each EU member state. Every year the NRAs report a summary to ENISA, covering a selection of these incidents, i.e. the most significant incidents, based on a set of agreed EU-wide thresholds. This document, the Annual Security Incidents Report 2019, aggregates the incident reports reported in 2019 and gives a single EU-wide overview of telecom security incidents in the EU.

This is the 9th year ENISA publishes an annual incident report for the telecom sector. ENISA started publishing such annual reports in 2012. Mandatory incident reporting has been part of the EU's telecom regulatory framework since the 2009 reform of the telecom package: Article 13a of the Framework directive (2009/140/EC) came into force in 2011.

The mandatory incident reporting under Article 13a has a specific focus on security incidents with a significant impact on the functioning of the service. There is some divergence and discussion about what is in scope here, but the authorities agreed to focus on network/service outages. This would leave out of scope for example an attack involving a wiretap on an undersea cable or a BGP hijack, if the attack causes no outages. Recently the Council and Parliament agreed about an update of the EU telecom rules called the European Electronic Communications Code (EECC). The incident reporting requirements in (Article 40 of) the EECC have a broader scope, including explicitly also for example breaches of confidentiality. An incident like the one just mentioned would be reportable under (Article 40 of) the EECC.

This document is structured as follows: In section 2 we briefly summarize the reporting procedure and to give an idea about the kind of incidents that are reported we give some specific but anonymized examples of incidents that occurred in 2019. In Section 3 we provide some key facts and statistics about the 2019 incidents. In Section 4 we take a closer look at Human Errors as a root cause of incidents. In section 5 we look at multiannual trends over the years 2012-2019.

Note that conclusions about trends and comparisons with previous years have to be made with care, because national reporting thresholds have changed over the years, reporting thresholds have been lowered in most countries, and because the incident reporting only covers the most significant incidents (and not smaller incidents which may be more frequent).

This is the 9th time ENISA publishes an annual incident report for the telecom sector.

Mandatory incident reporting has been part of the EU's telecom regulatory framework since the 2009 reform of the telecom package: Article 13a of the Framework directive (2009/140/EC) came into force in 2011.

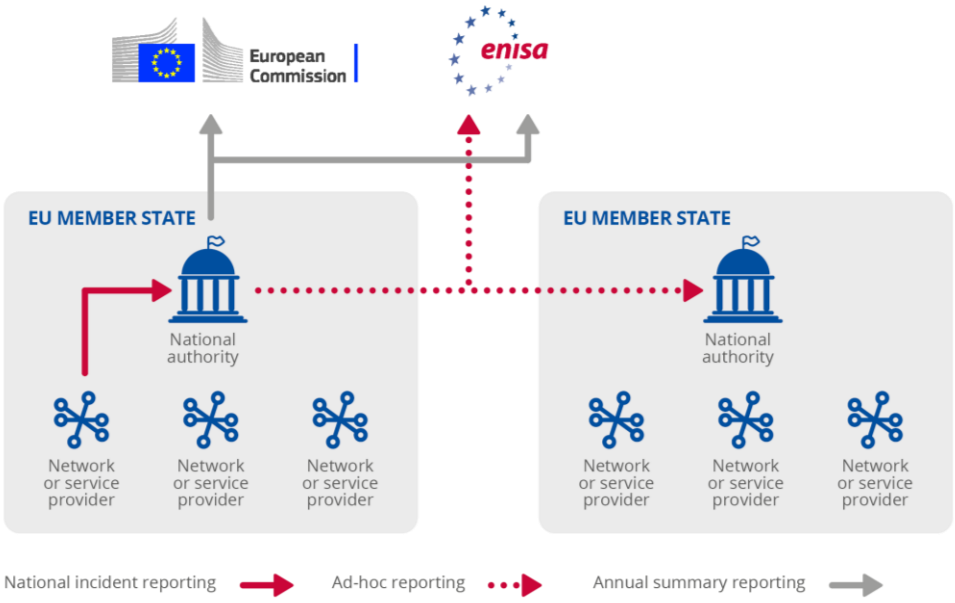
2. INCIDENT REPORTING FRAMEWORK

We briefly explain the main features of the incident reporting process, as described in the Article 13a Technical Guideline on Incident Reporting[2], which was developed in collaboration with the national authorities.

2.1 INCIDENT REPORTING FRAMEWORK

Article 13a introduces three types of incident reporting: 1) National incident reporting from providers to NRAs, 2) Ad-hoc incident reporting between NRAs and ENISA, and 3) Annual summary reporting from national authorities to the EC and ENISA. The different types of reporting are shown in the diagram below.

Figure 5: Incident Reporting Framework for Telecom Servicies



Note that in this setup ENISA acts as a collection point, anonymizing aggregating and analysing the incident reports. In the current setup NRAs can search incidents in the reporting tool (CIRAS) but the incident reports themselves do not refer to countries or providers, making the overall summary reporting process less sensitive.

2.2 EXAMPLES OF INCIDENTS REPORTED

We give some specific examples of incidents to give an idea of the kind of incidents that are notified to NRAs and then included in the annual summary reporting to ENISA:

- **Three high-capacity optical fibres were simultaneously cut, which caused mobile internet and telephony and also fixed internet and telephony outage in a national level for three hours (duration: hours, connections: thousands, cause: human errors)**: In two of these cases, the cables were cut as a result of road modernization

[2] https://resilience.enisa.europa.eu/article-13/guideline-for-incident-reporting

works (carried out by third parties); in the third case, the optical fiber was affected following a landslide. The incident had a national impact.

- **The fixed network of an operator got isolated from all other networks during 3 hours, affecting emergency calls from all the other networks for millions of users for 3 hours (duration: hours, connections: millions, cause: system failures):** Since all emergency call centres were connected to this fixed network, emergency calls were not possible from all those other networks. The cause of the incident was a software bug that caused an interconnection platform to fail due to a combination of circumstances.
  Following this incident, multiple meetings were organized between the NRA, the main operators and the emergency services to identify single points of failure and discuss possible technical solutions to avoid similar incidents in the future and reduce their impact.

- **A DDos attack caused a 13 hour outage of the VoIP service for 400.000 users (duration: hours, connections: thousands, cause: malicious actions)**: Corrective measures taken included hardening of the systems and hardening of firewall rules.

- **A power outage caused mobile telephony, internet and sms outage for 100000 users and duration of 10 hours (duration: hours, connections: thousands, cause: natural phenomena):** A power outage caused by a storm had as a result the failure of the technological terminal equipment in the whole country. All processes we set up successfully and spare power supplies were activated.

