enisa 20 years!

EUROPEAN UNION AGENCY
FOR CYBERSECURITY

TELECOM SECURITY INCIDENTS 2022

ANNUAL REPORT

ABOUT ENISA

The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union's infrastructure, and, ultimately, to keep Europe's society and citizens digitally secure. More information about ENISA and its work can be found here: www.enisa.europa.eu.

CONTACT

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

Author

Marie-Laure LULE, European Union Agency for Cybersecurity

Acknowledgements

We are grateful for the review and input received from the members of the ENISA ECASEC expert group, which comprises national telecom regulatory authorities (NRAs) from the EU and European Economic Area, European Free Trade Association and EU candidate countries.

Legal notice

Copyright notice

ISBN: 978-92-9204-668-2 DOI: 10.2824/902186

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The present report provides anonymised and aggregated information about major telecom security incidents that happened in 2022. Security incident reporting is a hallmark of EU cybersecurity legislation. It is an important enabler of cybersecurity supervision and a support tool for policymaking at the national and EU levels.

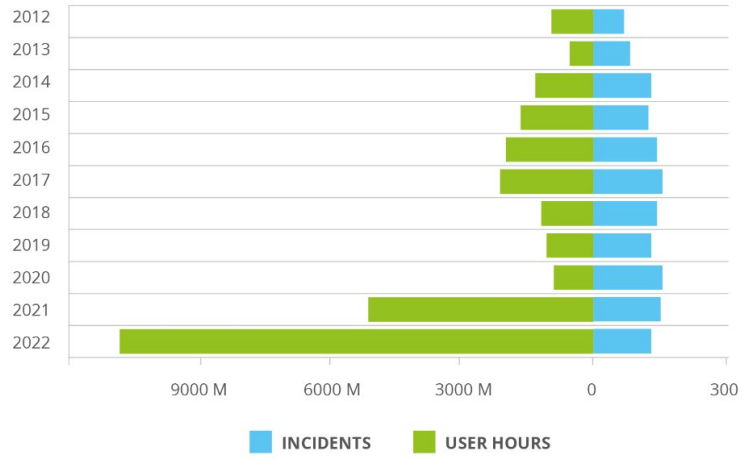
In the European Union, telecom operators notify significant security incidents to their national authorities. At the start of every calendar year, the national authorities send a summary of these reports to ENISA. The European Electronic Communications Code (EECC 2018/1972) reinforces the provisions ([1]) for reporting incidents, clarifying what incidents fall within its scope ([2]), as well as the technical guidelines ([3]) and the notification criteria. ENISA offers an online visual tool for analysing incidents, which can be used to generate custom graphs, available on https://ciras.enisa.europa.eu.

Key findings in 2022 summary report

The 2022 annual summary contains reports of **155 incidents** submitted by national authorities from 26 EU Member States and two European Free Trade Association countries.

In 2022, **11 209 million user hours** ([4]) were lost in total, compared to 5 106 million in 2021. This is clearly a much higher number compared to previous years, as we can see in Figure 1. The reason for this is the important increase of incident reports related to Over-The-Top (OTT) services, a recent metric taken on board in the cybersecurity incident-reporting and analysis system since 2021.

Figure 1: Number of incidents submitted by countries and user hours lost each year (2012–2022)



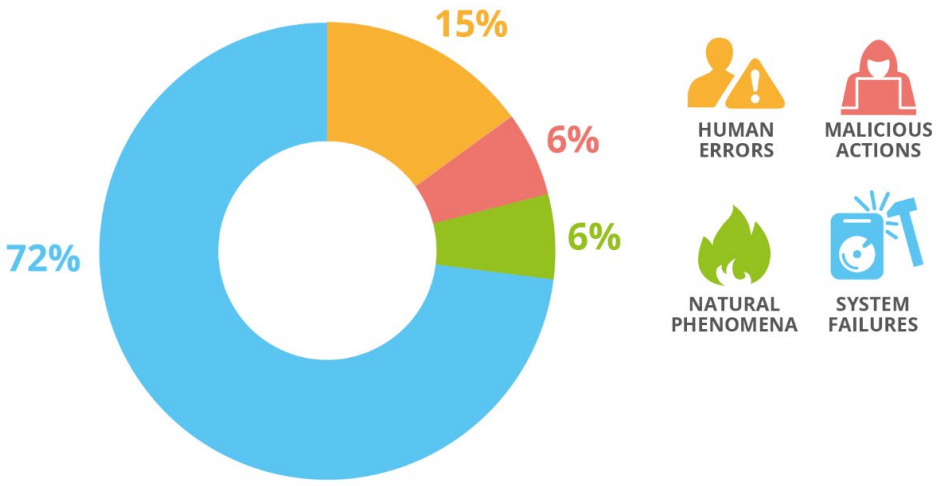
([1]) The reporting of security incidents has been part of the EU's regulatory framework for telecoms since the 2009 reform of the telecoms package, in line with Article 13a of the framework directive (2009/140/EC) that came into force in 2011.
([2]) It is worth noting that since 2016 security incident reporting is also mandatory for trust service providers in the EU under Article 19 of the eiDAS regulation. In 2018, under the NIS directive, 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.
([3]) ENISA technical guidelines on incident reporting under the EECC, including on thresholds and calculation of hours lost.
([4]) Derived by multiplying for each incident the number of users by the number of hours.

Key takeaways from incidents in 2022

Incident reporting confirms the following.

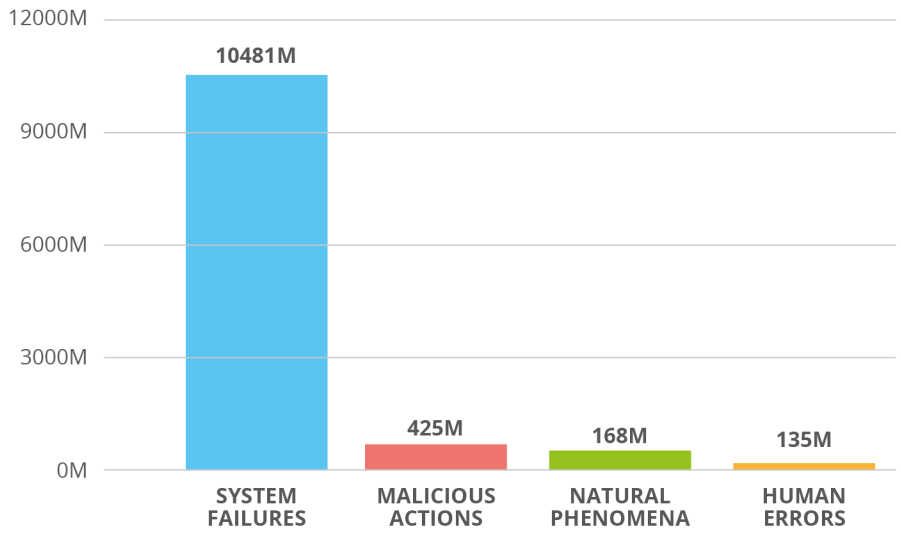
- **Mobile telephony and mobile internet** were the most impacted sectors, with respectively 52 % and 40 % of incidents.
- **Over-The-Top services (OTT)** accounted for 26 % of incidents.
- Traditional **fixed telephony, fixed internet and broadcasting services** continued to drop in terms of incident reports.
- **System failures** continued to largely dominate in terms of impact, reaching 72 % in 2022. They globally accounted for 10 481 million user hours lost (against 10 025 million for OTT) compared to 363 million user hours in 2021 and 419 million in 2020. In 2022, 36 incidents (23 % of total system failures) were marked as hardware failures. They resulted in 797 million user hours lost compared to 53 million in 2021. All of them were reported as system failures.
- **Human error** incidents have steadily decreased since 2020, from 26 % in 2020 to 23 % 2021 and 15 % in 2022. Human error accounted for 135 million user hours lost in 2022.
- **Malicious actions** accounted for 435 million of user hours lost in 2022, 6 % of that year's total incidents, compared to 70 million (8% of that year's total) in 2021 and 13 million (4% of that year's total) in 2020.
- Five **distributed denial-of-service** incidents were reported, resulting in 1 million user hours lost.
- The share of incidents due to **natural phenomena** remained stable, at 6 %. However, the number of user hours lost increased.
- Incidents flagged as **failures by third parties** represented 23 % of incidents, with a total of 35 incident reports, compared to 22 % in 2021, 29 % in 2020 and 32 % in 2019. Four of them originated from human errors, three from malicious actions and one from natural phenomena.
- Five incidents concerning confidentiality and authenticity ([5]) were reported, compared to three in 2021.
- One incident concerning impact on redundancy was reported for the first time.
- One incident concerning a near-miss incident was reported for the first time.

Figure 2: Root cause category (2022)



([5]) The reporting of type B incidents was a new provision of the EECC in 2021.

Share of user hours lost for each root cause category, 2022

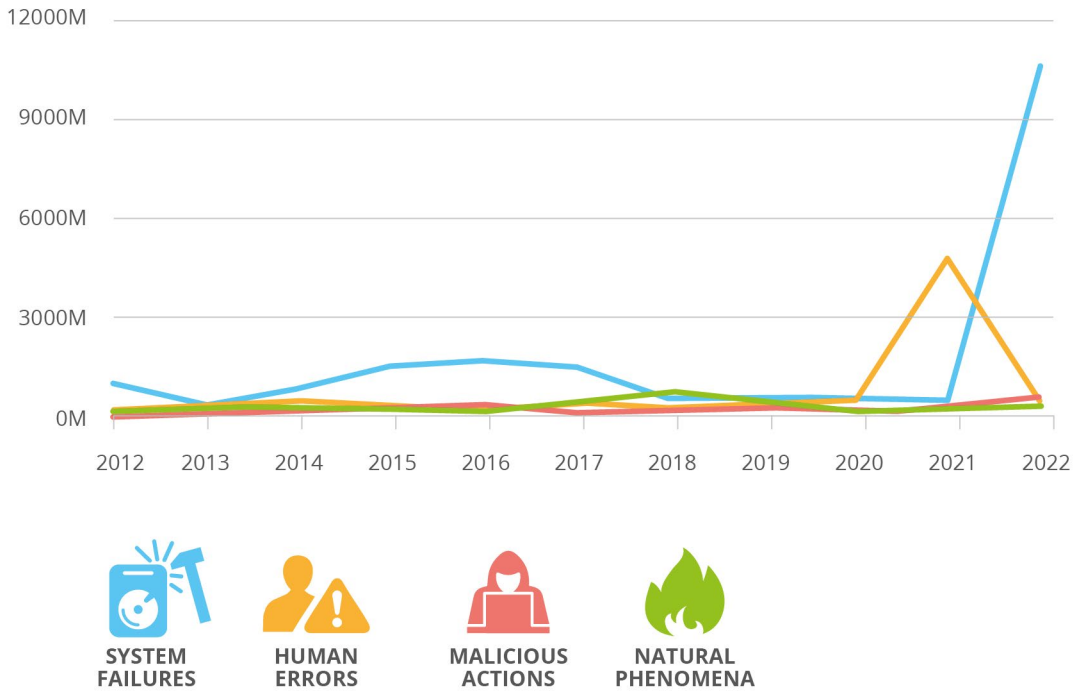


Multiannual trends over the period 2012–2022

Over the years, EU Member States reported **1 586** telecom security incidents, stored in the ENISA cybersecurity incident reporting and analysis system **(CIRAS)**; the statistics ([6]) are accessible online.

