Reference: 02182705

Information Requests
information.requests@ofcom.org.uk

6 May 2026

Dear,

Freedom of Information request: Right to know request

Thank you for your request for information concerning cyber security breaches from 2020 to 2026.

We received this request on 4 April 2026 and we have considered your request under the Freedom of Information Act 2000 ("the FOI Act").

Your request

I would like to request the following information for each calendar year from 2020 to 2026 inclusive:

1. The number of cyber security breaches that have being identified that were found to be a result of a malicious threat actor (i.e. not accidental data breach).

2. The breakdown in high-level causes of these breaches as identified by cyber security incident response teams (CSIRTs), for example (but not limited to) unpatched software/hardware, lack of multi-factor authentication (MFA), leaked user credentials, lack of in-transit encryption, etc.

3. The number of breaches that occurred that were attributed to a previously known vulnerability to the organisations hardware, software, policies, or processes, for example where system was known to be at risk due to being unpatched or out of support, or security controls were recommended but not enforced, and was defined within the resulting incident response report.

4. The estimated combined costs incurred as a result of cyber security breaches defined in request number one in each year.

Our response

We can confirm that we hold information in response to this request, however we are unable to disclose this information as we consider it is exempt from disclosure under Section 31(1)(a) of the FOI Act. This part of the act deals with information that, if disclosed would, or would be likely to, prejudice the prevention or detection of crime.

Section 31(1)(a) of the FOI Act is a qualified exemption which means that we have had to consider whether or not the public interest in disclosing the information you have requested outweighs the public interest in withholding the information. In this case, we consider the public interest favours withholding the information. The attached Annex A to this letter sets out the exemption in full, as well as the factors Ofcom considered when deciding where the public interest lay.

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.

<table>
<tr><th colspan="2">Section 31 (1) of the FOI Act provides that:
Information which is not exempt information by virtue of section 30 is exempt information if its disclosure under this Act would, or would be likely to, prejudice –
(a) the prevention or detection of crime;</th></tr>
<tr><th>Factors for disclosure</th><th>Factors for withholding</th></tr>
<tr><td>Disclosure would promote general transparency with the public in relation to areas and stakeholders we regulate.</td><td>We comply with relevant obligations in relation to reporting of incidents, and where we do communicate publicly in this area we are very careful to ensure that anything we say does not undermine our security measures
If the information is disclosed, it may enable individuals to learn about our security systems and where there may be loopholes to carry out a cyberattack.
The information requested can be analysed with other public information to create a mosaic effect and increase the chances of a more precise cyberattack.
Cyberattack is a criminal offence, by providing this information we would be aiding a malicious actor in committing a crime.</td></tr>
<tr><th colspan="2">Reasons why public interest favours withholding information</th></tr>
<tr><td colspan="2">Disclosing this information could cause harm and damage if disclosed. It can also undermine our security measures. Those negative consequences would be prejudicial to the prevention or detection of crime and contrary to a strong public interest.
We consider that, on balance, the public interest in withholding disclosure of the requested information outweighs the public interest in disclosing the information.</td></tr>
</table>