An Coimisiún um
Rialáil Cumarsáide
Commission for
Communications Regulation

Network Operations
Annual Report 2023

Information Notice

Reference:	ComReg 24/53
Version:	Final
Date:	26/06/2024

An Coimisiún um Rialáil Cumarsáide
Commission for Communications Regulation
1 Lárcheantar na nDugaí, Sráid na nGildeanna, BÁC 1, Éire, D01 E4X0.
One Dockland Central, Guild Street, Dublin 1, Ireland, D01 E4X0.
Teil | Tel +353 1 804 9600 Suíomh | Web www.comreg.ie

Additional Information

Document No:	24/53
Date:	26 June 2024

Content

Section Page

1 Executive Summary

1. ComReg's Network Operations Unit ("NOU") is a specialised unit which, among other things, is focussed on the resilience of Electronic Communications Networks ("ECN ")and Electronic Communication Services ("ECS") and the analysis of the root causes of significant security incidents in respect of same.

2. In this regard, a revision of the European Telecommunications Regulatory Framework, namely the European Electronic Communications Code (the "EECC")[1] was published and entered into force on 20 December 2018.

3. Significantly, Articles 40 and 41 of the EECC, relating to the security of networks and services, replaced Article 13a and 13b of the then European Telecommunications Regulatory Framework Directive, as amended. Articles 40 and 41 of the EECC are transposed in Part 2 ("Security of Networks and Services") of the Communications Regulation and Digital Hub Development Agency (Amendment) Act 2023, (No. 4 of 2023) (the "Act of 2023"). The current obligations on providers and ComReg's associated powers are outlined in Chapter 2 below while the previous obligations and powers available to ComReg[2] are contained in Annex 1.

4. The Act of 2023 brings more electronic communications services within scope, and the terms "Security"[3] and "Security Incidents"[4]are now explicitly defined. Part 2 of the Act of 2023 details security obligations for providers of: electronic communications networks and services, and of Number Independent Interpersonal Communication Service ("NI-ICS")[5].

[1] Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code.
[2] Prior to 09 June 2023 and the Commencement of the Act of 2023.
[3] 'security of networks and services' means 'the ability of electronic communications networks and services to resist, at a given level of confidence, any action that compromises the availability, authenticity, integrity or confidentiality of those networks and services, of stored or transmitted or processed data, or of the related services offered by, or accessible via, those electronic communications networks or service', see Article 2(21) of the EECC, as transposed in section 5 of the Act of 2023.
[4] 'security incident' means 'any action that compromises the availability, authenticity, integrity or confidentiality of networks and services, of stored or transmitted or processed data, or of the related services offered by, or accessible via, those electronic communications networks or services', see section 5 of the Act of 2023.
[5] NI-ICS are as defined in Article 2(7) of the EECC and Regulation 2 of the European Union (Electronic Communications Code) Regulations 2022, S.I. No. 444 of 2022, (the "Regulations of 2022"), and are now included in the revised definition of an ECS, as set out in Regulation 2 of the Regulations of 2022 and furthermore NI-ICS are now included in Article 2(4) of the EECC.

5. Furthermore, under section 13 of the Act of 2023, ComReg shall take reasonable steps to ensure that providers comply with the obligations placed on them, by or under Part 2 of the Act of 2023.

6. As technology and macro (climatic, legislative, and socio-economic) conditions evolve, the focus of ComReg's work on resilience of networks and services has changed. Since 2022, the focus has been squarely on the resilience of the ECN and ECS due, among other things to the disruption of their power supply, particularly during the peak winter consumption season. In 2023 ComReg initiated a project to study and assess this risk and this is expected to conclude in 2024.