([6]) Note that conclusions about trends and comparisons with previous years have to be made with caution, as national reporting thresholds change over the years. Indeed, reporting thresholds have been lowered in most countries in recent years, and reporting only covers the most significant incidents (not smaller incidents that may well be more frequent).

Figure 3: Root cause categories for telecom security incidents in the EU reported over the 2012–2022 period



Over the years, the European Commission has extensively supervised Member States' reporting of incidents with determined outages. Comparing incident reporting results over the years, it is fair to conclude that the European telecommunication networks have shown robustness and resilience.

The following trends, in particular, have emerged.

- **The number of incidents is stabilising**, between 150 and 170 annually over the 2017–2022 period.
- **Human errors continue to decrease** in terms user hours lost.
- **Malicious actions continue to constitute a minority of incidents:** over the reporting period, the frequency of malicious actions was stable, accounting for approximately 5 % of incidents per year on average.

National authorities for telecom security continue to focus on the transposition and the implementation of the EECC, which brings the following changes.

- The incident-reporting requirements in Article 40 of the EECC have a broader scope, explicitly including, for example, breaches of confidentiality.
- In addition, the arrival of the network and information security directive (NIS2) in 2022 has consolidated the reporting of breaches of integrity, availability… across multiple sectors including – but not limited to the EECC – as of 17.10.2024.

ENISA will continue to work with national authorities through the European competent authorities for secure electronic communications ([7]) working group and the NIS Cooperation

([7]) Also called 'ECASEC'.
https://resilience.enisa.europa.eu/article-13
https://www.enisa.europa.eu/topics/critical-information-infrastructures-and-services/telecoms

group to find and exploit synergies between various pieces of EU legislation, particularly when it comes to incident reporting and cross-border

1. INTRODUCTION

Electronic communication providers in the EU have to report security incidents that have a significant ([8]) impact on the continuity of electronic communication services to the national telecom regulatory authorities (NRAs) in each EU Member State. Every year the NRAs provide ENISA with a summary of the most significant incidents based on a set of agreed EU-wide thresholds. This document, *Telecom Security Incidents Report 2022*, aggregates the 155 incident reports received in 2022 and provides an overview of telecom security incidents in the EU.

The European Electronic Communications Code ([9]) (EECC), includes a broader scope on the requirements for incident reporting in Article 40 and requires mandatory incident reporting with a specific focus on security incidents with a significant impact on the functioning of each category of telecommunication services.

Over the years, the regulatory authorities (Art. 41 EECC) have agreed to focus on network/service outages. This year, ENISA also received five reports of incidents related to breaches of confidentiality, one incident report received concerning the impact on redundancy and one incident report concerning a near-miss incident.

In 2022 ([10]), a total of 155 incidents were reported.

This document is structured as follows:

- in Section 2, the policy context and background are provided;
- in Section 3, key facts and statistics about incidents in 2022 are provided;
- in Section 4, we take a closer look at faulty software changes; and
- in Section 5, a summary of multiannual trends over the 2012–2022 decade is provided.

This is the annual ENISA report on Incident Reporting for the telecom sector.

Mandatory incident reporting has been a part of the EU's telecom regulatory framework since 2009.

Article 40 of the European Electronic Communications Code is the legal basis for this document.

([8]) Note that the telecom security incidents that are reported to national authorities are only the major incidents, i.e. those with significant impacts. Smaller incidents, affecting small percentages of population, such as SIM-swapping attacks or fraud are not reported, since they do not cause outages.
([9]) https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX %3A32018L1972
([10]) In 2021, 165 incidents were reported, among them three marked as type B, impacting confidentiality and authenticity of services. Until 2021, incidents of the other four types had not been reported.

2. BACKGROUND AND CONTEXT

In this chapter, the policy context is explained, along with the main features of the incident reporting process, as described in *ENISA Technical Guideline on Incident Reporting* ([11]), which was developed in collaboration with national authorities.

2.1 POLICY CONTEXT

By the end of 2020, the EECC came into effect across the EU. The year 2022 saw progress in its implementation ([12]) by Member States.

Under Article 40 of the EECC the incident-reporting requirements have a broad scope, including not only outages but also breaches of confidentiality. In addition, there are more services included: not only traditional telecom operators, but also over-the-top OTT providers of communications services ([13]), for example messaging services like Viber and WhatsApp and number-based interpersonal communications services and/or number-independent interpersonal communications services ([14]).

The years 2020 and 2021 were characterised by the COVID-19 pandemic, which radically transformed the way people around the world live and work, driving towards more digitization. The year 2022 was then shaken by the Russian war of aggression against Ukraine and the numerous disruptions in telecommunications network and services like.

2.2 INCIDENT REPORTING FRAMEWORK

There are three types of incident reporting:

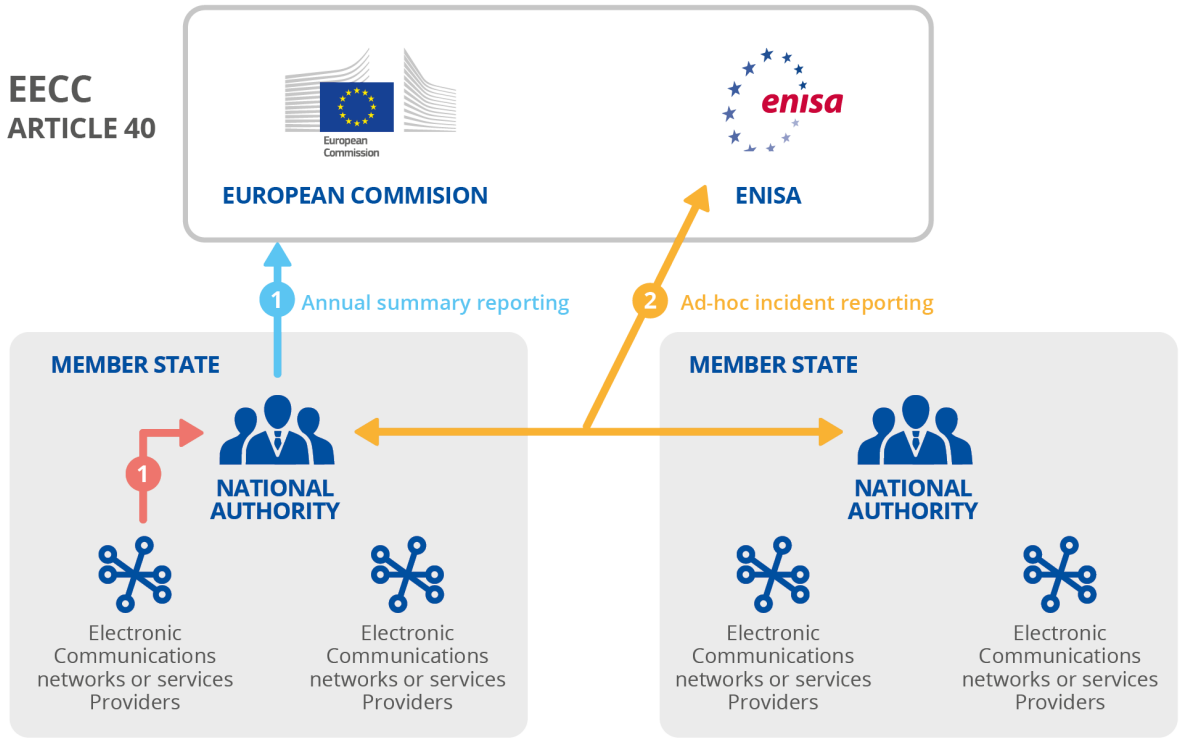
- national incident reporting from providers to NRAs;
- ad hoc incident reporting between NRAs and ENISA; and
- annual summary reporting from national authorities to the European Commission and ENISA.

It bears noting that in this setup ENISA acts as a collection point, anonymising, aggregating and analysing the incident reports. In the current setup, NRAs can search for 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 to telecommunications providers.

The different types of reporting are shown in **Figure 4.**

([11]) See https://resilience.enisa.europa.eu/article-13/guideline-for-incident-reporting.
([12]) See https://digital-strategy.ec.europa.eu/en/policies/eu-electronic-communications-code.
([13]) See Security supervision changes in the new EU telecoms legislation – ENISA (europa.eu).
([14]) See When & How to Report Security Incidents – ENISA (europa.eu).

Figure 4: Incident reporting under Article 40 of the EECC



2.3 INCIDENT REPORTING TOOL

ENISA maintains an incident reporting tool, **CIRAS**, for the authorities to upload reports and search for and study specific incidents.

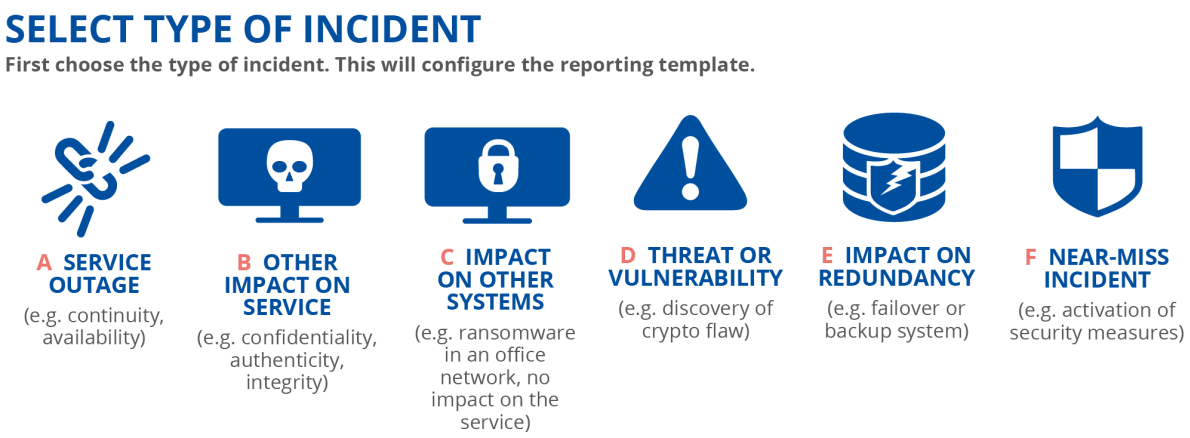
For the general public, ENISA also has an online visual tool, which is publicly accessible and can be used for custom analysis of data. This tool anonymises the country or operator involved. Link: https://ciras.enisa.europa.eu/

The reporting template starts with the type of incident (choice between six types of cybersecurity incidents, explained in **Figure 5**). The field contains three parts:

- **impact of the incident:** communication services impacted and by how much;
- **nature of the incident**: the cause of the incident;
- **details of the incident:** detailed information about the incident, including a short description, the types of network, the types of assets, the severity level, etc.

CIRAS
is a free online tool where ENISA stores reported incidents and provides annual and multiannual statistics.

