Trade Remedies Authority
Premier House
60 Caversham Road
Reading
RG1 7EB

Ref: FoI 01 – 2026/27
Date: 21 April

Dear

Freedom of Information: Cyber Security Breaches

Thank you for your email of 4th April 2026 to the Trade Remedies Authority (TRA) in which you requested the following information:

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

The TRA considers that the information you are requesting is exempt from release under section 31(1)(a) and (3) of the Freedom of Information Act 2000.

Section 31(1)(a) says a public authority does not have to disclose information when doing so would or would likely prejudice the prevention or detection of crime. Section 31(3) allows an organisation to refuse to confirm or deny if it holds the requested information.

The TRA is mindful that disclosing information in response to a freedom of information request is essentially disclosure to the world at large. Placing such

information into the public domain would or would likely give cyber criminals insight into any potential vulnerabilities which may or may not exist and encourage a cyber-attack which is a criminal offence.

This approach is consistent with guidelines from the National Cyber Security Centre (NCSC), which highlights the need for organisations to carefully manage communications relating to cyber incidents and avoid disclosing information that could increase risk.

Threat actors routinely make use of publicly available information to profile and prioritise targets. Even high-level or aggregated information regarding cyber incidents, their causes, or associated control weaknesses can assist malicious actors in identifying patterns, assessing defensive maturity, and tailoring attack methods accordingly.

This type of activity is consistent with open-source intelligence (OSINT) techniques widely used in cyber-attacks, where seemingly low-sensitive information is combined with other data to build a more complete picture of an organisation's security posture.

As a government organisation, the TRA is a potential target for cyber criminals across the world. With emerging technologies, the environment within which the TRA operates, and the nature of its work, it is important that the TRA takes all appropriate steps to prevent cyber criminals from accessing its data.

Public interest test

As section 31 is a qualified exemption, the TRA has carried out a public interest test in considering its neither confirm nor deny response.

Public interest in disclosure:

- The public need to know that effective arrangements are in place to protect information
- Importance of transparency and openness so public authorities can be held accountable

Public interest in withholding:

- Revealing whether or not the TRA has been subject to cyber-attacks would disclose information about the effectiveness of its security controls. This could enable malicious actors to infer the likelihood of a successful attack, identify potential weaknesses, and tailor their methods, accordingly, thereby facilitating the commission of crime or hindering its detection. This risk would not be in the public interest.
- The TRA has a duty to maintain the integrity of personal information, in accordance with GDPR. Increasing the chances of an attack which could compromise this data, could lead to financial consequences. As a publicly funded authority, this could result in increased expenditure, ultimately funded by the taxpayer.
- Confirming or denying if the information is held could lead to an increased likelihood of interference from overseas organisations, and the disruption of the TRA’s core function. For example, confirmation of incidents may indicate

successful attack vectors, while confirmation of no incidents may suggest a perceived level of resilience that could attract more sophisticated targeting.

- Real-world cyber incidents demonstrate how knowledge of vulnerabilities or control weaknesses can be exploited by threat actors. For example, the WannaCry ransomware attack impacted organisations including the NHS where unpatched systems were widely exploited. Similarly, the breach of Equifax arose from a known but unpatched vulnerability, and the attack on Colonial Pipeline involved compromised credentials in the absence of multi-factor authentication (MFA). These examples illustrate how information relating to system weaknesses, even at a high level, can be leveraged to enable successful attacks.

On balance, the TRA concludes that the balance of public interest lies in upholding the exemption, and that subsection 3, neither confirm nor deny, is engaged.

Appeals procedure

If you are dissatisfied with the handling of your request, you have the right to ask for an internal review. Internal review requests should be submitted within two months of the date of receipt of the response to your original request and should be addressed to Knowledge and Information Management:

Knowledge and Information Management
Trade Remedies Authority
Premier House
60 Caversham Road
Reading
RG1 7EB

Email: InformationRights@traderemedies.gov.uk

Please remember to quote the reference number above in any future communications.

If you are not content with the outcome of the internal review, you have the right to apply directly to the Information Commissioner for a decision. The Information Commissioner can be contacted at: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

Yours sincerely,

Information Rights

Trade Remedies Authority

E: InformationRights@trade.remedies.gov.uk