7. Section 4.5 provides an analysis of the root causes of significant security incidents in Ireland during the period in question. In noting ENISA's[6] nomenclature, faulty hardware (whether misconfigured or otherwise), faulty software and software bugs are all considered system failures. The following infographic captures the key outturn:

[6] ENISA is the European Union Agency for Cybersecurity, see https://www.enisa.europa.eu/

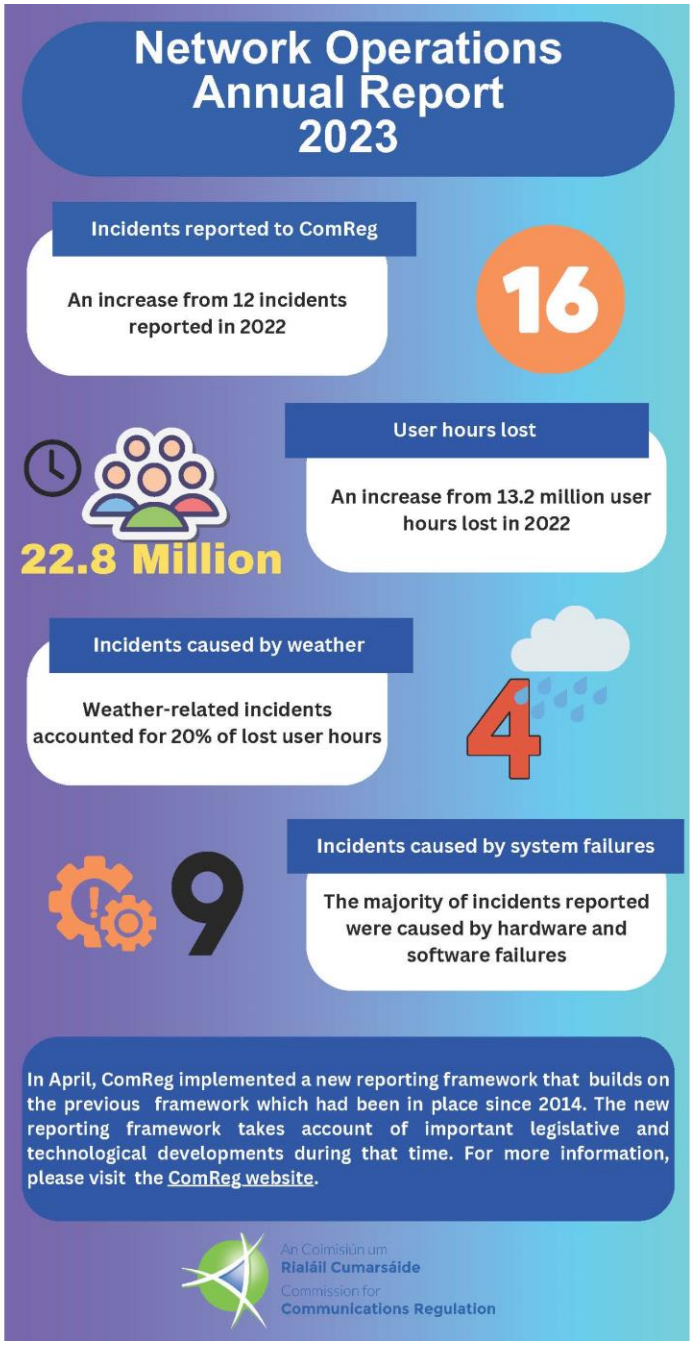

Figure 1: Security Incidents Reported to ComReg during 2023

8. The main cause of significant security incidents during 2023, was software related; be that faulty software or software bugs. ComReg notes that this is not an isolated occurrence but rather it also featured frequently in prior years. Nor is it specifically related to Irish providers as figures from ENISA show the average for this category over the last ten years across all member states was 64% of all reported incidents.

9. This could be better mitigated against by:

    - Improving testing, industry-wide, by both vendors and providers, of software and hardware;

    - The presence of appropriately experienced staff, during swap-outs or upgrades; and

    - clearer escalation and roll-back procedures.

10. ComReg will continue to monitor significant security incidents and their causes, in the year ahead. Under section 6 of the Act of 2023, operators of ECN and ECS need to continue to take care to manage the risks to their networks and services; by ensuring appropriate measures are put in place appropriate to mitigate the risks identified.

11. As ComReg continues to gather more information about reported security incidents, trends and their resolution, this evidence will assist ComReg in determining whether operators of ECN and ECS are managing the various risks appropriately and in accordance with their obligations.

12. If operators are found wanting in their obligations, ComReg will consider using the powers available to it under Part 2 of the Act of 2023, to ensure that operators comply with the obligations placed on them under the Act of 2023.