- **A software bug of a third party internet access service provider affected a data center, causing email (OTT service) outage for more than a hundred users during 8 hours (duration: hours, connections: thousands, cause: system failures:** The affected data center caused an outage of the email service. The connections with the third party internet access service provider were reduced.

2.3 INCIDENT REPORTING TOOL

In 2020, ENISA has released a new version of CIRAS, the tool for statistical analysis of cybersecurity incidents. Telecom security incidents reported for the year 2019 are available on the new CIRAS

Experts from the national authorities have access to the ENISA CIRAS incident reporting tool, where they can search for and study specific incidents. This tool anonymizes the country or operator involved.

https://www.enisa.europa.eu/topics/incident-reporting/cybersecurity-incident-report-and-analysis-system-visual-analysis/visual-tool

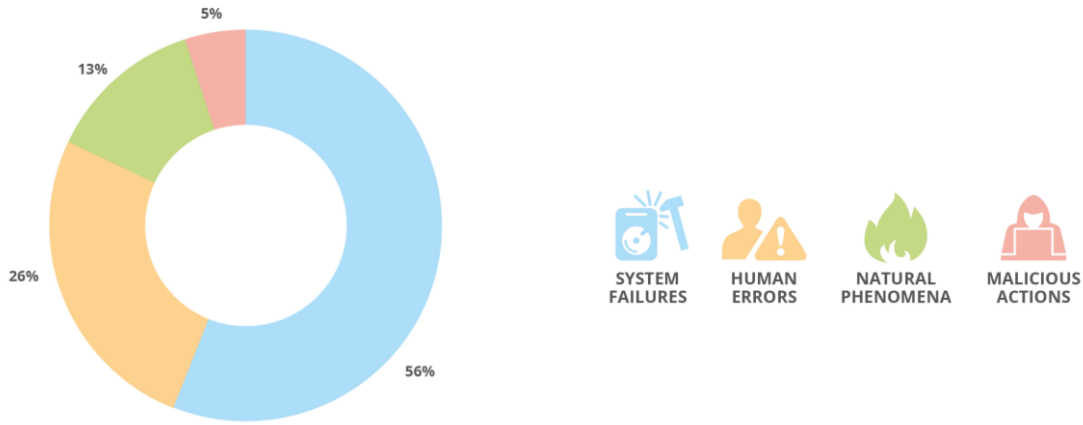
3. ANALYSIS OF THE INCIDENTS

In 2019, 26 EU Member States and 2 EFTA countries participated in the annual reporting, reporting a total of 153 significant incidents. In this section, the 153 reported incidents are aggregated and analysed. First, the impact per root cause category is analysed (in section 3.1), in section 3.2 we focus on the user hours that have been lost per root cause category, then detailed causes are examined (Section 3.3), and in Section 3.4 the impact per service is analysed.

3.1 ROOT CAUSE CATEGORIES

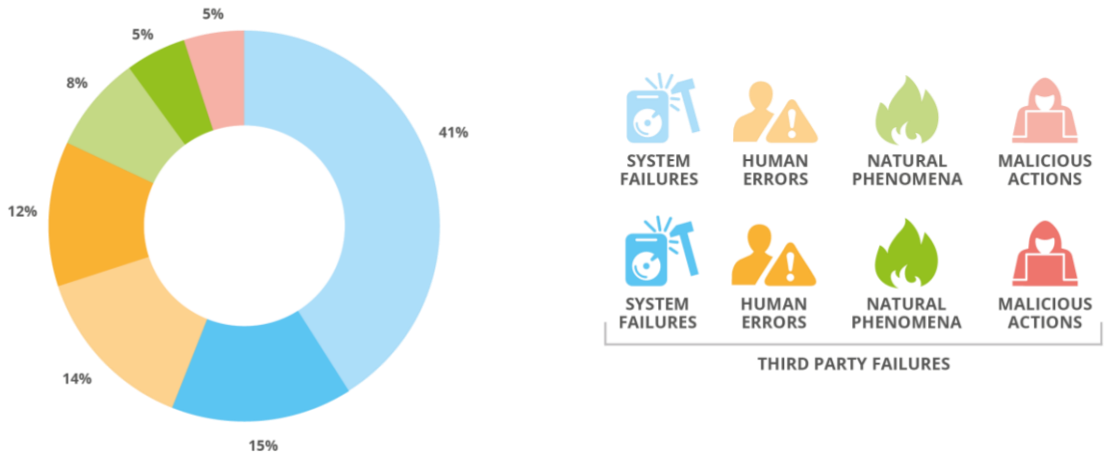
In 2019 more than half of the telecom security incidents were system failures. This is consistent with previous years, although somewhat lower. Often they are hardware failures and software bugs. Human errors show an increase, rising up to one fourth of the security incidents. Most often these are accidental cable cuts and faulty software changes/updates. 13% of the incidents are caused by natural phenomena also increased up to 30% compared to the previous year. Only 5% of incidents were due to malicious actions. Typically these cases are denial of service attacks, cable theft and arson.

Figure 6: Root cause categories Telecom security incidents – 2019



There is a fifth category called Third-party failures, which can be selected (only) in conjunction with another root cause category. Typically third party failures are incidents which happen at a utility company or supplier and then affect the telecom providers, for example a cable cut.

Figure 7: Root Causes and Third party failures - 2019



In total over 2019, 32% of incidents were flagged as third-party failures, which is greatly increased in comparison with the previous years. The division is shown in the chart below.

3.2 USER HOURS LOST FOR EACH ROOT CAUSE CATEGORY

Adding up the total user hours lost for each root cause category we find that almost half of the total user hours lost were due to system failures (48%, 479 million user hours). Natural phenomena account for almost one third of user hours lost (30%, 289 million user hours) and human errors for almost one fifth of user hours lost (21%, 208 million user hours).

Figure 8: Share of user hours lost for each root cause category in 2019

So system failures are the most common (see section 3.1) and they also have more impact than the other root causes. However, human errors have doubled their percentage in impact and they are also more common than in 2018. Also, natural phenomena have less impact than 2018, although the number of incidents caused by natural phenomena has raised.