Figure 5: Types of cybersecurity incidents



- **Type A.** Service outage (e.g. continuity, availability).
  For example, an outage caused by a cable cut due to a mistake by the operator of an excavation machine used for building a new road would be categorised as a type A incident.
- **Type B.** Other impact on service (e.g. confidentiality, authenticity, integrity).
  For example, a popular collaboration tool has not encrypted the content of the media channels, which are being established when a session is started, between the endpoints participating in the shared session. This leads to the interception of the media (voice, pictures, video, files, etc.) through a man-in-the-middle attack. This incident would be categorised as a type B incident.
- **Type C**. Impact on other systems (e.g. ransomware in an office network, no impact on the service).
  For example, a malware being detected on several workstations and servers of the office network of a telecom provider would be categorised as a type C incident.
- **Type D**. Threat or vulnerability (e.g. discovery of crypto flaw).
  For instance, the discovery of a cryptographic weakness would be categorised as a type D incident.
- **Type E.** Impact on redundancy (e.g. failover or backup system).
  For example, one of two redundant submarine cables breaking would be categorised as a type E incident.
- **Type F**. Near-miss incident (e.g. activation of security measures).
  For instance, a malicious attempt that ends up in the honeypot network of a telecom provider would be categorised as a type F incident.

For more information about the incident reporting process, please refer to:
Technical Guideline on Incident Reporting under the EECC ([15])

([15]) See https://www.enisa.europa.eu/publications/enisa-technical-guideline-on-incident-reporting-under-the-eecc.

3. ANALYSIS OF INCIDENTS

For the year 2022, 26 EU Member States and two European Free Trade Association countries participated in the annual reporting process, reporting 155 significant incidents (compared to 168 in 2021 and 170 in 2020). In this section, the 155 reported incidents are aggregated and analysed.
First, the impact on each root cause category is analysed in Section 3.1.
In Section 3.2, the focus is on the user hours that were lost in each root cause category.
Detailed causes are then examined in Section 3.3, and in Section 3.4 the impact on each service is analysed.
This year, ENISA also received five reports of incidents related to breaches of confidentiality, one incident report concerning the impact on redundancy and one incident report concerning a near-miss incident.

155 telecom security incidents reported in 2022 by EU Member States.

3.1 CATEGORIES OF ROOT CAUSES OF INCIDENTS

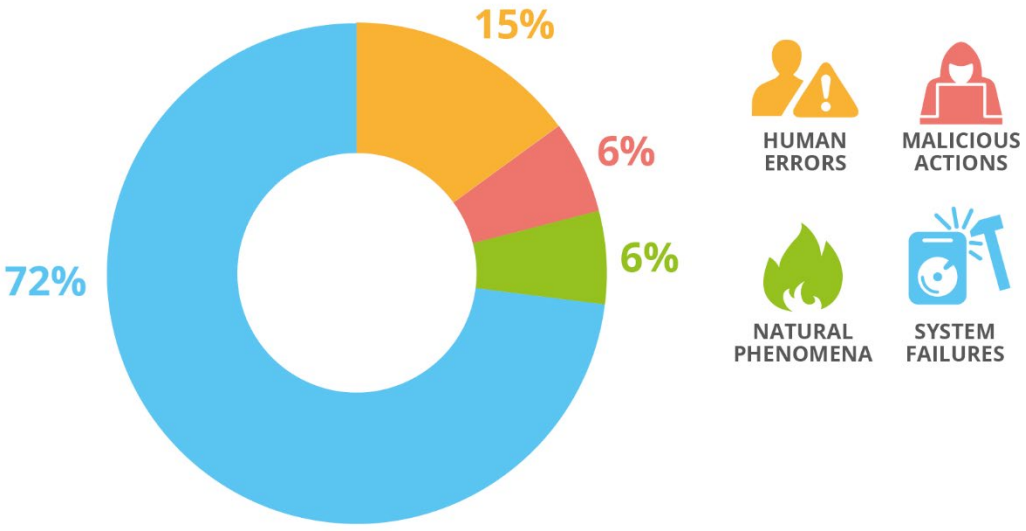
In 2022, there was a rise in incidents related to **system failures**, reaching 72 % despite a slight decrease in the number of incidents. In 2021, 59 % of telecom incidents were marked as system failures, against 61 % in 2020.

Human errors consistently rank second after system failures, with 15 %, when in 2021 it was 23 % (compared to 26 % in 2020).

Malicious actions accounted for 6 % of incidents in 2022, a slight decrease compared to 2021 (8 %), which was double the share of 2020 (4 %).

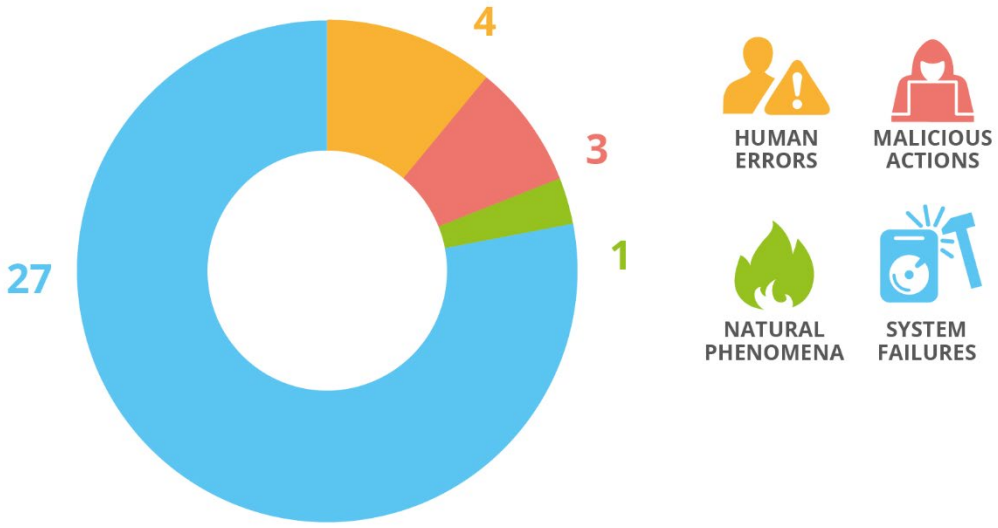
Natural phenomena decreased to 6 % from 10 % in 2021 and from 9 % in 2020.

Figure 6: Root cause categories – Telecom security incidents in 2022



In 2022, incidents flagged as **failures by third parties** represented 23 % of incidents, with a total of 35 incident reports, compared to 22 % in 2021, 29 % in 2020 and 32 % in 2019. Four of them originated from human errors, three from malicious actions and one from natural phenomena, while the majority of them were related to system failures (see **Figure 7**).

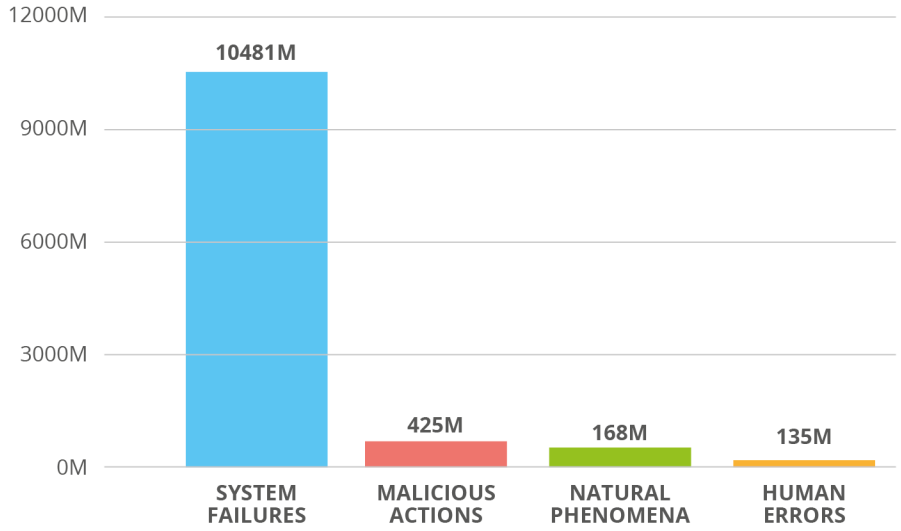
Figure 7: Root cause categories – Telecom security incidents in 2022 (third-party failures)



3.2 USER HOURS LOST IN EACH CATEGORY OF ROOT CAUSES

- **System failures** continue to largely dominate in terms of impact, reaching 72 % of incidents in 2022. They accounted for 10 481 million user hours lost compared to 363 million user hours in 2021 and 419 million in 2020. Among 8 527 million hours out of the 10 481 million were due to faulty software changes/updates. Another 1 048 million hours were due to power cuts.
- **Human error** incidents steadily have decreased since 2020: from 26 % in 2020 to 23 % in 2021 and 15 % in 2022. Human error accounts for 135 million of user hours lost in 2022.
- **Malicious actions** constitute a minority of total user hours lost with a percentage of 6% in 2022. However the number of user hours lost increased drastically, reaching 425 million in 2022 compared to 70 million in 2021.
- User hours lost due to **natural phenomena** reached a record high in 2022, at 168 million, compared to 41 million in 2021 and 58 million in 2019; they accounted for 6 % of the total number of incidents.

Figure 8: Share of user hours lost for each root cause category, 2022

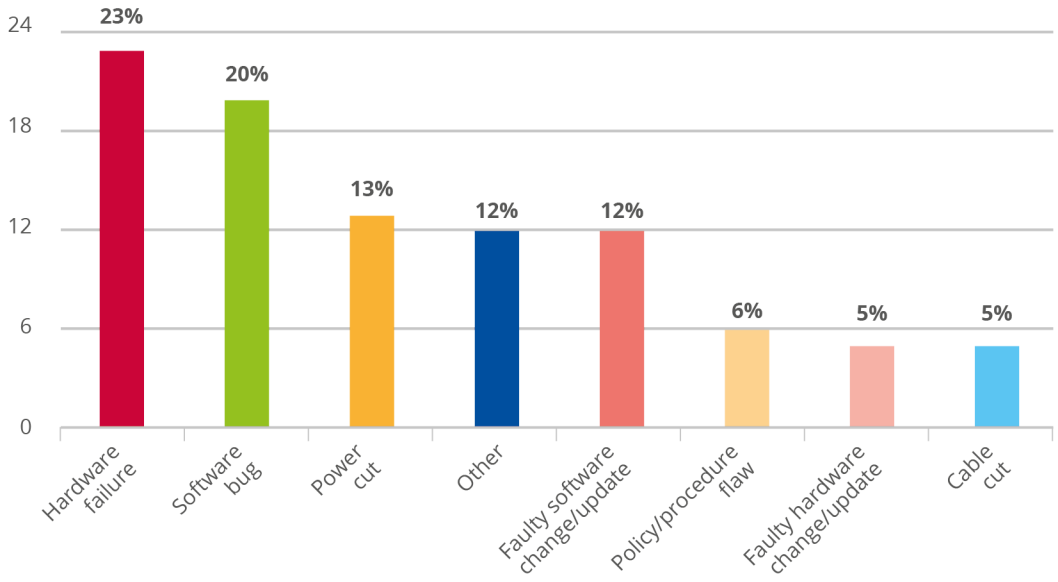


3.3 DETAILED ROOT CAUSES AND USER HOURS LOST

Detailed causes for all incidents are tracked, in addition to root cause categories in **Figure 9.** An incident is often a chain of events. For instance, an incident may be triggered by a storm, which tears down power supply infrastructure, cutting cables and thus power, which in turn results in a telecom outage. In this example, the root cause of the incident would be natural phenomenon and the detailed causes would be: heavy wind, cable cut, power cut and battery depletion.

The most frequent detailed cause appearing in incident reports for 2022 is hardware failure followed by software bugs, power cuts and faulty software changes/updates.

