DE/2026-063– Freedom of Information Request

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.

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.

Department Response:

I refer to your request under the above legislation for information about cyber security breaches for each calendar year from 2020 to 2026 inclusive.

I wish to advise you that following a search of our records the information you have requested is not held by the Department. I have included your request below:

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

- 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

- 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.

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

As part of the transformation of the Northern Ireland Civil Service (NICS), IT provision including cyber security was centralised for all Departments under one body called Digital, Security & Financial Shared Services (DSF). This body is under the sponsorship of DoF. You can request further information from DSF via DoF at this email address - foi@finance-ni.gov.uk