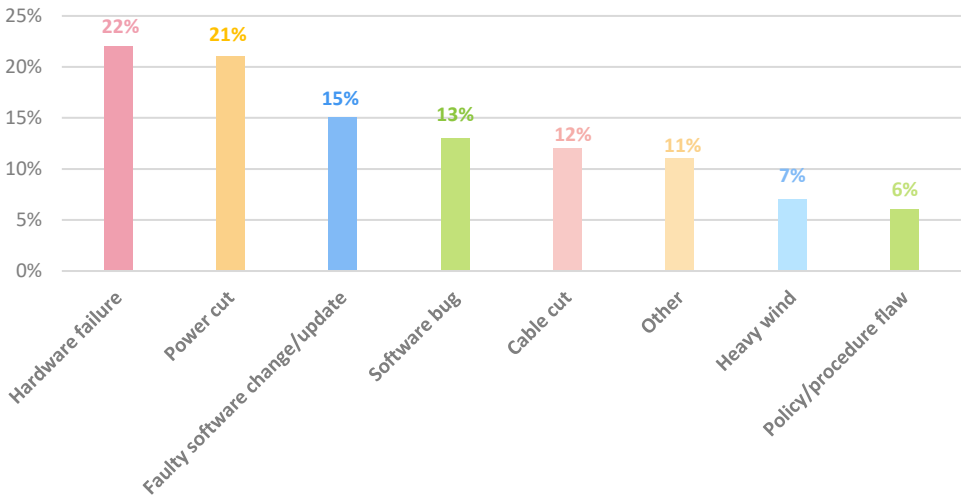
The multi annual trends graph for user hours lost per root cause category (see section 5.3) shows this is the first year that natural phenomena account for more user hours lost than system failures.

3.3 DETAILED CAUSES

An incident is often not only triggered by one cause but can involve multiple detailed causes, a chain of events.For instance, an incident may be triggered by a storm, which tears down power supply infrastructure, power cuts and cable cuts, which in turn leads to a telecom outage. For this example detailed causes could be: Heavy wind, Cable cut, Power cut, Battery depletion. The root cause of the incident would be natural phenomena.

In the following graph we show the frequency of the detailed causes.

Figure 9: Detailed causes - 2019



In 2019, the most common cause of incidents was hardware failures, which confirms the multi-annual trend in which hardware failure is always either the first or the second most common cause. Power cuts became the second most common “detailed cause”. Around a fifth of the incidents reported involved a power cut. Hardware failures, power cuts, faulty software updates and software bugs remain the top four causes, as in the previous years. Some detailed causes mentioned in incidents reports do not fall under a specific category and they are grouped under “Other”.

In the following charts, we look at the frequency of detailed causes under each root cause category.

Figure 10: System failures - detailed causes

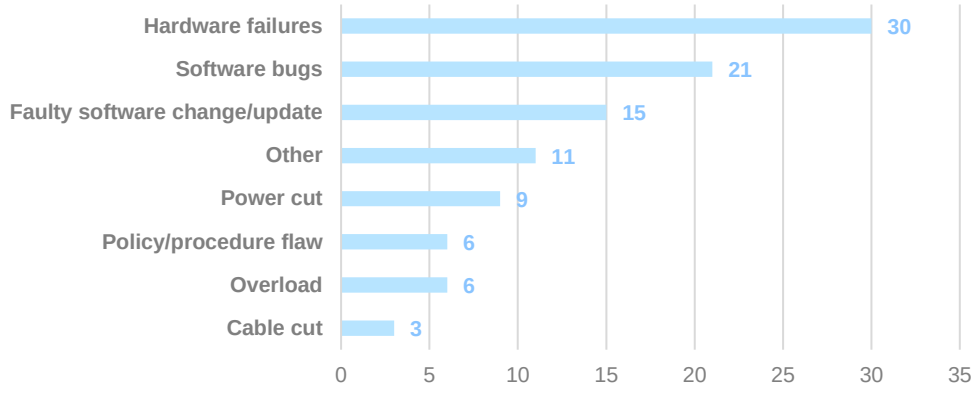


Figure 11: Human errors - detailed causes

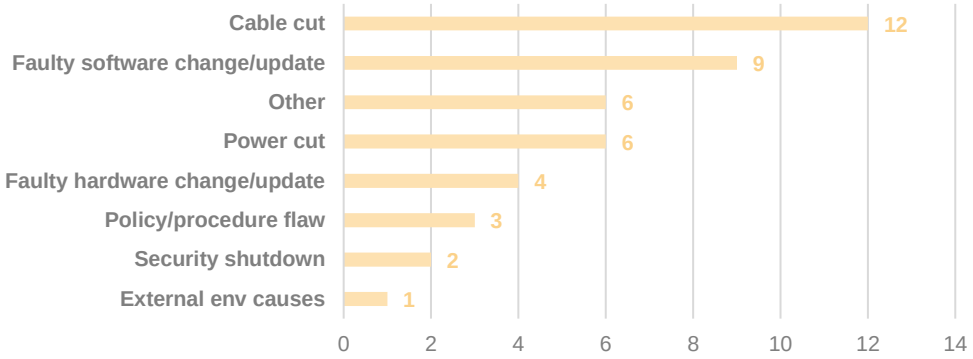


Figure 12: Natural phenomena - detailed causes

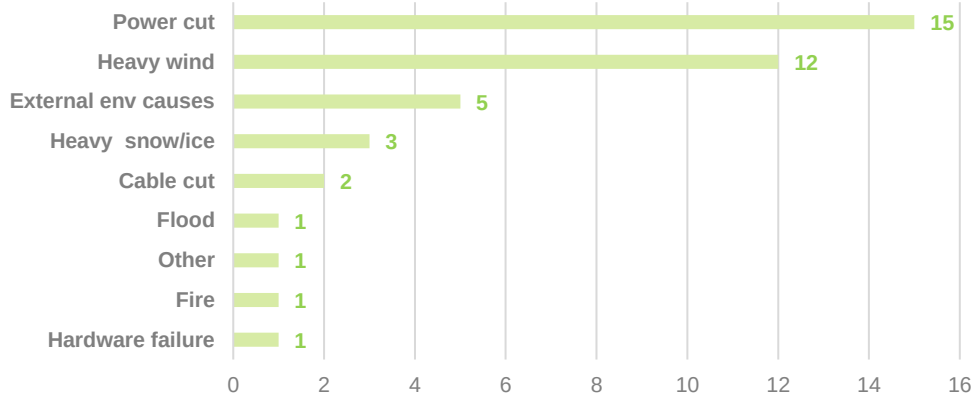
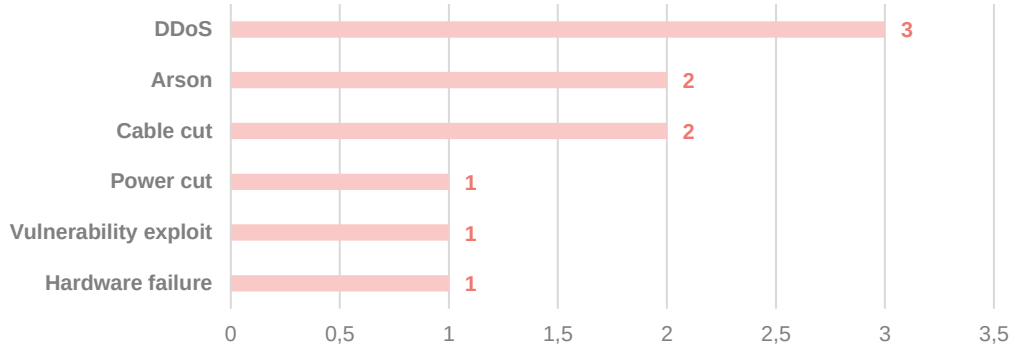