Figure 9: Detailed root causes – Telecom security incidents in 2022

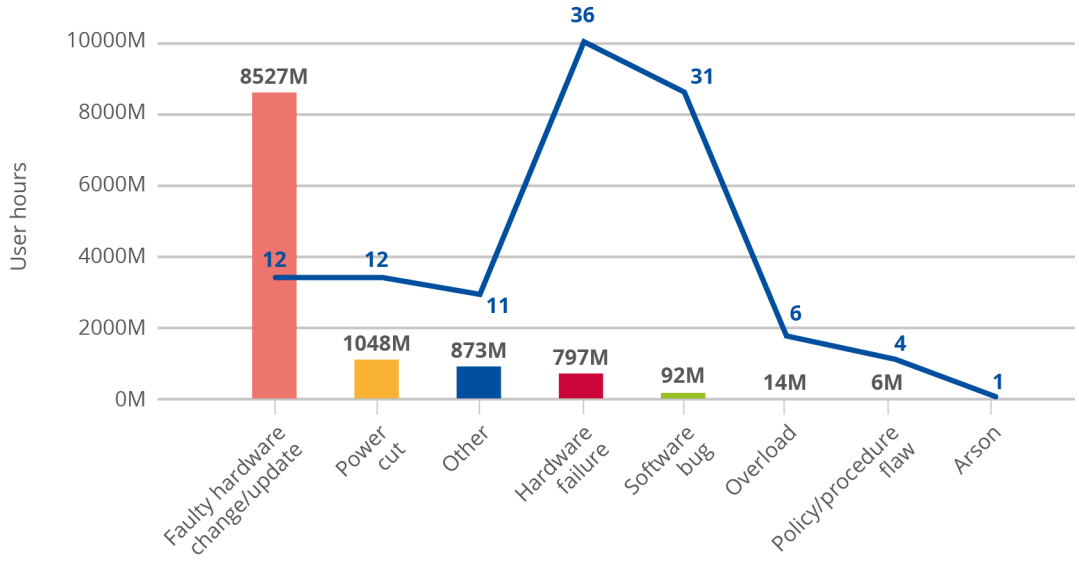


3.3.1 Breakdown of root causes

What follows is an overview of detailed causes and user hours lost for each category of incident in an effort to provide clarity and transparency for specific root causes, which differ significantly between categories of incidents.

Figure 10 shows the frequency of detailed causes across incident reports for 2022 and the corresponding lost user hours.

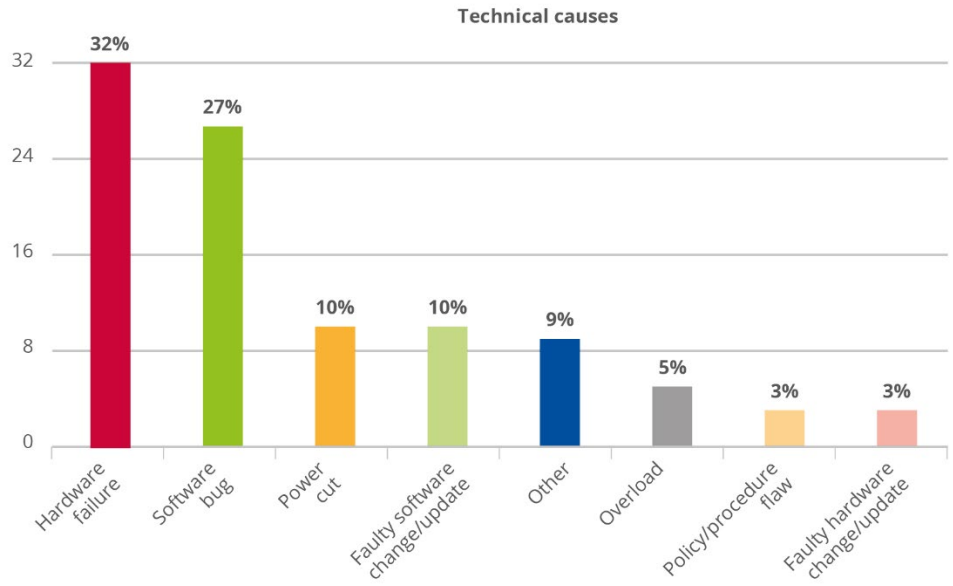
Figure 10: Root causes of incidents v user hours lost – Telecom security incidents in 2022



3.3.2 Breakdown of system failures

System failures counted for 111 incidents reports, meaning 72 % of total incidents for 10 481 million user hours lost.

Figure 11: Root causes of system failure incidents vs user hours lost – Telecom security incidents in 2022 (system failures)



3.3.3 Breakdown of human errors

Human errors counted for 23 incidents and 15 % of total incidents for 135 million user hours lost.

Figure 12.a: Technical causes – Telecom security incidents in 2022 (human errors)

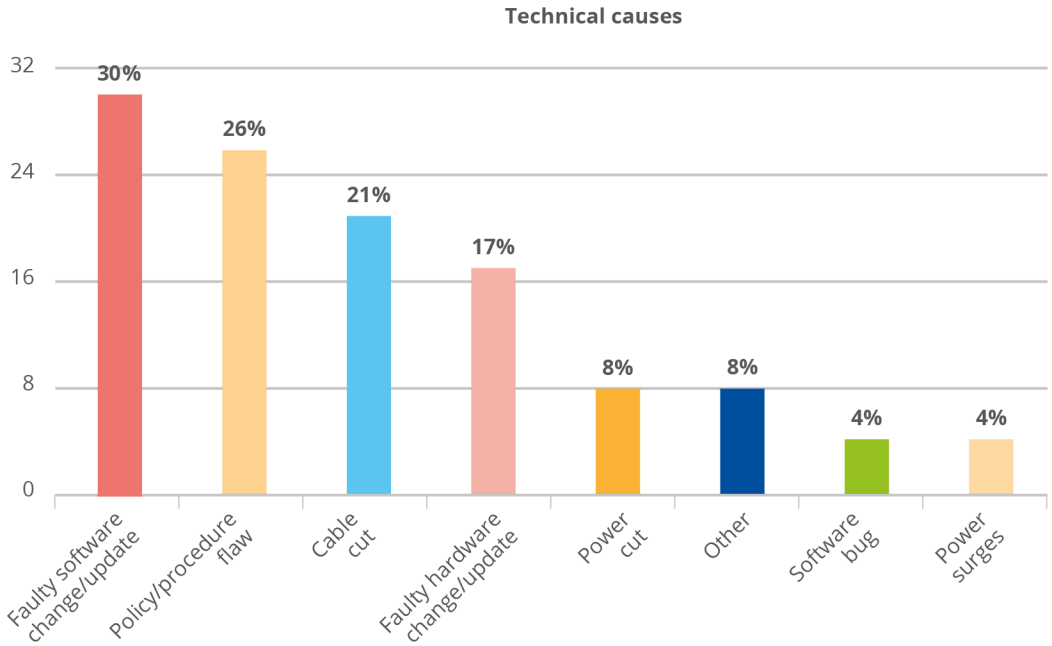
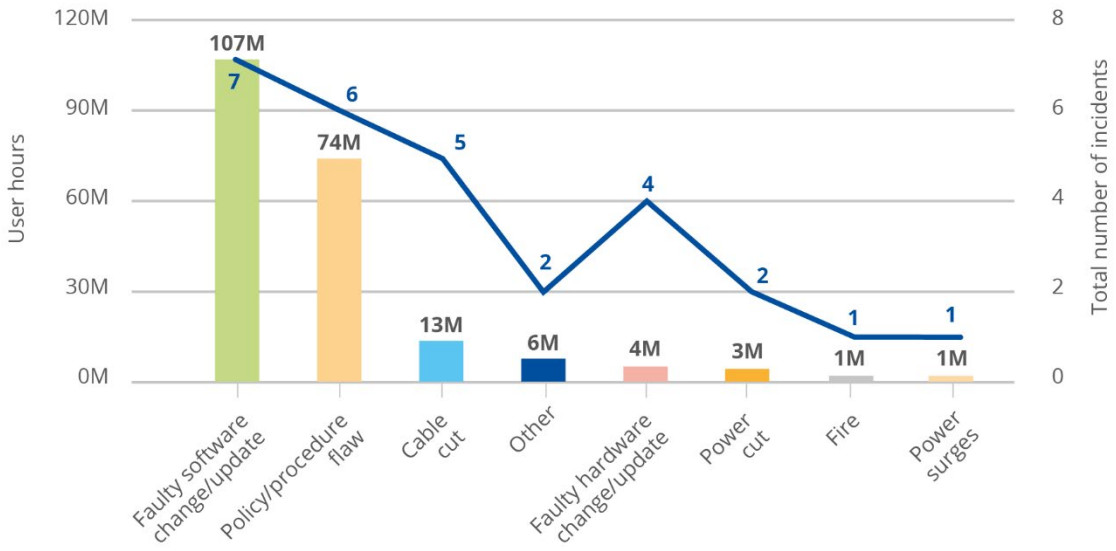


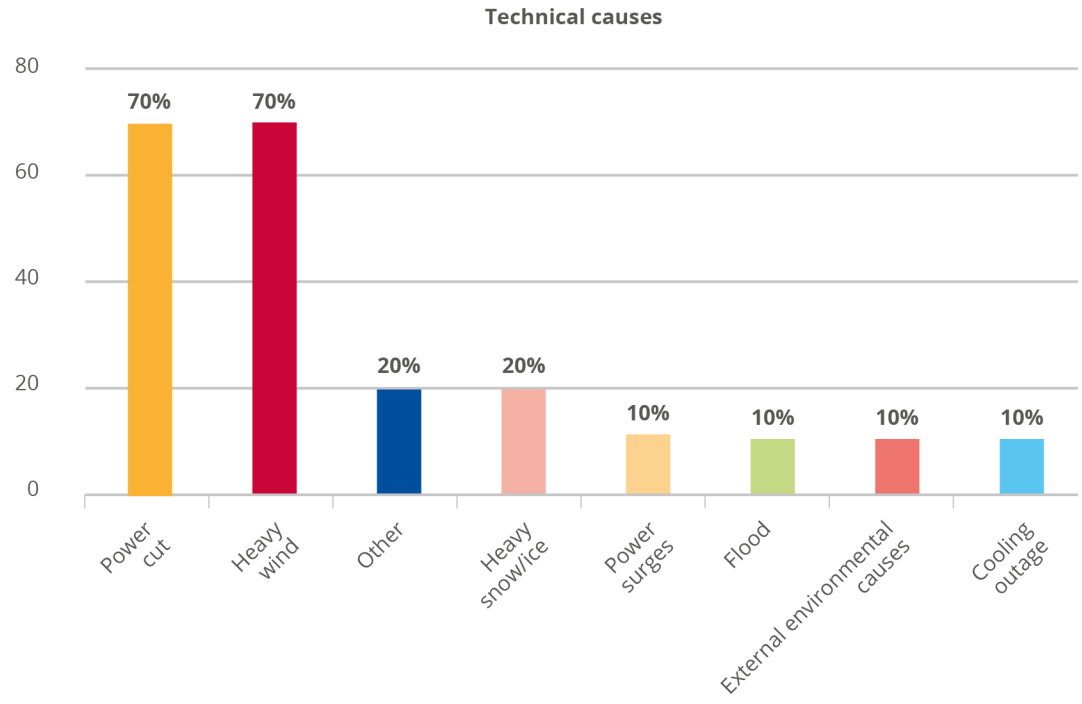
Figure 12.b: Root causes of human error incidents vs user hours lost – Telecom security incidents in 2022 (human errors)