13. The remainder of this document is structured as follows:

    - Chapter 2: Briefly summarises the current obligations on providers and relevant ComReg powers since 9 June 2023, pursuant to, the Communications Regulation and Digital Hub Development Agency (Amendment) Act 2023, No.4 of 2023 (the “Act of 2023”);

    - Chapter 3: Covers Resilience and Security Incidents[7] [8];

    - Annex 1: Outlines the previous obligations on providers and relevant ComReg powers during 2023, pursuant to, Regulations 23 and 24 of the Framework Regulations[9].

[7] As defined in section 5 of the Act of 2023.
[8] This includes a review of security incidents that happened in 2023.
[9] European Communities (Electronic Communications Networks and Services) (Framework) Regulations 2011 (S.I. 333/2011)

2 Obligations on Providers and Relevant ComReg Powers

2.1 Security provisions of the EECC, transposed into Irish Law by the Act of 2023

14. The European Electronic Communications Code (the "EECC")[10], sets out provisions in relation to the Security of Networks and Services in Article 40 and the Implementation and Enforcement of those provisions in Article 41.

15. Specifically, Articles 40 and 41 of the EECC have been transposed by sections 11, 13, 14, 15 and 16 of the Communications Regulation and Digital Hub Development Agency (Amendment) Act 2023 (the "Act of 2023"). ComReg notes that the security incident reporting obligation applies to all "providers" of Electronic Communications Networks and Services ("ECN" and "ECS"). In the context of this document, the term 'provider' is as defined in section 5 of the Act of 2023[11]. Further, it should be noted that failure to comply with section 11 of the Act of 2023 is an offence.

[10] Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code.
[11] "provider" means a provider of public electronic communications networks or of publicly available electronic communications services.

3 Resilience and Security Incidents

3.1 Resilience of Networks and Services

16. The ISO standard[12] defines resilience as *"the ability of an organization to prevent or resist being affected by an event or the ability to return to an acceptable level of performance in an acceptable period of time after being affected by an event".*

17. Furthermore resilience, as the term relates to ECN or ECS (Including NI-ICS), describes the ability of a provider's network or service, to return to its normal state following a disruptive security incident. Security Incidents are defined in section 5 of the Act of 2023 and are actions that compromise the availability, authenticity integrity or confidentiality of networks and services. Therefore, in order to ensure that providers' ECN or ECS are appropriately resilient, the amount of user hours lost[13] due to security incidents should be measured and ultimately minimised. It is obligatory that providers manage the risks to their ECN and ECS as required by section 6 of the Act of 2023.

18. The resilience of an ECN can be affected in multiple ways and in its core network[14], distribution or access sections, all of which can then adversely impact the provider, its customers, or other providers of ECN or ECS who rely on wholesale access or interconnection to the impacted network or service. Furthermore, a large security incident that affects a provider's network resilience, at the core or distribution level, can have effects that propagate outside of Ireland, such as international switching or routing issues or a damaged international fibre network.

19. Since 2019, ComReg has engaged in best understanding and assessing the risk management practices of providers including, those providing publicly available electronic communications networks and services. Where appropriate, ComReg undertakes an assessment of risk management practices based on the information provided by the providers concerned.

20. As technology and macro (climatic, legislative, and socio-economic) conditions evolve, so too does the focus of ComReg's work on resilience of networks and services. A prime concern since 2022 is that of the resilience of the ECN and ECS due to the disruption of the power supply to their networks and services (during the peak winter consumption season). As such, and since 2022 ComReg has

[12] See ISO 22300(en), Definition 3.193: ISO/DIS 22300(en), Security and resilience — Terminology
[13] User Hours Lost is the product of the duration of the security incident and the number of users affected by it.
[14] Including all relevant Operational and Business Support Software (OSS and BSS).

conducted a winter check-in with the providers of ECN and ECS in order to ensure that each had factored in the risks to Electricity Supply issued by the Commission for the Regulation of Utilities (the "CRU"). Furthermore, in 2023 ComReg instigated a project to study and assess the risks to ECN and ECS resilience due to the disruption of the power supply. This project is expected to conclude in 2024.