Figure 13: Malicious actions - detailed causes

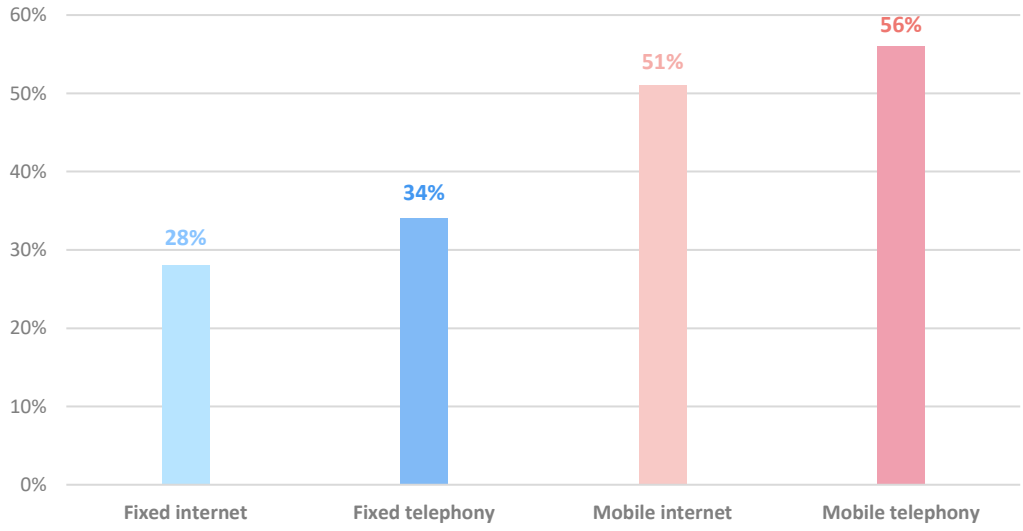


Custom analysis over the full dataset can be done using CIRAS (see par. 2.3). For example, by selecting system failures (top left), then fixed internet and telephony (top right), the charts at the bottom show the detailed causes for the selected subset of incidents.

3.4 SERVICES AFFECTED

In this section we look at the services affected by the incidents. For the fourth year in a row, most of the reported incidents affected mobile services. In 2019, almost the half of the incidents reported had an impact on mobile telephony and internet in the EU. This confirms the shift over the last years. Fixed telephony was the most affected service only in the early years of reporting.

Figure 14: Services affected



Note that for most reported incidents there is impact on more than one service, which explains why the percentages in the chart here add up to more than 100%.

In the following pie charts the affected services are presented in relation to the four root causes.

Figure 15: Mobile telephony vs root causes

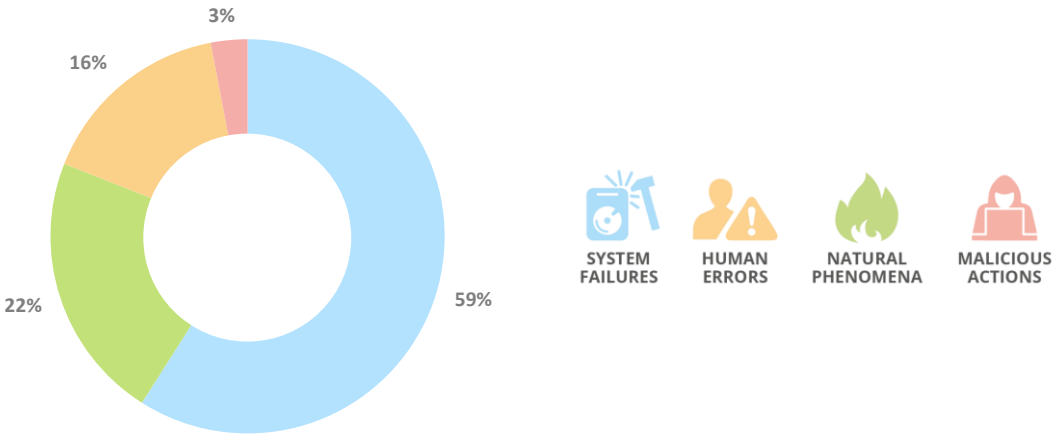
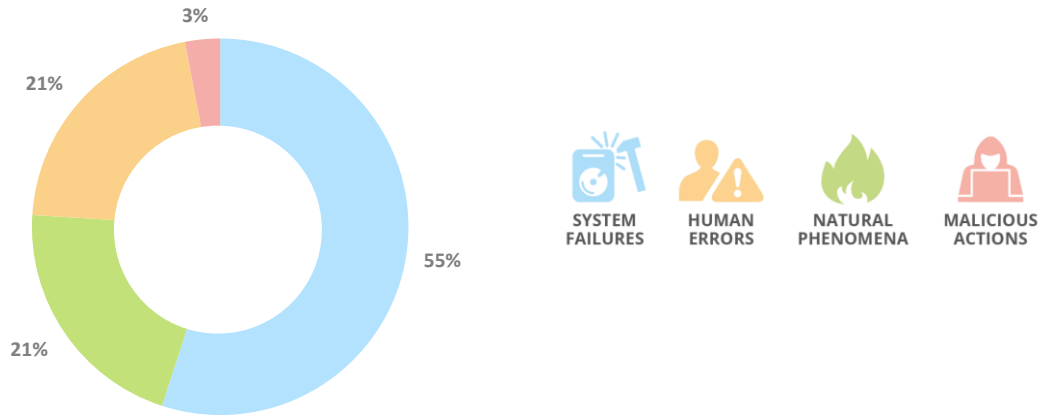
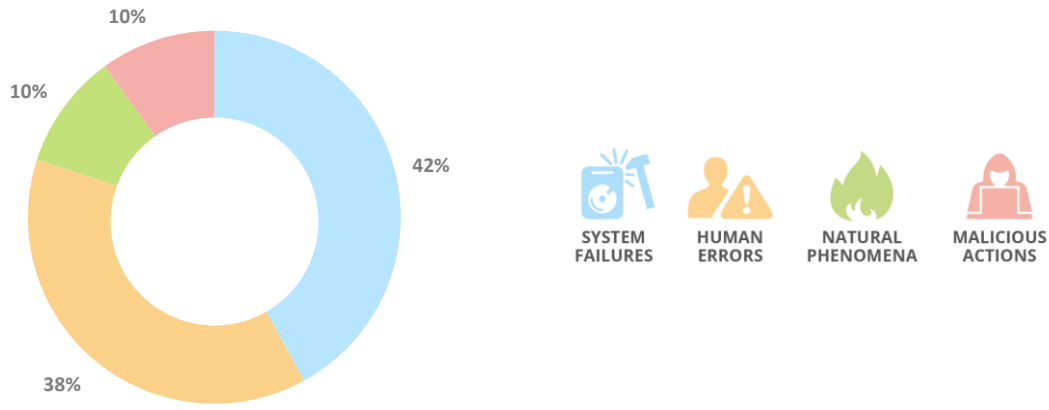