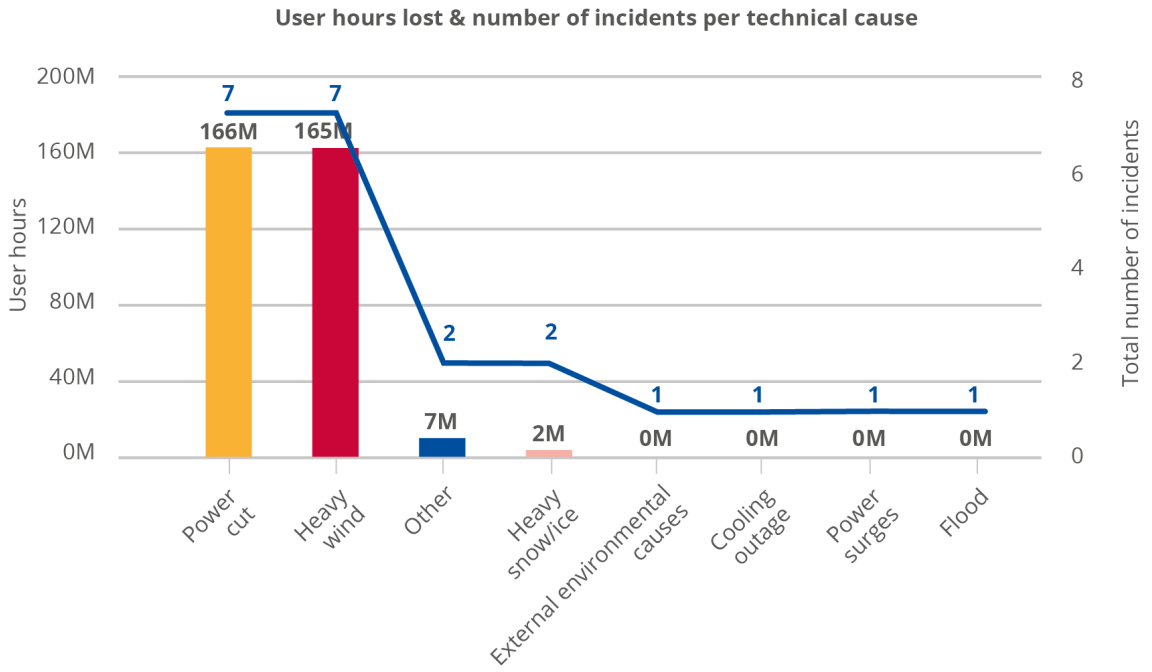
3.3.4 Breakdown of natural phenomena

Natural phenomena accounted for 10 incidents and 6 % of total incidents for 168 million user hours lost.

Figure 13: Root causes of natural phenomena incidents vs user hours lost – Telecom security incidents in 2022 (natural phenomena)



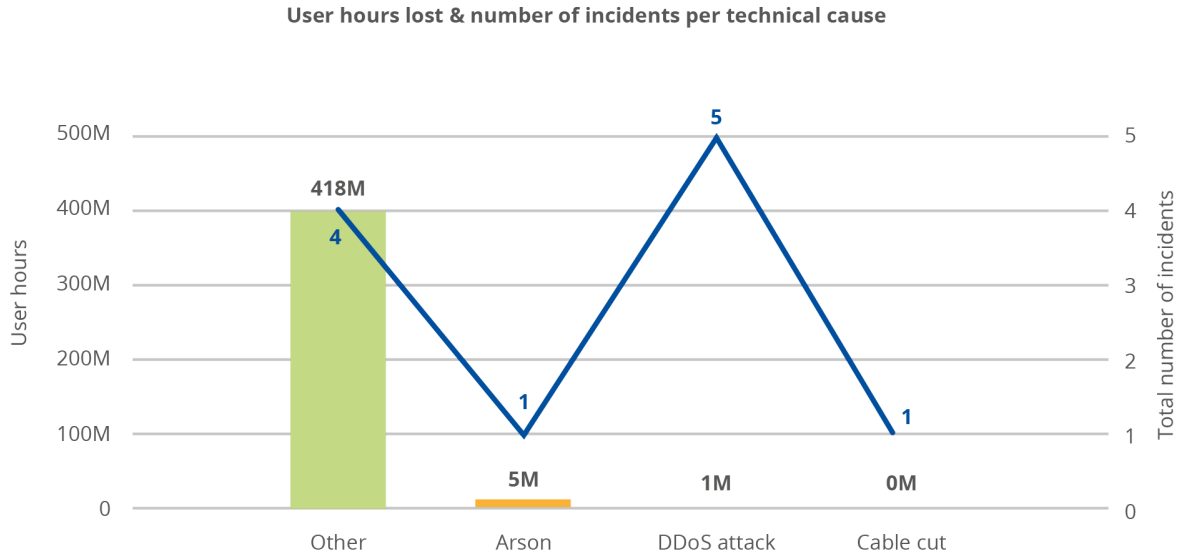
a)



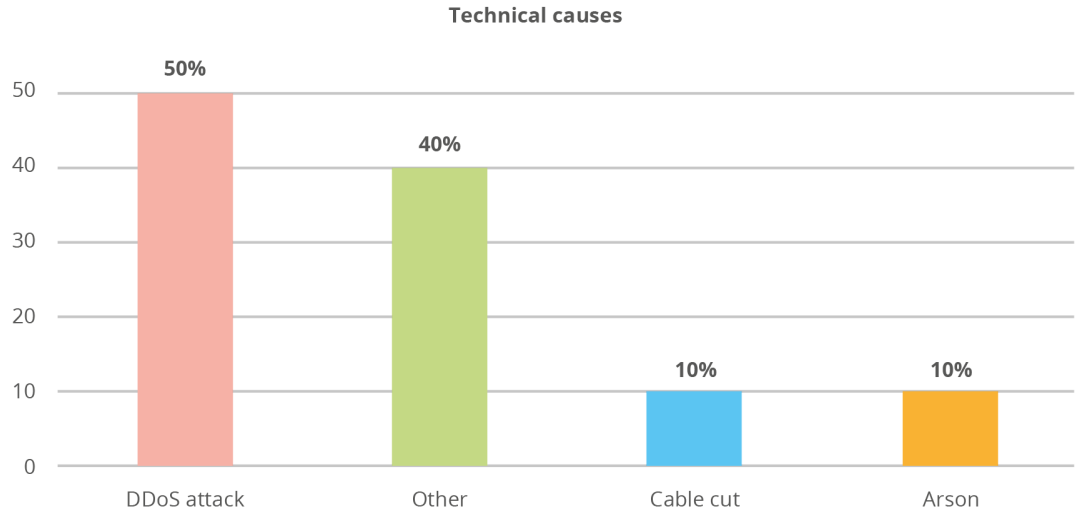
3.3.5 Breakdown of malicious actions

Malicious actions counted for 10 incidents and 6 % of total incidents, for 425 million user hours lost, mainly due to DDoS attacks and other reasons ([16]). In 2022, five DDoS incidents were reported, resulting in 1 million user hours lost.

Figure 14: Root causes of malicious action incidents v user hours lost – Telecom security incidents in 2022 (malicious actions)



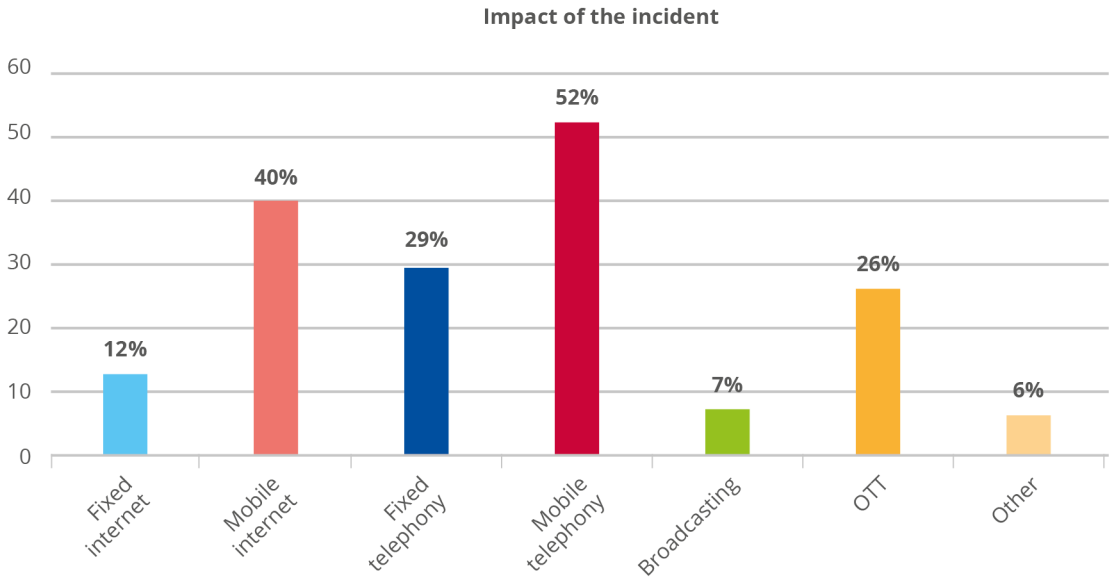
([16]) 'Other' implies that no information was provided. Therefore, there will be a need to provide more information in future incident reports.



3.4 SERVICES AFFECTED

Figure 15 examines the services affected by incidents – from mobile and internet telephony, fixed internet and telephony, broadcasting and OTT services according to EECC-type services.

Figure 15: Services affected ([17]) – Telecom security incidents in 2022



Again, most of the reported incidents affected **mobile services**. In 2022, around 52 **%** of reported incidents had an impact on mobile telephony and internet in the EU, while fixed telephony continued to decline.

Mobile internet followed, with around 40 % in 2022 – almost the same percentage as in 2021.

Reported incidents affecting **OTT services ([18])** rose to 26 % of all reported incidents in 2022.

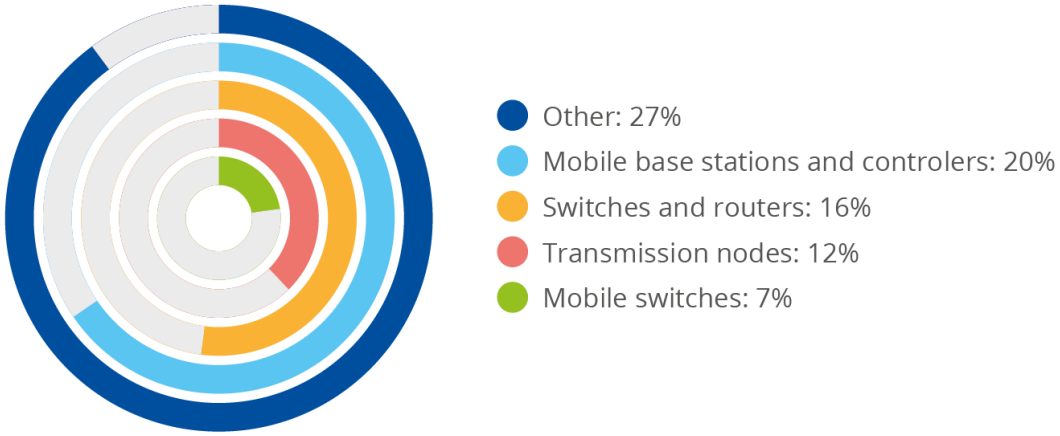
([17]) It bears noting that for most reported incidents there was an impact on more than one service, which explains why the percentages in Figure 15 add up to more than 100 %.