Further Work

21. Work on the resilience of networks and services is a continuing core activity. Over the next year the concentration of effort in this area will be to evaluate the learnings from the previous resilience project[15], while at the same time considering advances in network technology and the obligations on ComReg as a consequence of the Act of 2023.

3.2 Security Incidents

22. Security Incidents are defined in section 5 of the Act of 2023 as "*any action that compromises the availability, authenticity, integrity or confidentiality of networks and services, of stored or transmitted or processed data, or of the related services offered by, or accessible via, those electronic communications networks or services"*.

23. Typically, causes of security incidents include:

- Weather and natural phenomena: storms, wind, high temperatures, fog, snow and ice, and solar storms;
- Third party damage including: vehicular impact, cable theft; fibre cuts, deep diving submarines, remotely operated vehicles ("ROV"), anchor, cable plough or trawler related, cable damage;
- Malicious acts: theft, Telephony Denial of Service ("TDoS") incidents, Distributed Denial of Service ("DDoS") incidents, cyberattacks, vandalism, espionage, and sabotage;
- Power outages due to weather, including: insufficient protection (for example surge protection) of mains supply, insufficient or no back-up power and poor maintenance of back-up power; and

[15] See NOU Annual Reports 23/60 and 22/44, (Chapters 2.1 and 3.1 respectively).

- System failures including but not limited to hardware and software failure; insufficient redundancy; poor procedures, particularly 'roll-back' procedures[16]; poor supervision of both own and outsourced staff.