Figure 16: Mobile internet vs root causes



Having a closer look at the charts, we can conclude that system failures are the dominant root cause for mobile telephony and internet, whereas in fixed internet, human errors are the most common root cause.

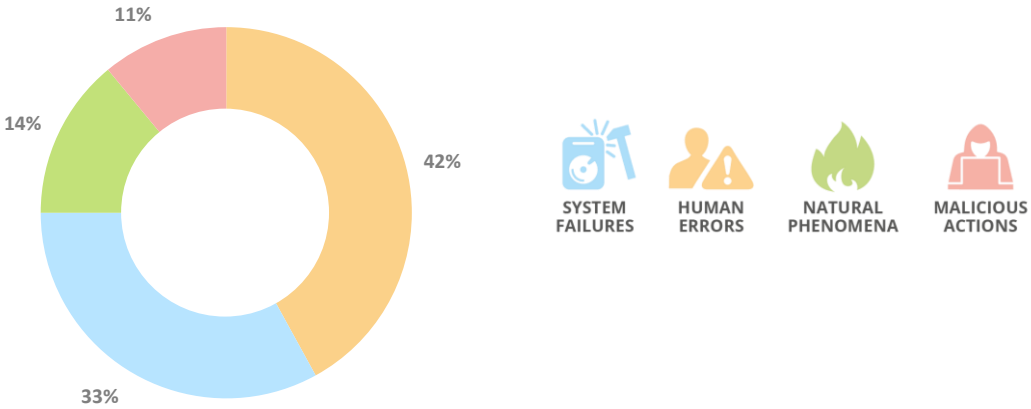
Figure 17: Fixed telephony vs root causes



In general, fixed telephony and internet seem to be severely affected by human errors even more than natural phenomena. Natural phenomena are responsible for 1 out of 10 incidents in fixed telephony and for the 14% of incidents in fixed internet.

Finally, malicious actions are responsible for 10% and 14% of incidents in fixed telephony and internet respectively, however in mobile telephony and internet this percentage is much lower (3% for mobile telephony and the same for mobile internet).

Figure 18: Fixed internet vs root causes



4. DETAILED ANALYSIS – HUMAN ERRORS

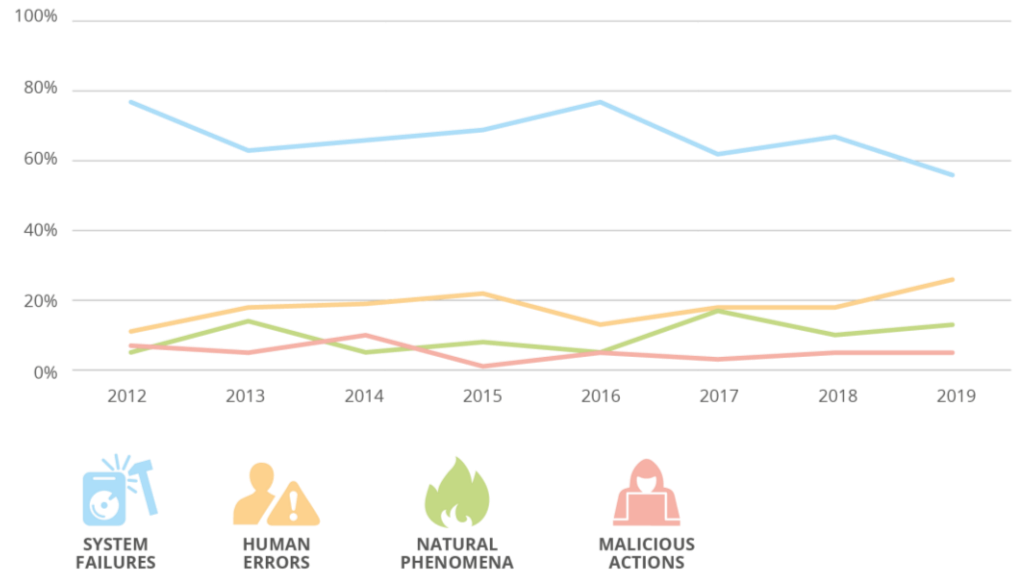
In 2019, the number of incidents caused by human errors has risen up to 50% compared to the previous year. More than one fourth of the security incidents were caused by human errors and these incidents account for one fifth of the total user hours lost (21%, 208 million user hours). Considering the above remarks, in this section we perform a deep dive in human errors.

Looking carefully at the multiannual graph above, though it is not the first time since 2012 that human errors are responsible for almost 20% of the incidents, it seems that they are trending up since 2016.

50%

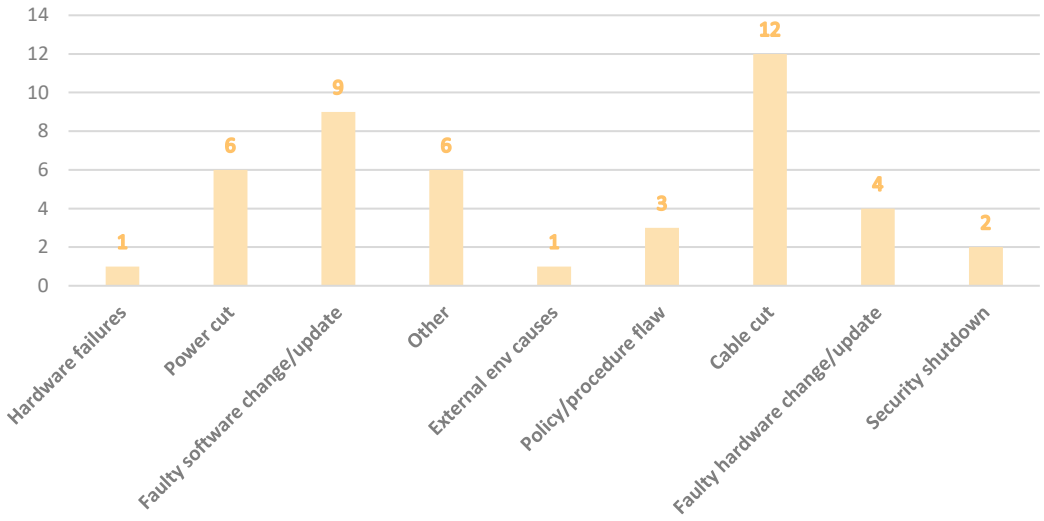
of the incidents were caused by human error, accounting for 208 million user hour lost, 21% of the total.