([18]) These newly introduced services and data still need to be consolidated and normalised over 3 years. In 2021, OTT represented 4 %.

3.5 TECHNICAL ASSETS AFFECTED

Each incident report also describes the (secondary) assets affected during the incident. **Figure 16** shows the assets most affected. 'Other' means that detailed information was not provided. In the future, more information will need to be provided by Member States to improve the analysis of incidents. Incidentally, reassessing the asset taxonomy will also be needed to improve incident reporting.

Figure 16: Assets affected – Telecom security incidents 2022



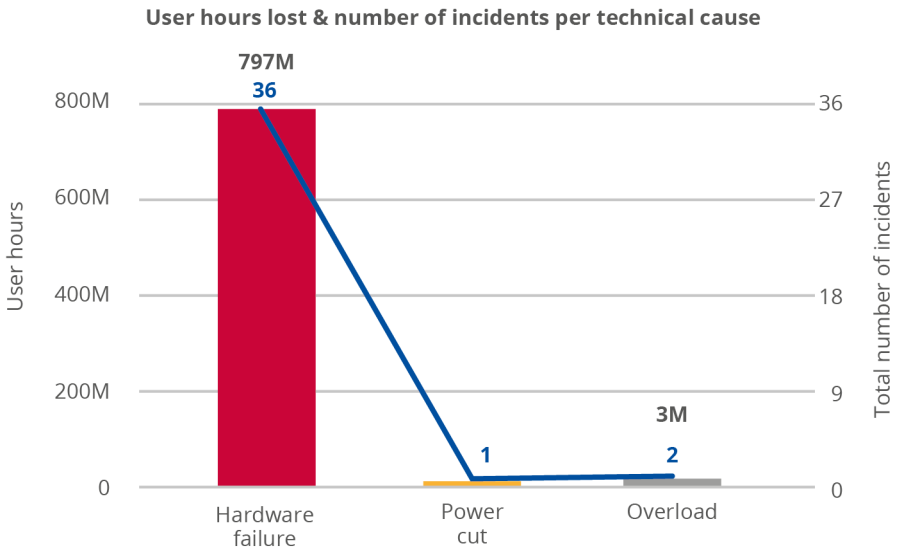
4. DEEP-DIVE ANALYSIS OF THE TECHNICAL CAUSES OF INCIDENTS

This section contains an in-depth review of the most high-profile technical causes behind reported incidents, focusing not only on 2022 but also on previous years.

4.1 HARDWARE FAILURES

In 2022, 36 incidents (23 % of total) were marked as hardware failures; they resulted in 797 million user hours lost, as seen in **Figure 17**. All of them were reported as system failures.

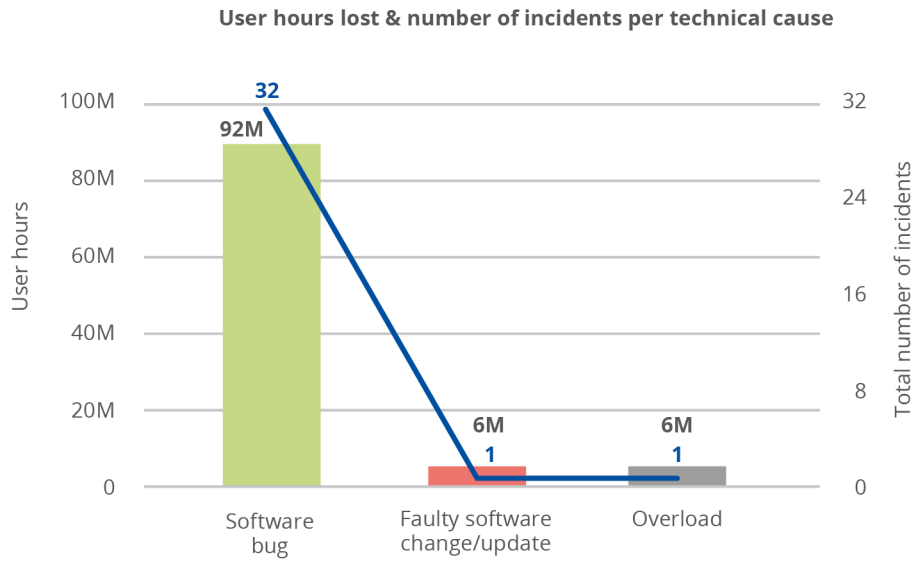
Figure 17: Incidents with hardware failure as the root cause – Telecom security incidents in the EU in 2022



4.2 SOFTWARE BUGS

In 2022, 32 incidents (20 % of total) were marked as being due to software bugs; they resulted in 92 million user hours lost, as can be seen in **Figure 18.** compared to 216 million in 2021. All but one of them were reported as system failures, with one incident being reported as due to human error.

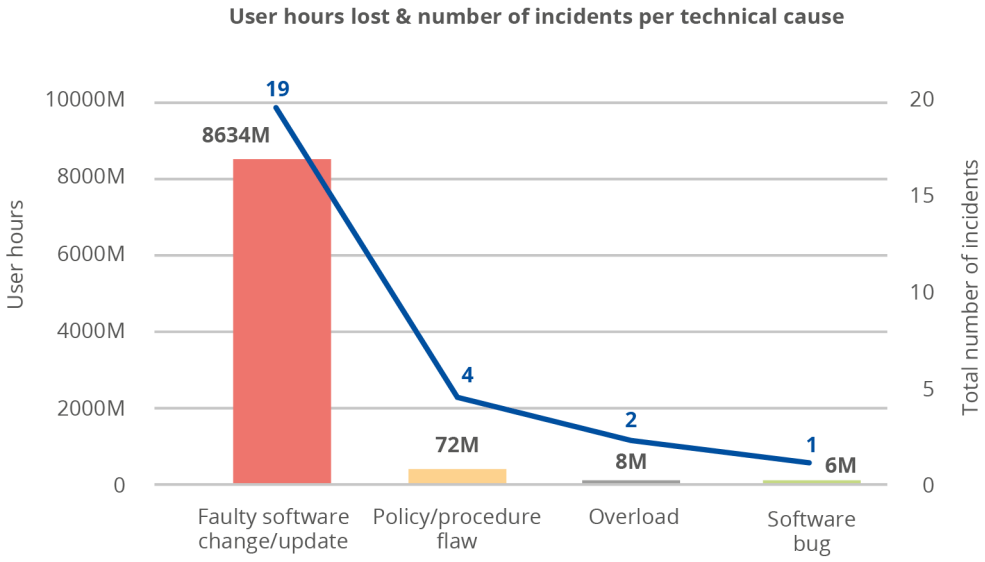
Figure 18: Incidents having software bugs as the root cause – Telecom security incidents in the EU in 2022



4.3 FAULTY SOFTWARE CHANGES/UPDATES

In 2022, 12 % of total incidents (**19 incidents**) were marked as being due to faulty software changes or updates, resulting in a staggering **8 634 million** user hours lost, as can be seen in **Figure 19**. Among them, seven incidents were due to human errors, accounting for 107 million user hours lost.

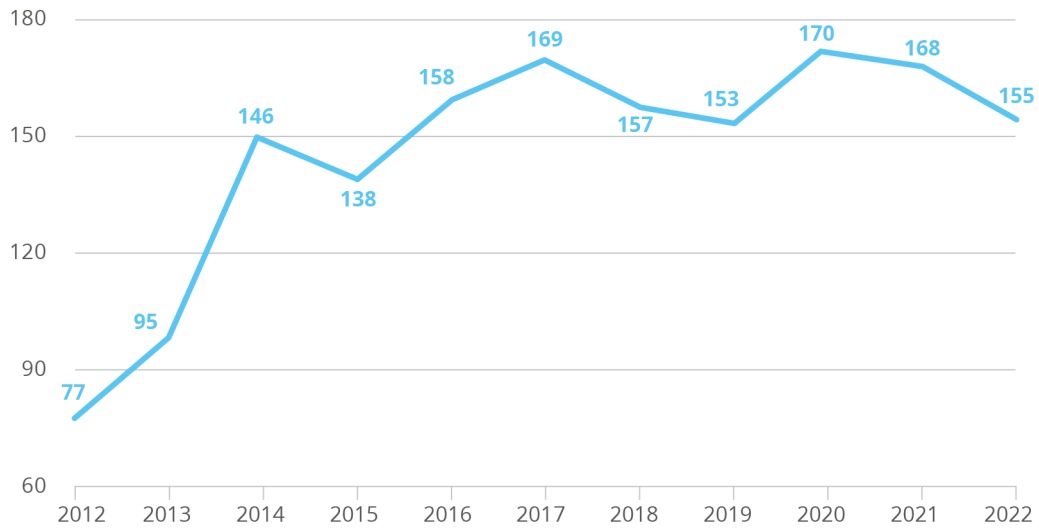
Figure 19: Incidents having faulty software changes/updates as the root cause –Telecom security incidents in the EU in 2022



5. MULTIANNUAL TRENDS

ENISA has been collecting and aggregating incident reports since 2012. In this section, we present multiannual trends over the last 11 years, from 2012 to 2022. This dataset contains 1 586 reported incidents in total, as we can see in **Figure 20**. Over the course of the last 5 years, the number of incidents has been stabilising at around the 160/year mark, meaning an average of one incident every 2 days.

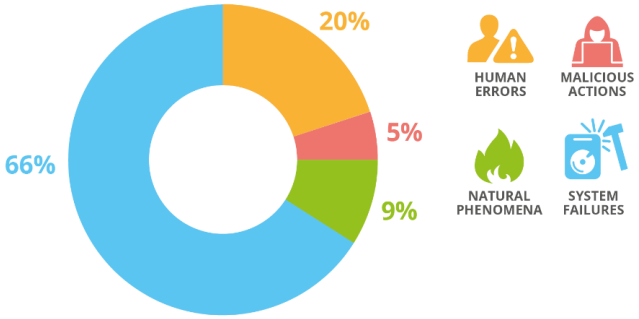
Figure 20: Number of incidents reported per year (2012–2022)



5.1 MULTIANNUAL TRENDS – CATEGORIES OF ROOT CAUSES

Every year, from 2012 to 2022, system failures were the most common root cause. In 2022, the share of system failures remained stable, continuing the trend first observed in 2020 as seen in **Figure 21**.