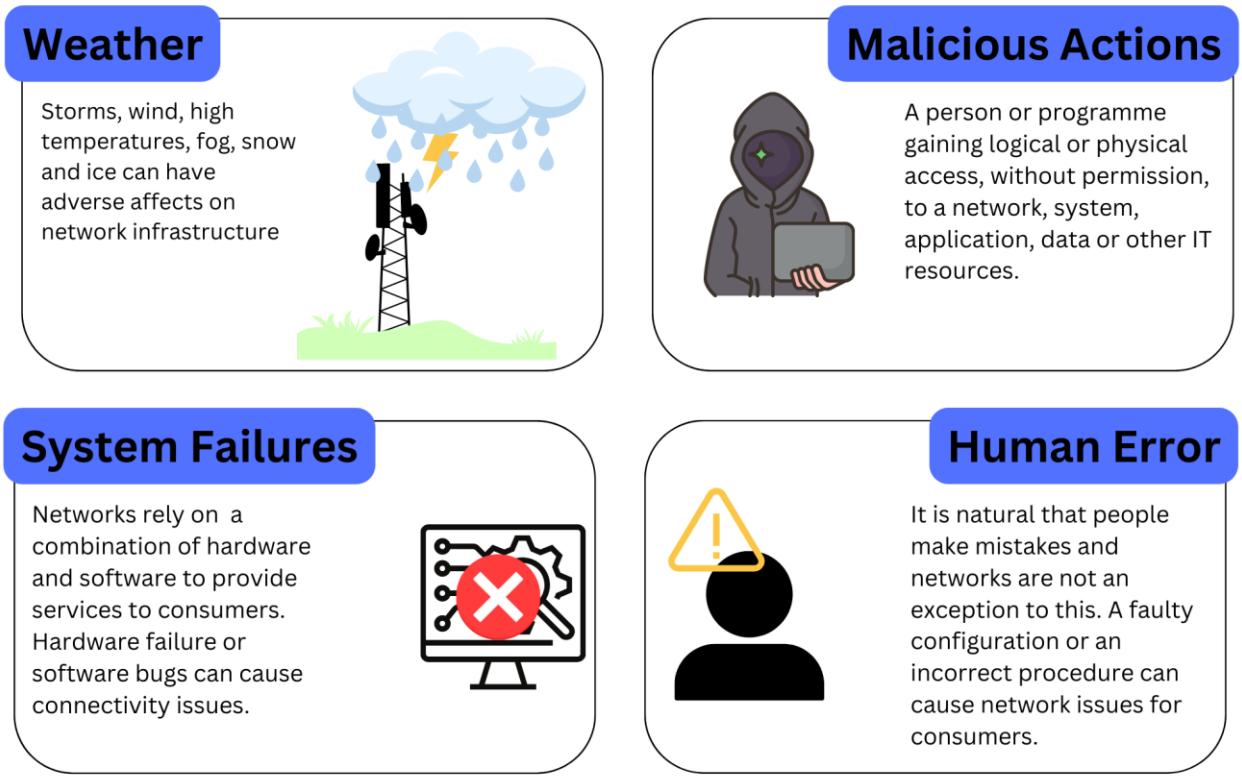

Figure 1: Examples of reported security Incidents (from ComReg Document No. 23/59

24. ComReg notes that systems failures and human errors again make up the majority of significant security incidents, involving ECN and ECS, that are reported to all Member States ("MS") as illustrated in Figure 2 below.

25. ComReg emphasises that this could be mitigated against, by industry-wide improved testing of software and hardware, along with clear escalation and roll-back procedures.

[16] This is where a software or hardware change is restored to is original state prior to the implementation of the change.

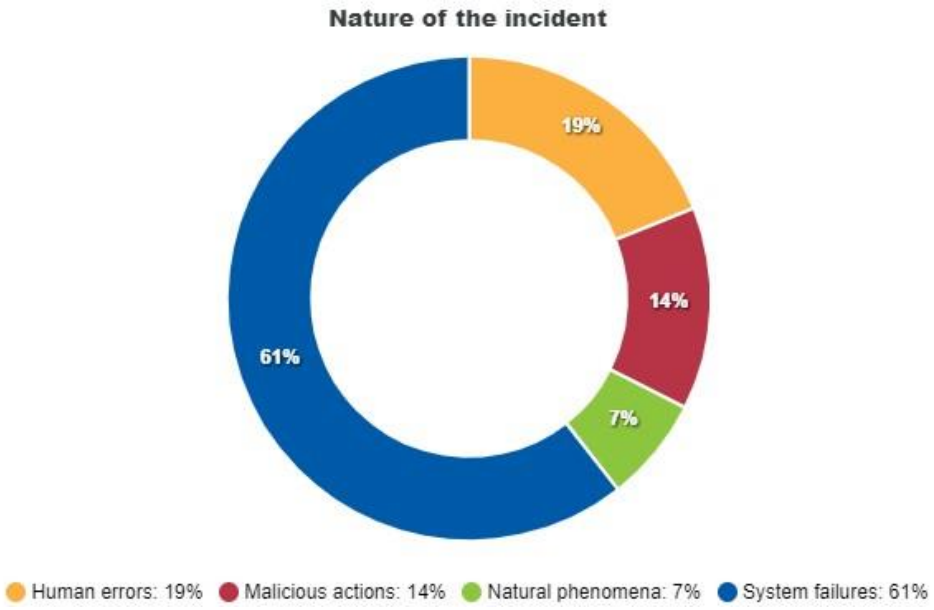

Figure 2: Nature of Security Incidents Across all MS for 2023 (Source: ENISA)

26. Furthermore, ComReg notes that across the last ten years this trend has been consistent across all MS and the ten-year averages for each security incident category are shown in figure 4 below. For system failures this has ranged from a low of 56% in 2019 to a high of 76% in 2016.

