Reference: 01874139

Information Requests
information.requests@ofcom.org.uk

28 August 2024

Freedom of Information request: Right to know request

Thank you for your request for information about cyber security breaches.

We received this request on 6 August 2024 and we have considered your request under the Freedom of Information Act 2000 ("the FOI Act").

Your request

"Under the Freedom of Information Act, I would like to request the following information:

How many cyber security breaches have been reported to Ofcom in the last five years, and how many of these cyber security breaches have threatened operational technology.

Please could you provide this data broken down for each of the last five full calendar years (2019-2023), or for the most recent five full calendar years for which you have data available."

Our response

There is no statutory definition for "Cyber security breaches".

Incidents falling within the category of "Cyber security breaches" which we think you may be referring to may be reported to us under several areas that we regulate including the Communications Act 2023 (as amended by the Telecommunications (Security) Act 2021) and the NIS Regulations 2018. Please note that under these specific regimes, there are different thresholds that need to be met for the providers to report incidents to us.

Again, neither of these two regimes refer to "cyber security breaches" nor separate these from any other types of reportable event:

- Under the NIS Regulations, 'any incident which has a significant impact on the continuity of the essential service which that OES provides', where "incident" means 'any event having an actual adverse effect on the security of network and information systems' is reportable to Ofcom.
- Similarly, under TSA, 'any security compromise that has' or 'that puts any person in a position to be able to bring about a further security compromise that would have a significant effect on the operation of the network or service' is reportable to Ofcom. "Security compromise" is broadly defined, and includes among other things 'anything that compromises the availability, performance or functionality of the network or service'.

Therefore, whilst some incidents that could be considered as "cyber security breaches" are likely to be among the total set of incidents that have been reported to us, it is not possible for us to reliably separate out those that would be from those that would not.

Accordingly, the remainder of this response relates to all incidents reported to us under these obligations, which will include, but not be limited to, those caused by what you may consider as "cyber security breaches".

Under the NIS Regulations, there has only been one incident reported in the last 5 years (please also see these previous FOI responses published here: Networks-and-systems-regulation-incidents.pdf and NIS-Regulations-Incidents.pdf

We publish a summary of incidents reported to us each year in our Connected Nations report pursuant to work we do under the Communications Act 2003.

You will find further information on this on our website, including on the following pages:

- https://www.ofcom.org.uk/__data/assets/pdf_file/0022/273721/connected-nations-2023-uk.pdf: Pages 61 to 62 in particular talk about cyber security compromises.
- Our network security and network resilience work is outlined in this document: https://www.ofcom.org.uk/phones-telecoms-and-internet/information-for-industry/network-security-and-resilience/our-work
- Page 56 of our Connected Nations report: Connected Nations 2022 - UK report
- Previous 6 years' Connected Nations reports can be found here: Connected Nations and infrastructure reports

The second part of your question asks "*how many of these cyber security breaches have threatened operational technology*". Incidents that are reportable to Ofcom under the two regimes are limited to those which have a 'significant impact on the continuity of the… service' or 'a significant effect on the operation of the network or service'. Given this, it is reasonable to conclude that most, if not all, of the incidents referred to in our answers above would have "threatened operational technology".

We hope this information is helpful. If you have any further queries, then please send them to information.requests@ofcom.org.uk – quoting the reference number above in any future communications.

Yours sincerely,

Information Requests

Request an internal review

If you are unhappy with the response you have received to your request for information, or think that your request was refused without a reason valid under the law, you may ask for an internal review. If you do, it will be subject to an independent review within Ofcom. We will either uphold the original decision, or reverse or modify it.

If you would like to ask us to carry out an internal review, you should get in touch within two months of the date of this letter. There is no statutory deadline for us to complete our internal review, and the time it takes will depend on the complexity of the request. But we will try to complete the review within 20 working days (or no more than 40 working days in exceptional cases) and keep you informed of our progress. Please email the Information Requests team (information.requests@ofcom.org.uk) to request an internal review.

Taking it further

If you are unhappy with the outcome of our internal review, then you have the right to complain to the Information Commissioner's Office.