Figure 21: Root cause categories – Telecom security incidents in the EU reported over 2012–2022

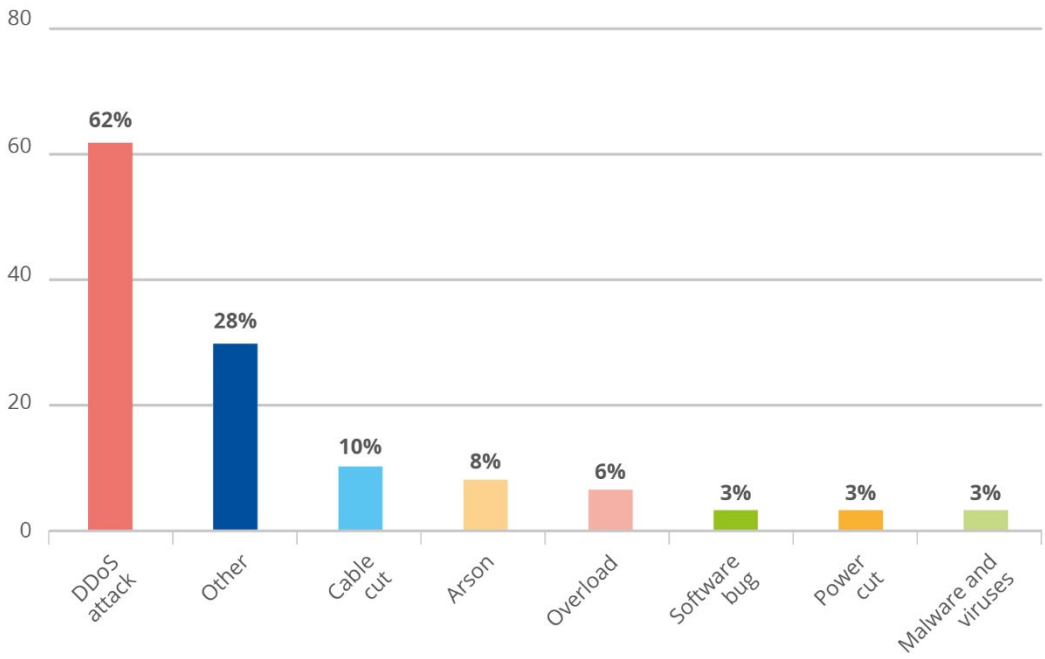


In total, **system failures** accounted for 1 036 incident reports (66 % of the total). For this root cause category, over the last 11 years, the most common causes for system failures were hardware failures (34 %) and software bugs (27 %). The second most common root cause over

the 11 years of reporting was **human errors**, with nearly a fifth of total incidents (20 %, 309 incidents in total). **Natural phenomena** come third, at almost a tenth of total incidents (9 %, 149 incidents in total).

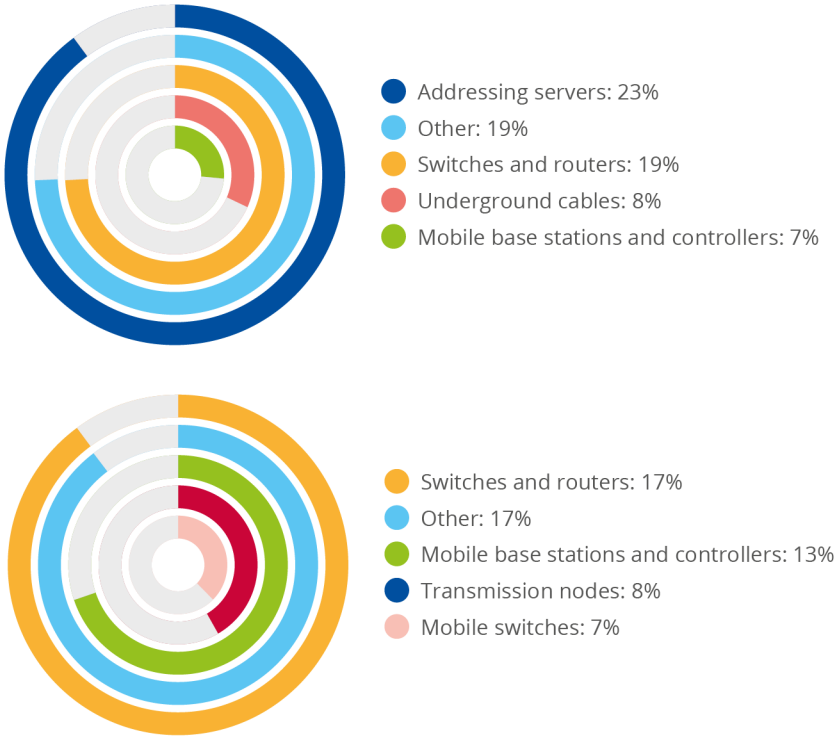
Only 5 % of incidents have been categorised as **malicious actions**, with 83 incidents over the course of 11 years. In the 2012–2022 period, nearly two thirds of malicious actions consisted of denial-of-service attacks (62 %), while the remainder were mainly comprised of lasting damage to physical infrastructure, for example cable cuts and arson. Only 3 % was attributed to malware and viruses, as shown in **Figure 22**. Incidentally, 28 % of technical causes are being classified as 'other'. This highlights the need to update the taxonomy of malicious actions – something that the NIS2 report has underlines as well.

Figure 22: Technical causes for incidents due to malicious actions – Telecom security incidents in the EU reported over 2012–2022



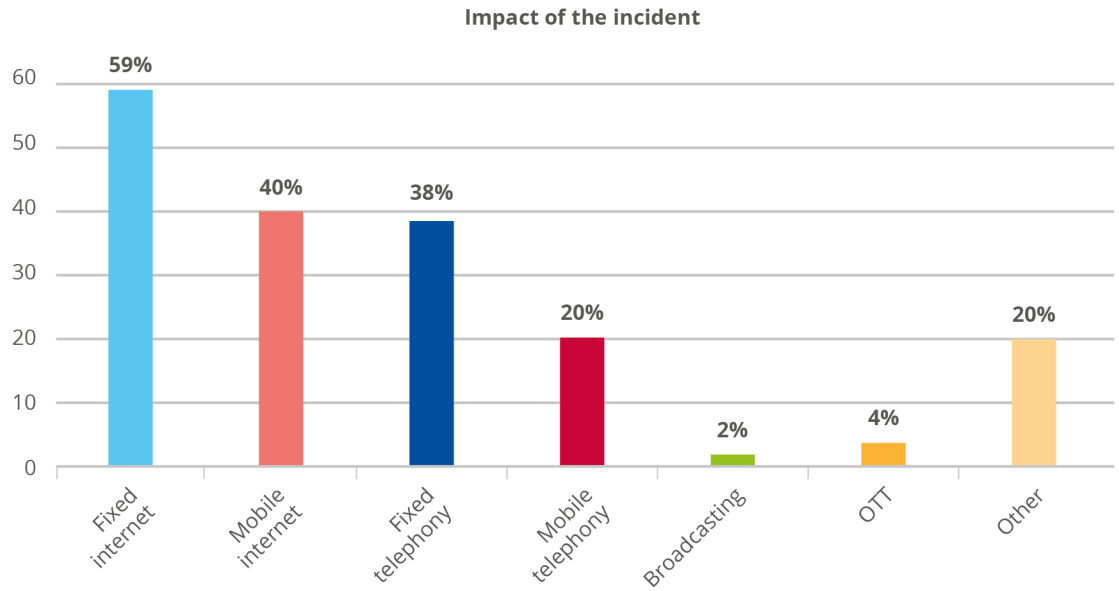
Interestingly, the **assets** affected by malicious actions differ significantly from the overall categorisation of affected assets. Addressing servers came first, with 23 %, followed by switches and routers, at 19 %, as seen in **Figure 23**.

Figure 23: Assets affected by incidents due to malicious actions v assets affected by all types of incidents



Moreover, with respect to **services** affected by malicious actions, 59 % referred to fixed internet and 40 % to mobile internet services, whereas 4 % referred to OTT services.

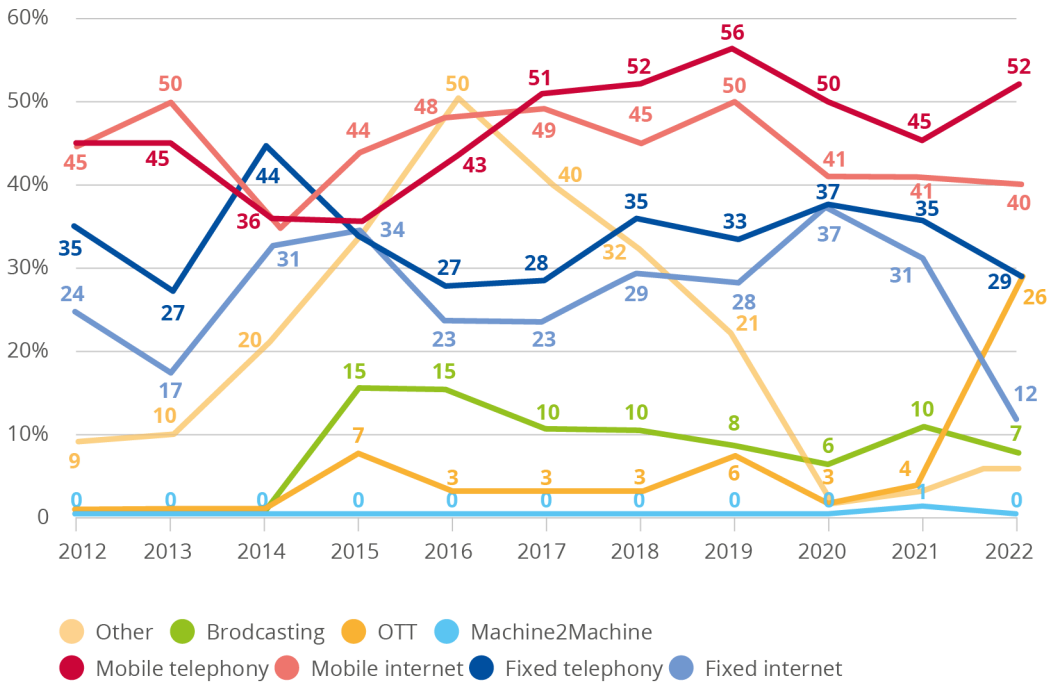
Figure 24: Services affected by incidents due to malicious actions – Telecom security incidents in the EU reported over 2012–2022



5.2 MULTIANNUAL TRENDS – IMPACT ON EACH SERVICE

Over the period, mobile internet and mobile telephony were once more the most impacted by incidents (44 % and 47 %, respectively). The first one remained stable, when the second pursued its decrease. Fixed internet decreased to 27 %, while fixed telephony services decreased to 33 %. The increase in broadcast-related incidents has persisted since 2020. Since 2021, reporting of incidents related to OTT communication services has been organised.