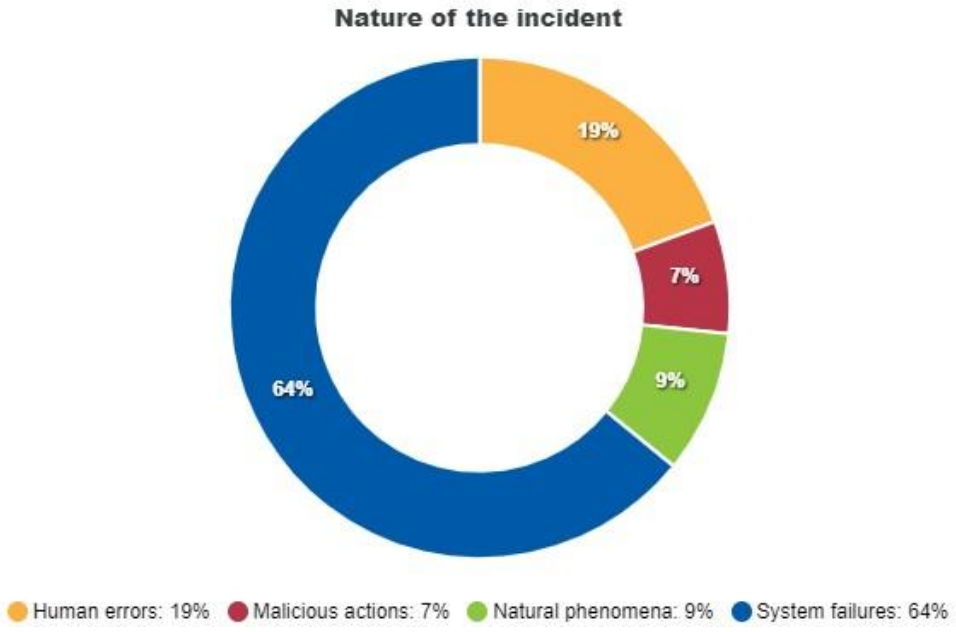

Figure 4: Nature of Security Incidents Across all MS, 10 Year Average 2013-2023 (Source: ENISA)

3.3 Reporting of Security Incidents and Thresholds

27. Once ComReg has been notified by a provider of a security incident that has had a significant impact on the operation of ECN or ECS; ComReg must in turn inform the Minister for the Environment, Climate and Communications (the "Minister")[17]. Following the agreement of the Minister and if necessary, ComReg must also inform the respective NRAs or Competent Authorities ("CA") in other MS and ENISA.

28. ComReg must also submit a summary report annually to the Minister, the European Commission and ENISA regarding the security incidents notified to it. The last such report was lodged with ENISA on 11 February 2023 and the summary statistics are presented in section 3.4 below.

29. ComReg's approach to management of reported security incidents and the coordination of its response to these incidents, was previously set out in its Reporting & Guidance on Incident Reporting & Minimum Security Standards, ComReg Document 14/02[18] ("Document 14/02").

30. ComReg began its review of Document 14/02, in 2022 and published its proposals – "*Network Incident Reporting Thresholds, A consultation to revise and replace ComReg Document 14/02 (Reporting & Guidance on Incident Reporting & Minimum Security Standards)*"[19]. A review was undertaken to update the guidelines due to technological changes, the new legislative framework post EECC – as transposed by the Act of 2023 and changes introduced in the updated ENISA Technical Guidelines[20] (the "Revised Guidelines").

31. The consultation closed on 25 May 2023 and following the consideration of all of the responses received from nine stakeholders, ComReg prepared the Response to Consultation and its associated Decision Instrument. The Decision Instrument,[21]

[17] See section 11(5) of the Act of 2023.
[18] Reporting & Guidance on Incident Reporting & Minimum Security Standards - https://www.comreg.ie/media/dlm_uploads/2015/12/ComReg1402.pdf
[19] ComReg Document No. 23/36: https://www.comreg.ie/publication-download/network-incident-reporting-thresholds-a-consultation-to-revise-and-replace-comreg-document-14-02-reporting-guidance-on-incident-reporting-minimum-security-standards
[20] https://www.enisa.europa.eu/publications/enisa-technical-guideline-on-incident-reporting-under-the-eecc
[21] Network Incident Reporting Thresholds: Response to Consultation | Commission for Communications Regulation (comreg.ie)

now in force, puts the thresholds and timescales for the reporting of a security incident on a statutory basis.

32. The reporting of security incidents to ComReg will be kept under review in light of future legislative and technological changes.

3.4 Network Incidents in 2023

General Commentary on the 2023 ENISA Report for Ireland

33. All security incidents reported to ENISA by ComReg are drawn from notifications made through the incident reporting portal[22]. The portal facilitates efficient incident updates[23] while the incident is in progress. Once the incident has concluded, and the root cause analysis has been completed satisfactorily, the incident report can then be closed by the provider concerned.

34. This information facilitates ComReg in actively monitoring trends, including but not limited to the type and occurrence of incidents and informs further investigation as required.