Figure 19: Root cause categories Telecom security incidents in the EU - reported over 2012-2019



For all incidents having as a root cause human errors, we can see the detailed causes in the graph below. Most incidents caused by human errors are about cable cuts and the second more frequent detailed cause is faulty software change or update.

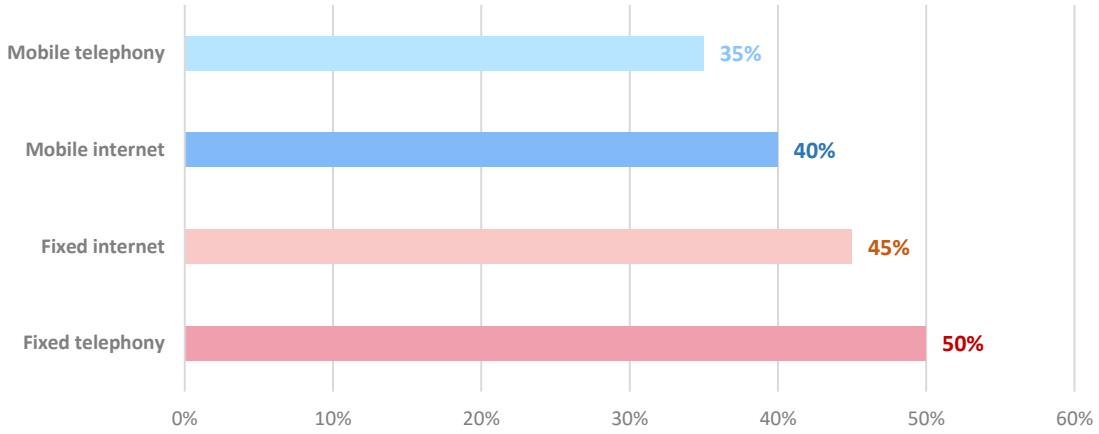
Figure 20: Human errors - detailed cause



In 2019, the increased number of incidents caused by human errors (raising from 18% in 2018 to 26% in 2019) is due to third-party failures, taking into account that third-party failures accounted in 2019 for 12% of incidents that had human errors as the root cause, whereas in 2018 this percentage was 3%.

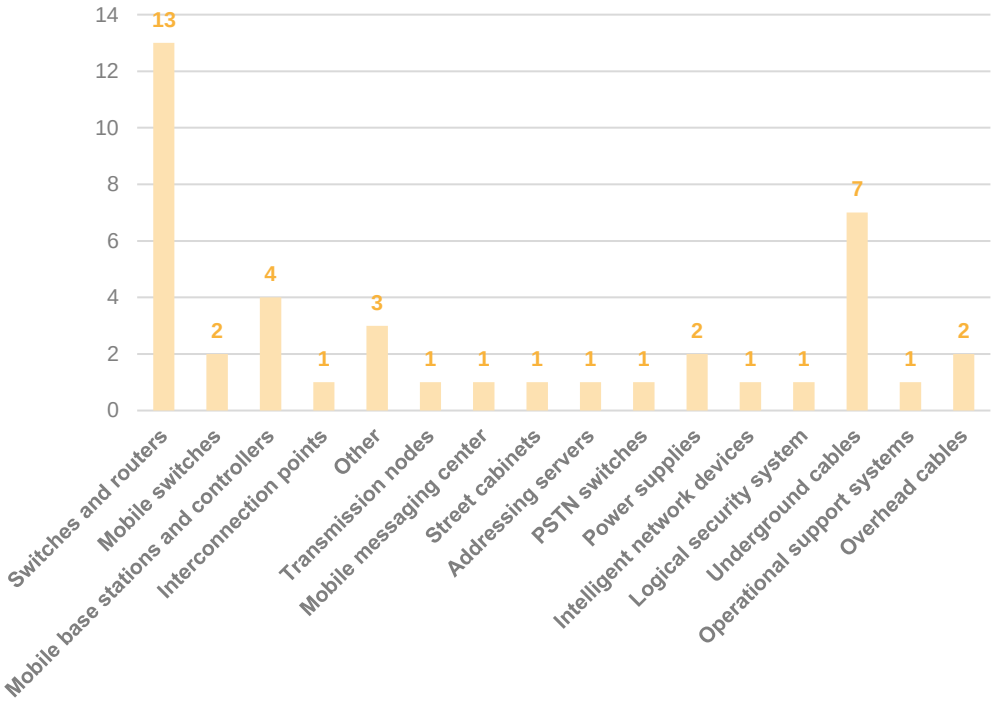
Also, as far as human errors are concerned, fixed telephony and internet are the most affected services, which doesn't follow the general conclusion that mobile internet and telephony are mostly affected by security incidents during the last years.

Figure 21: Services affected by human errors



As for the affected assets, the graph below indicates that human errors have a major impact on switches and routers in fixed telephony and internet.

Figure 22: Assets affected by Human Errors



5. MULTI-ANNUAL TRENDS

ENISA has been collecting and aggregating incident reports since 2012. In this section, we look at the multiannual trends over the last 8 years, covering from 2012 to 2019. This dataset contains 1093 reported incidents in total.