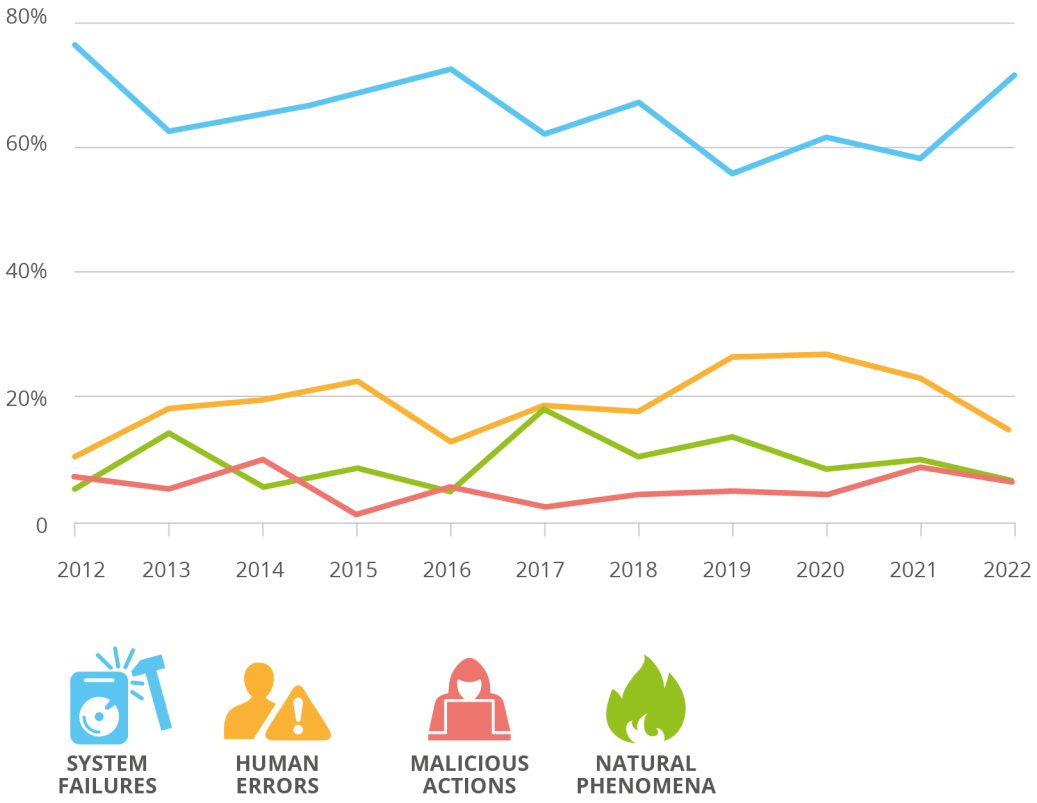
Figure 25: Trends on impact for each service reported over 2012–2022



5.3 MULTIANNUAL TRENDS – USER HOURS FOR EACH ROOT CAUSE

In terms of overall impact, as indicated in **Figure 26**, system failures traditionally rank high in terms of user hours lost. After a peak in 2020, the impact of human errors is steadily decreasing. The overall impact of natural phenomena has been trending downward over the last 3 years, while the impact of malicious actions is steadily rising, reaching 508 million user hours lost since 2020, after 3 years.

Figure 26: User hours lost for each category of root causes, 2012–2022



5.4 MULTIANNUAL TRENDS FOR SEVERITY OF IMPACT OF INCIDENTS

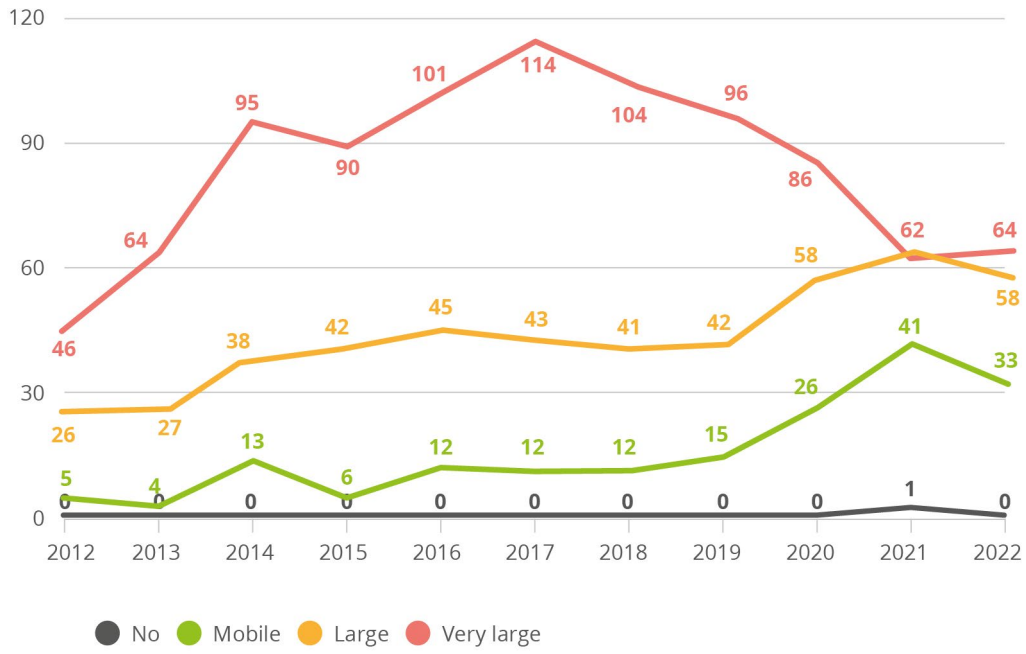
ENISA has published technical guidelines on incident reporting under the EECC ([19]), including on thresholds, severity estimation and calculating hours lost. Since 2017, a noteworthy and constant decrease in reports of extremely severe incidents was observed, slightly halted in 2022. Conversely, there has been a steady increase in minor and large incidents since 2019.

These findings point, on the one hand, to the growing maturity of electronic communication providers with respect to the incident reporting process and, on the other hand, to the improvement of resilience and the provision of security services (including incident reporting itself) that has led to a lower number of very large severe incidents.

Relevant multiannual trends may be found in **Figure 27.**

([19]) See https://www.enisa.europa.eu/publications/enisa-technical-guideline-on-incident-reporting-under-the-eecc, March 2021.

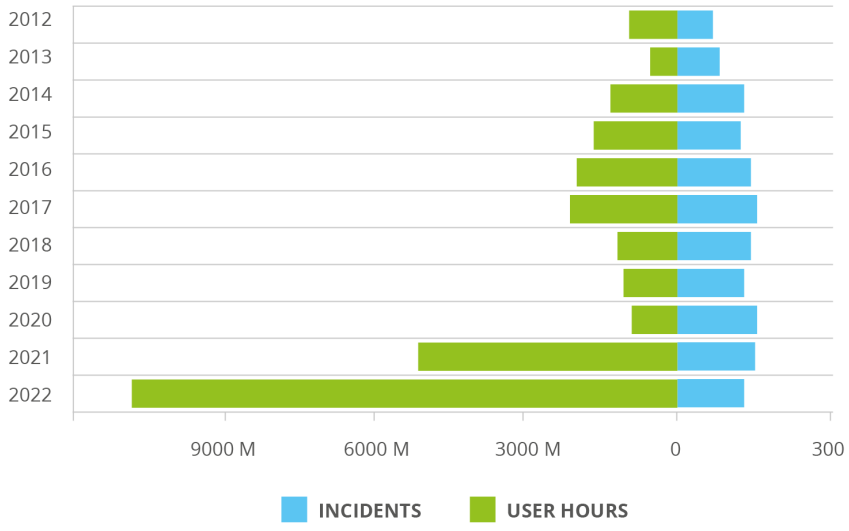
Figure 27: Severity of impact for each year – multiannual trends 2012–2022 (number of incidents)



5.5 MULTIANNUAL TRENDS FOR THE NUMBER OF INCIDENTS AND USER HOURS LOST

Over the years, the number of incidents has increased steadily and is now stabilising at around 150–170 a year.
Precisely, in 2022 data were as follows: 155 incidents for 11 216 million hours lost.

Figure 28: Number of incidents and user hours lost each year



6. CONCLUSIONS

The present document covers the incidents reported by the authorities for the calendar year 2022 and gives an anonymised, aggregated EU-wide overview of telecom security incidents. It marks the 11th time ENISA has published an annual report for the telecom sector. To conclude, here are the main findings and some general observations about this process and the broader policy context.

Main findings

Reporting of incidents shows the following.

- Mobile telephony and mobile internet were the most impacted sectors, with respectively 52 % and 40 % of incidents.
- OTT services accounted for 26 % of incidents.
- Traditional fixed telephony, fixed internet and broadcasting services continued to drop in terms of reports.
- System failures continued to largely dominate in terms of impact, reaching 72 % in 2022. They globally accounted for 10 481 million user hours lost (against 10 025 million for OTT) compared to 363 in 2021 and 419 million user hours in 2020. In 2022, 36 incidents (23 % of total) were marked as hardware failures. They resulted in 797 million user hours lost compared to 53 million in 2021. All of them were reported as system failures.
- Human error incidents have steadily decreased since 2020, from 26 % in 2020 to 23 % in 2021 and 15 % in 2022. Human error accounts for 135 million user hours lost in 2022.
- Malicious actions slowed down their progression in 2022, at 6 % of total incidents. In 2020, incidents marked as malicious actions represented 4 % of the total, a number which rose to 8 % in 2021. However, they accounted for 435 million of user hours lost in 2022, compared to 70 million in 2021 and 13 million in 2020.
- In 2022, five distributed denial-of-service incidents were reported, resulting in 1 million user hours lost.
- The share of incidents due to natural phenomena remained stable, at 6 %. However, the number of user hours lost increased.
- In 2022, incidents flagged as failures by third parties represented 23 % of incidents, with a total of 35 incident reports compared to 22 % in 2021, 29 % in 2020 and 32 % in 2019. Four of them originated from human errors, three from malicious actions and one from natural phenomena.
- Five incidents concerning confidentiality and authenticity were reported, compared to three in 2021.
- One incident concerning impact on redundancy was reported for the first time.
- One incident concerning a near-miss incident was reported for the first time.

General observations

- In the coming months, national authorities for telecom security will continue to focus on the transposition and the implementation of the EECC, which will bring the following changes.
  - The incident reporting requirements in Article 40 of the EECC have a broader scope, explicitly including, for example, breaches of confidentiality.
  - In addition, the arrival of the NIS2 directive in 2022 will consolidate the reporting of security breaches across multiple sectors including – but not limited to – the EECC as of 17.10.2024.
- In 2023 and 2024, ENISA will continue to work with national authorities through the ECASEC working group as well as the NIS Cooperation group to find and exploit synergies between different pieces of EU legislation, particularly when it comes to incident reporting and cross-border supervision.
- ENISA will also pursue the work with national authorities and regulators on how to implement the consolidated reporting of incidents under the NIS2 directive, since it brings significant

changes to security incident reporting in the EU by consolidating all relevant streams under the NIS2 umbrella, namely consolidating incident reporting under the EECC, NIS2 and electronic identification, authentication and trust services (eiDAS) regulations, among others.

- Additionally, it is worth noting that many smaller-scale incidents, however frequent, remain under the radar. Some of these incidents, such as targeted DDoS, SIM-swapping and SS7 attacks, can still have major impacts on individual customers. In coming years, this area needs to be analysed better with the possible introduction of a summary reporting format for these smaller-scale incidents.
- The CIRAS methodology and guidelines may also be reviewed during our regular discussions to better reflect new developments and to facilitate reporting and alleviate the administrative burden.

ENISA looks forward to continuing its close collaboration with EU Member States, the NRAs and experts from the telecom sector from across Europe to implement security incident reporting efficiently and effectively, and takes the opportunity to thank all the contributors of this report

TP-09-24-167-EN-N

ABOUT ENISA

The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union's infrastructure, and, ultimately, to keep Europe's society and citizens digitally secure. More information about ENISA and its work can be found here: www.enisa.europa.eu.

ENISA
European Union Agency for Cybersecurity

Athens Office
Agamemnonos 14
Chalandri 15231, Attiki, Greece

Heraklion Office
95 Nikolaou Plastira
700 13 Vassilika Vouton, Heraklion, Greece

Brussels Office
Rue de la Loi 107
1049 Brussels, Belgium

enisa.europa.eu

ISBN: 978-92-9204-668-2
DOI: 10.2824/902186