35. An incident report is provided to ENISA annually. A summary of the major incidents experienced during 2023 is outlined below.

Overview of incidents reported to ENISA

36. The main highlights of the 2023 Annual Summary Report to ENISA are as follows:

- There have been sixteen incidents, reported to ComReg in 2023, compared to twelve in 2022, with a total number of 22,818,885 User Hours lost;
- Of these incidents, there were four that were weather related, these included: the extended cold period of 09-10 March 2023; Storms Agnes; Betty; and Debbi. The overall number of User Hours lost to weather related security incidents amount to 4,675,138. These storms significantly impacted ECN and ECS during 2023, compared to the previous 2022 reporting period, that had none. This also goes some way to explaining the increase in reportable security incidents.
- A single security incident was of a malicious nature and involved a ransomware attack, in a third country. This affected a provider's Business Support Systems

[22] https://www.elicensing.comreg.ie/login.aspx .
[23] The guide to the new portal was published by ComReg as ComReg 19/98 and is expected to be updated during Q2 2024 to reflect the changes brought in under the Act of 2023 and due to advances in technology.

across several MS. ComReg staff note that the availability of the network concerned was not affected in Ireland.

37. That said, there were several security incidents that affected the availability of ECN and ECS over the past twelve months. The incident reports outline that the main causative factor of most security incidents is software related, be that faulty software or software bugs. This could be mitigated against by better testing of software along with improved escalation and roll-back procedures.

38. ComReg notes that mobile, radio and overhead copper networks tend to be more prone to the effects of adverse weather, (wind damage, ice, and heavy rain); while fixed underground plant tends generally to be more vulnerable to flooding, caused by storm surges and heavy rain. Such adverse effects can be usefully mitigated against by using equipment and enclosures that have an appropriate Ingress Protection ("IP") rating and maintenance of seals following repairs, in case of water ingress. In the case of mechanical damage to cables, adequate pruning of overhanging vegetation can mitigate against this.

39. ComReg notes, that these incidents have both an economic cost, in terms of the loss of services, impacting productivity and commerce; as well as a societal cost, limiting communications options for the citizens of the state. With the increase in remote working, this is a matter of growing importance. With this in mind, ComReg commissioned the Consultants DotEcon to provide a foundational report on the Economic and Societal Impacts of Network Incidents, see ComReg Document No. 23/59[24].

[24] The Economic and Societal Impacts of Network Incidents Study | Commission for Communications Regulation (comreg.ie)