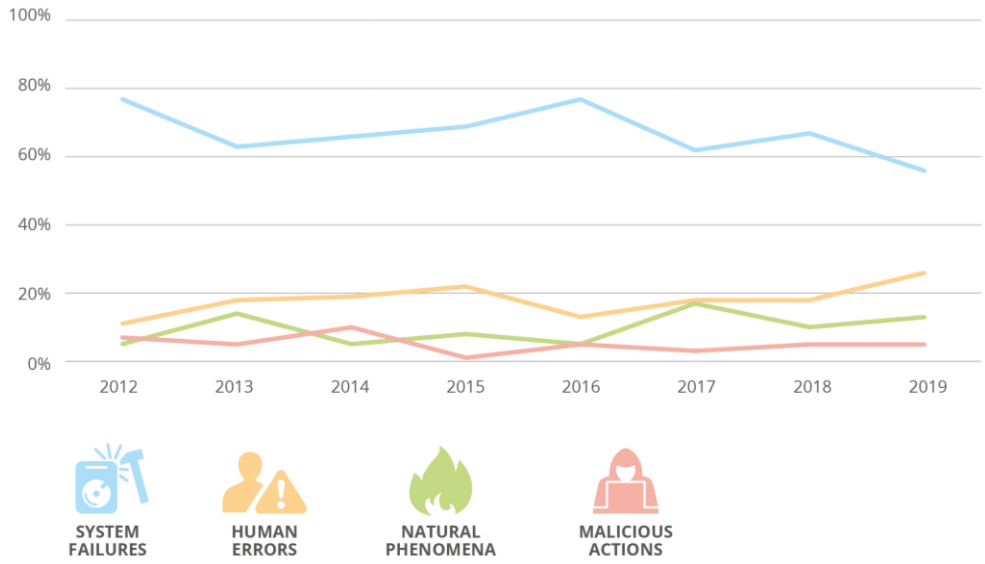
1093

Incidents were reported over 8 years of reporting, 2012-2019.

5.1 MULTIANNUAL TRENDS - ROOT CAUSE CATEGORIES

Every year from 2012 to 2019, system failures are the most common root cause. In 2019, however, system failures show a considerable decrease. In fact, in 2019 the number of incidents due to system failures is the lowest since 2012. In total system failures account for 722 of incident reports (66% of the total). For this root cause category, over the last 8 years, the most common causes were hardware failures (36%) and software bugs (28%). The second most common root cause over the 8 years of reporting is human errors with nearly a fifth of total incidents (19%, 202 incidents in total). Natural phenomena come third at almost a tenth of total incidents (9%, 109 incidents in total). Only 5% of the incidents are categorized as malicious actions. In the period 2012-2019 nearly two thirds of the malicious actions consist of Denial of Service attacks, and the rest resulted mainly in lasting damage to physical infrastructure.

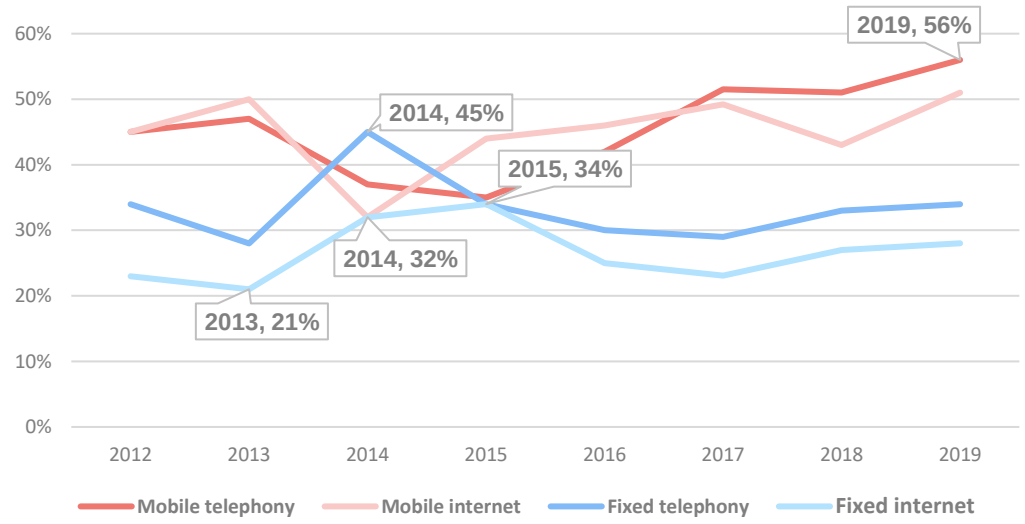
Figure 23: Root cause categories Telecom security incidents in the EU - reported over 2012-2019



5.2 MULTIANNUAL TRENDS - IMPACT PER SERVICE

In 2019 mobile networks and services were the most impacted by incidents. This is part of a multiannual trend. Only in 2014 the fixed networks and services was where the most affected. Looking back at the 8 years of annual incident reporting, a total of 1093 incidents, almost half had an impact on mobile internet or mobile telephony. The chart below shows the multiannual trends over the 2012-2019 period. It indicates the share of the total incidents for each year that involved one of the four classic telecommunication services. For instance, in 2019 56% of the incidents had to do with mobile telephony.

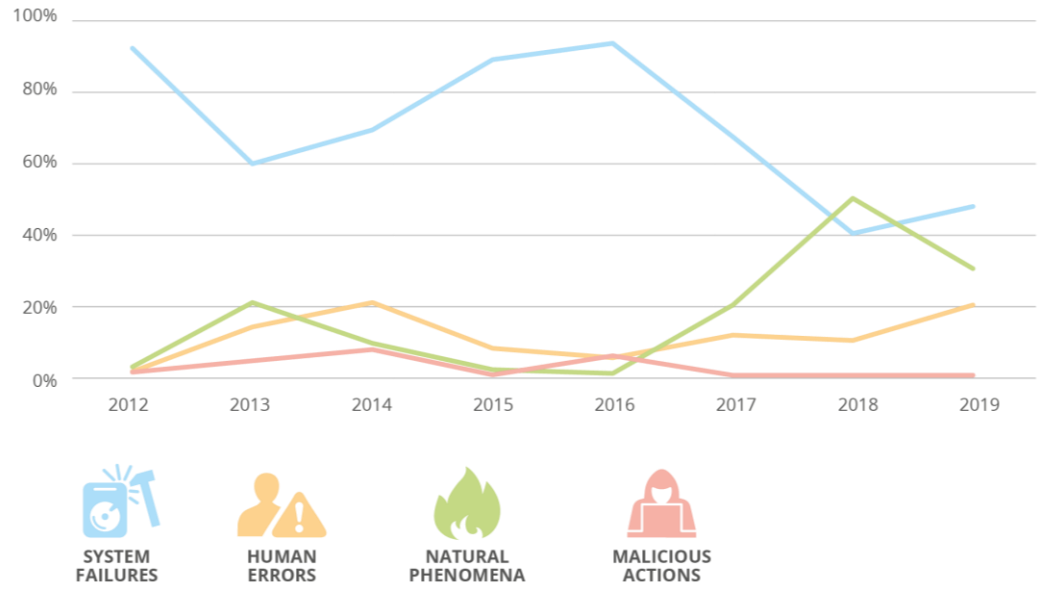
Figure 24: Trend on classic services affected per year



5.3 MULTIANNUAL TRENDS - USER HOURS PER ROOT CAUSE

Adding up the total user hours lost per root cause category, we observe that human errors have been increasing since 2016. In 2019, although system failure is the dominant root cause category, human errors show a raise of almost 50% compared to the previous year. Between 2018 and 2019 we observe a slight increase in lost user hours due to system failures, and a corresponding decrease to hours lost due to natural phenomena. Malicious actions are stable over the years.

