

Ref: FOI2026-012

05 May 2026

Dear [REDACTED],

We refer to your request for the following information:

“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.”

Your request has been handled as a request for information under the Freedom of Information Act 2000 (the Act).

The Act provides applicants with two rights under section 1. These are:

- s.1(1)(a) The right to be told (in writing) whether the authority holds the information that has been requested, and
- s.1(1)(b) The right to have that information communicated to them.

The duty under s.1(1)(a) is referred to as the duty to confirm or deny. When responding to a request for information, it may be necessary for the authority to Neither Confirm Nor Deny (NCND) that it holds the information. AWE can neither confirm nor deny whether it holds the information you have requested.

In accordance with sections 24(2) and 26(3) of the Act, the duty to confirm or deny under section 1(1)(a) of the Act does not arise where confirmation or denial itself would disclose exempt information.

Section 24(2) of the Act provides an exemption from the duty to confirm or deny where confirmation or denial itself would be likely to prejudice national security.

AWE undertakes activities that are fundamental to the United Kingdom's national security. Confirming or denying whether information relating to cyber security incidents, causes, vulnerabilities, or associated remediation costs is held would inherently reveal information about the resilience, exposure, monitoring capability, and threat landscape of a national security organisation.

Even where information is requested at a high level, confirmation or denial could:

- Reveal whether AWE has experienced malicious cyber activity within a defined period;
- Allow hostile actors to infer the effectiveness of cyber security controls and monitoring arrangements;
- Assist adversaries in identifying patterns, trends, or perceived weaknesses over time; and
- Undermine protective security arrangements by indicating the scope and nature of information AWE records and analyses.

Such disclosures would increase the risk to national security by potentially enabling or facilitating hostile activity against critical defence and security infrastructure.

Section 26(3) of the Act exempts public authorities from confirming or denying whether information is held where doing so would be likely to prejudice the defence of the United Kingdom.

AWE's role in supporting the UK's nuclear deterrent and wider defence apparatus means that its cyber security posture is intrinsically linked to national defence interests. Confirmation or denial of whether cyber incidents, systemic vulnerabilities, or financial impacts have been recorded could:

- Reveal intelligence of value to hostile states or threat actors regarding UK defence resilience;
- Assist in targeting defence-related organisations or tailoring cyber-attack methodologies; and
- Prejudice the capability, effectiveness, and security of defence operations.

The exemption applies irrespective of whether the information requested is historic, aggregated, or high-level, as any confirmation or denial could contribute to a broader intelligence picture when combined with other publicly available material.

Both section 24 and section 26 are qualified exemptions, and AWE has therefore conducted a Public Interest Test (PIT), to determine whether the public interest favours confirming or denying whether the information is held.

In considering the public interest, AWE has recognised the general public interest in transparency and accountability in the operations of public sector bodies. The disclosure of the requested information could contribute to greater public understanding of cyber security risks, the causes of cyber incidents, and the way in which such incidents are addressed within public authorities. Disclosure may also support informed public debate regarding cyber resilience across the public sector and provide reassurance that malicious cyber incidents are appropriately identified and managed.

However, AWE has also identified strong public interest factors in favour of maintaining a neither confirm nor deny response. Confirming or denying whether the requested information is held would risk disclosures that could assist hostile actors and compromise national security. There is a significant public interest in safeguarding the United Kingdom's defence capabilities and preventing the gradual accumulation of sensitive intelligence that may arise through disclosure of seemingly harmless information over time. Maintaining an NCND position also protects the effectiveness of cyber security monitoring, incident response, and protective security measures, and reduces the risk of disclosures that could increase the likelihood or success of future attacks against defence-related infrastructure. Given AWE's unique role and operating environment, the need to protect national security and defence interests carries considerable weight.

Having carefully balanced these competing considerations, AWE has concluded that the public interest favours neither confirming nor denying whether the requested information is held. While openness and transparency remain important principles, they are outweighed in this instance by the overriding public interest in protecting the nation's security and defence positions.

If you are unhappy with the way your request has been handled you have a right to request an internal review within 40 days of receiving this letter, by writing to information.requests@awe.co.uk or our postal address: Information Requests Team, AWE Aldermaston, Reading, RG7 4PR. If you are still unhappy after an internal review has been completed, under the provisions of Section 50 of the Freedom of Information Act 2000 you have the right to take your complaint to the Information Commissioner's Office. Please note the Commissioner will generally not consider a complaint until you have exhausted AWE's internal complaints process.

Yours sincerely,

AWE Information Requests Team