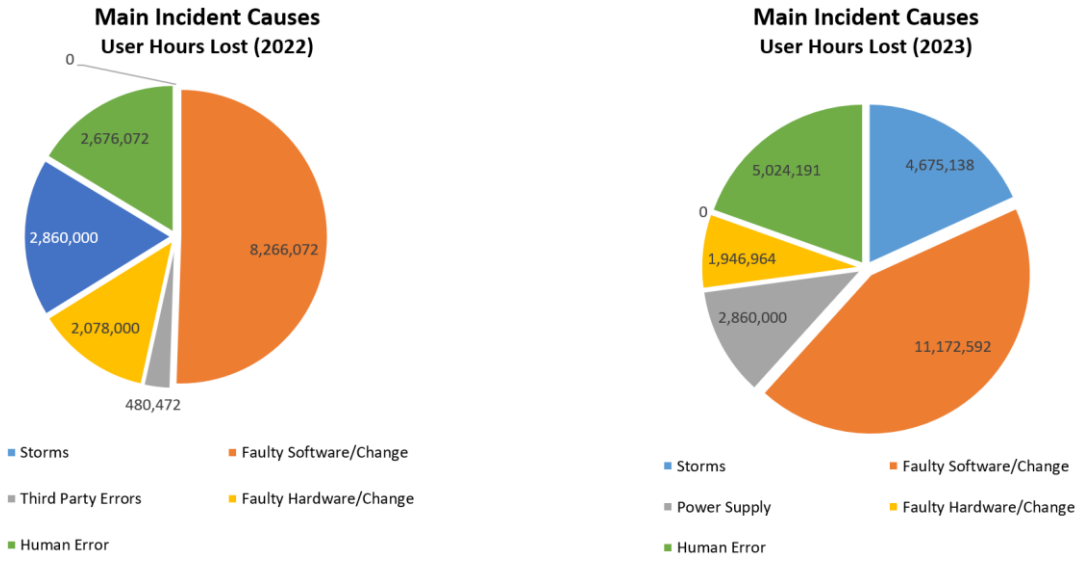

Figure 5: Comparison of security incidents reported to ComReg for 2022-2023

3.5 Storms, Other Natural Phenomena and their Effect on Resilience

40. During 2023, ComReg continued to monitor both weather and Space Weather[25] events that could affect the provision of ECN and ECS in Ireland.

41. This involves monitoring warnings that come from Met Éireann, using tools which rely upon data from the European Centre for Medium-Range Weather Forecasts ("ECMWF") model and from the US National Oceanic and Atmospheric Administration ("NOAA"). The latter can give advance warning of Atlantic storms originating as Atlantic Hurricanes and also gives warning of Space Weather Events. There were two major G4[26] Geomagnetic space weather events in March and April 2023, neither of which had any reported effects on ECN and ECS in Ireland.

42. If an orange-level warning or named storm is announced by Met Éireann, then ComReg monitors it as it develops and, where necessary, communicates with providers of national networks, and receives twice daily reports (six hours apart) from the operators concerned. This information is then passed on to the National Emergency Coordination Group ("NECG") and/or the DECC, as appropriate.

[25] In relation to Space Weather ComReg uses the tools offered by the NOAA and a useful information on Space Weather and its possible effects is here: https://www.swpc.noaa.gov/news/space-weather-educational-video

26 NOAA Space Weather Scales | NOAA / NWS Space Weather Prediction Center

43. Requests for assistance from providers are passed via the NECG to appropriate State agencies, to achieve a quicker resolution of any outage, than the operator could achieve without such assistance.

44. ComReg will continue to fulfil its obligation to report significant security incidents to both the Minister and ENISA pursuant to section 11 of the Act of 2023[27].

[27] From 9 June 2023 onwards.

Annex 1: Previous Obligations on Providers and Relevant ComReg Powers

A 1.1 Previous Obligations on Authorised Operators ("Undertakings")

45. Prior to its replacement by the European Electronic Communications Code (the "EECC") Regulations 23 and 24 of the Framework Regulations[28] were of particular relevance to ComReg's activities in this area. Current obligations on Undertakings are contained in Part 2 of the Act of 2023 which was commenced on June 9, 2023[29].

46. Regulation 23 required that an Undertaking that provided a "public communications network" or "publicly available electronic communications service" took appropriate technical and organisational measures to appropriately manage risks to the security of such network or service, having regard to the state of the art and ensuring a level of security appropriate to the risk. In addition, any undertaking providing a public communications network had to take appropriate steps to guarantee the integrity of that network.

47. Under Regulation 23, and in the event of a significant breach of security or integrity, the Undertaking concerned was obliged to notify ComReg, who in turn had to inform the Minister[30]. With the agreement of the Minister and where appropriate, ComReg had to advise the National Regulatory Authorities ("NRA") in other MS and the European Union Agency for Cybersecurity ("ENISA"). Where it was in the public interest, and again with the agreement of the Minister, ComReg could inform the public of a breach or require the Undertaking concerned to do so.

A 1.2 Previous ComReg Powers

48. Regulation 24 of the Framework Regulations set out the powers that were available to ComReg and provided that, for the purposes of Regulation 23, ComReg could issue a direction to an Undertaking requiring it to:

    a. provide information needed to assess the security or integrity of its network / services; and/or

[28] European Communities (Electronic Communications Networks and Services) (Framework) Regulations 2011 (S.I. 333/2011) ("the Framework Regulations")
[29] By means of the Communications Regulation and Digital Hub Development Agency (Amendment) Act 2023 (Commencement) (No. 2) Order 2023 (S.I. 299/2023).
[30] The Minister for the Department of the Environment, Climate and Communications.

b. submit to a security audit by a qualified independent body and to make the results available to ComReg.

49. These directions could also specify time limits for implementation and failure to comply with a direction was an offence.