Figure 25: User hours lost per root cause category - multiannual 2012-2019 (percentage of total user hours lost)

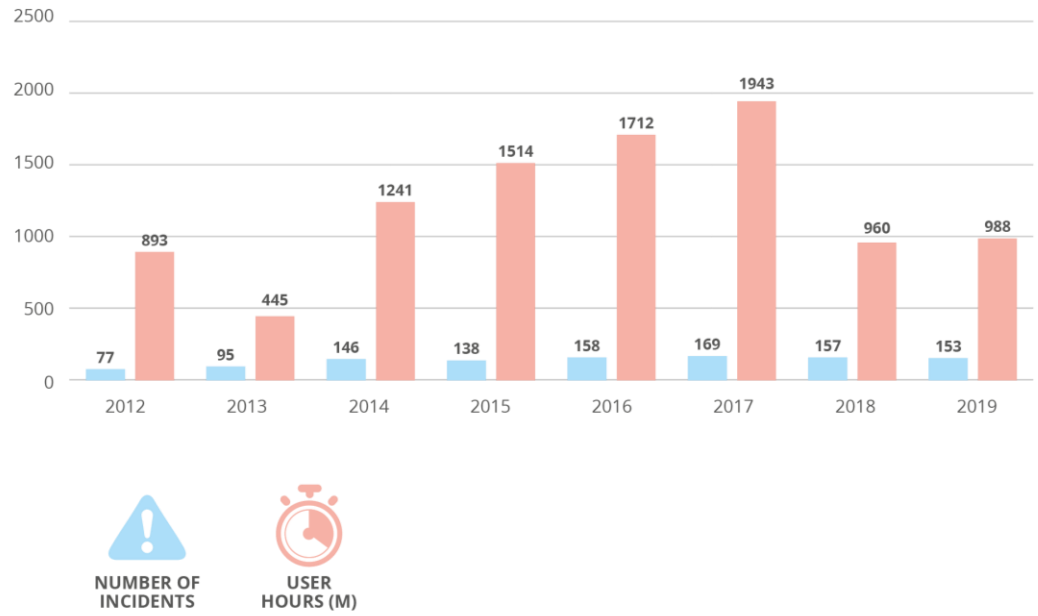


5.4 MULTIANNUAL TRENDS - NUMBER OF INCIDENTS AND USER HOURS

Over the years, the number of incidents included in annual summary reporting to ENISA has increased slowly and it seems to stabilize at around 160 per year. This is probably due to more reporting by providers, better awareness about the reporting obligations, and partly due to lower national thresholds for annual summary reporting.

In the chart below we also show total numbers of incidents reported and total user hours lost per year over the period 2012-2019. There was an upward trend in user hours lost reaching a peak in 2017 with 1942 million user hours lost. Interestingly there was a sharp drop in the average user hours lost per incident reported over 2018 and they remain at the same level in 2019. This could lead to the conclusion that 2018 was a start of a longer trend.

Figure 26: Number of incidents and million user hours lost per year



6. CONCLUSIONS

This document, the Annual Report Telecom Security Incidents 2019, covers the incidents reported by the authorities for the calendar year 2019 and it gives an anonymised, aggregated EU-wide overview of telecom security incidents. It marks the 9th time ENISA publishes an annual report for the telecom sector.

We would like to conclude highlighting the most important findings and including some more general observations about this process and the broader policy context.

6.1 KEY TAKEAWAYS

The key takeaways from the 2019 incidents are:

- **Annual number of incidents seems to be stabilizing at around 160:** this shows that the process of incident reporting has matured among operators and national authorities so that worth-mentioning incidents get the attention they deserve. This is probably due to more reporting by providers, better awareness about the reporting obligations, and partly due to lower national thresholds for annual summary reporting.

- **The sharp decline in total number of user hours lost:** between 2017 and 2018, was not an exception. Also in 2019, the number of user hours lost remained low.

- **Looking into the system failures, hardware failures are a major factor in 2019:** almost a quarter of incidents (23%) were caused by hardware failures and they also had a major impact in terms of user hours with 38% of the total. Also, software bugs are still a concern, since they are responsible for 15% of the incidents.

- **Frequency of human errors is trending up:** In 2019, this raise is mostly due to third-party failures, often during construction works that led to cable/optic fiber cuts or because of faulty software updates, performed by subcontractors.

- **Natural phenomena are trending up:** due to severe weather conditions and climate change.

- **One incident involving a fire had a major impact:** It can be difficult to recover from a fire and it often takes hours or days before the operator can even start repairs. Fire protection as well as redundancy are important to consider.

6.2 OBSERVATIONS

By the end of 2020, the European Electronic Communications Code (EECC) will come into effect across the EU. Under Article 40 of the EECC the incident reporting requirements have a broader scope, including not only outages, but also breaches of confidentiality. Also, there are more services in scope of the EECC, including not only traditional telecom operators, but also for example over-the-top providers of communications services.

In 2020, the annual reporting guideline will be updated to include new thresholds for annual summary reporting to ENISA combining quantitative and qualitative parameters. Furthermore, the notification of security incidents affecting not only the services of fixed and mobile internet and telephony, but also the number-based interpersonal communications services and/or number independent interpersonal communications services (OTT communications services).

TP-AD-20-001-EN-N

ABOUT ENISA

The mission of the European Union Agency for Cybersecurity (ENISA) is to achieve a high common level of cybersecurity across the Union, by actively supporting Member States, Union institutions, bodies, offices and agencies in improving cybersecurity. We contribute to policy development and implementation, support capacity building and preparedness, facilitate operational cooperation at Union level, enhance the trustworthiness of ICT products, services and processes by rolling out cybersecurity certification schemes, enable knowledge sharing, research, innovation and awareness building, whilst developing cross-border communities. Our goal is to strengthen trust in the connected economy, boost resilience of the Union's infrastructure and services and keep our society cyber secure. More information about ENISA and its work can be found www.enisa.europa.eu.

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 Vasilissis Sofias Str
151 24 Marousi, Attiki, Greece

enisa.europa.eu

ISBN: 978-92-9204-350-6
DOI: 10.2824/491113