

Freedom of Information request: Reference number FOI2026/00395

Date of request: 4th April

Request:

Under the Freedom of Information Act, 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.*

No specific details are requested in relation to software/hardware utilisation, but rather high-level causes of breaches. I believe the high-level nature of this request does not allow for the use of s.31(1)(a) of the FOIA as this would not be likely to prejudice the security of your systems or data, as these are historical incidents which have since been dealt with. The public interest in understanding breach causes across public sector organisations outweighs the public interest in the exemption. I would like you to provide the information in Word, Excel, or CSV format. Please contact me if you need me to clarify my request.

Response:

We hold information within the scope of your request. However, we will not be providing this information.

We consider the requested information to be exempt under [Section 31 of the Freedom of Information Act 2000 \(law enforcement\)](#). The exemption applies as disclosure would, or would be likely to, prejudice the prevention or detection of crime.

The information you have requested relates to cyber security incidents, including the number of incidents, their causes and associated vulnerabilities. Even at a high level, this type of information would provide insight into our systems, areas of weakness, and how incidents have arisen. This could be used by individuals seeking to carry out malicious activity to better understand and target our systems.

We have considered your view that the information is high-level and relates to historic incidents. However, cyber risks and vulnerabilities are not limited to a single point in time, and patterns in how incidents occur can remain relevant. Disclosure of this information could therefore still increase the risk of future attacks.

We have also considered the public interest in disclosure. We recognise there is a general public interest in transparency and in understanding how public authorities manage cyber security risks. However,

there is a stronger public interest in ensuring that our systems and the information we hold are properly protected.

On balance, we consider that the public interest favours maintaining the exemption.

We have dealt with your request under the Freedom of Information Act 2000. For more information about this process please see the guidance we publish about making a request on our website:
<https://www.london-fire.gov.uk/about-us/transparency/request-information-from-us>