Reference: 2026-033

Thank you for your email in which you requested the following information under the Freedom of Information Act 2000 (FOIA):

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.**

Response

The SFO neither confirms nor denies that it holds information relevant to your request, in accordance with section 24(2) of the FOIA.

Section 24(2) provides that:

The duty to confirm or deny does not arise if, or to the extent that, exemption from section 1(1)(a) is required for the purpose of safeguarding national security.

How the exemption is engaged

Confirming or denying whether the SFO holds the requested information would itself reveal information about the nature, frequency, and success of cyber attacks targeting the SFO. This would provide malicious actors with valuable insight into the SFO's cyber security position, including potential areas of vulnerability. Even a partial picture of the types of attacks that have or have not been attempted, or whether any were successful, could assist those seeking to target the SFO's systems, thereby increasing the risk of future attacks.

Public interest test

Section 24 is a qualified exemption, and we are therefore required to consider whether the public interest in maintaining the exclusion of the duty to confirm or deny outweighs the public interest in disclosing whether the information is held. More information about

exemptions in general and the public interest test is available on the ICO’s website at www.ico.org.uk.

The SFO recognises that cyber security is a matter of growing public concern, and that, as a publicly funded body, there is a legitimate public interest in transparency about how it manages its responsibilities.

Cyber attacks on government organisations can be costly and seriously damaging. Providing any assistance to those who may seek to target the SFO's systems would be contrary to the public interest and would undermine the SFO's ability to investigate and prosecute serious crime. As a government department operating on shared government IT infrastructure, information about the SFO's cyber security experience could also reveal, or allow inferences to be drawn about, the security posture of other government departments, thereby creating wider national security risks. This broader consideration is central to the application of section 24.

We further consider that the public interest in maintaining confidence in the security of government systems is not well served by confirming or denying whether this information is held. The SFO handles highly sensitive material relating to cases at pre-investigation, investigation, and prosecution stages, as well as beyond. Any disclosure that risks compromising the security of those systems would be detrimental to the administration of justice and could have serious consequences for the integrity of those investigations.

On balance, we are satisfied that the public interest in maintaining the exclusion of the duty to confirm or deny outweighs the public interest in disclosing whether the requested information is held.