20 April 2026 **FOI Ref 22738**

Request - You asked Staffordshire Police (SP) the following:

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.

SP received your request on 07/04/2026 and have processed this under the Freedom of Information Act (FOIA).

SP's response to your enquiry is as follows:

SP holds/does not hold the requested 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) **– Neither confirm nor deny, section 24 and 31.**

- 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 **– Neither confirm nor deny, section 24 and 31.**

- 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. **– Neither confirm nor deny, section 24 and 31.**

- 4.The estimated combined costs incurred as a result of cyber security breaches defined in request number one in each year. **– Neither confirm nor deny, section 24 and 31.**

The following exemption has been applied:

SP can neither confirm nor deny whether any information relevant to this request is held, as the duty in Section 1(1)(a) of the Freedom of Information Act 2000 does not apply by virtue of the following exemptions:

• Section 24 (2) National Security
Section 24 is a qualified exemption and as such there is a requirement to articulate the harm and conduct a test of the public interest.

• Section 31(3) Law Enforcement
Section 31 is a qualified and prejudice-based exemption and, as such, we are required to evidence the harm in disclosure and apply the public interest test

Harm:

To confirm or deny whether information is held in respect of cyber security breaches identified would provide actual knowledge that where an attempt has been made, it had been successful. Confirming that such information is not held may assist potential attackers by indicating that an attack had gone undetected. Equally, confirming information is held, especially at lower levels of detail, would enable understanding of where attacks have been successful and where possible weaknesses may exist. Attackers may then be able to tailor their methods to increase their chances of success.

Furthermore, in order to counter criminal and terrorist behaviour it is vital that the police and other agencies have the ability to work together, where necessary covertly, in order to obtain intelligence within current legislative frameworks to ensure the arrest and prosecution of offenders who commit or plan to commit acts of terrorism, whereby their modus operandi may involve cyber-attacks on secure databases. In order to achieve this goal, it is vitally important that information sharing takes place with other police forces and security bodies within the United Kingdom to support counter-terrorism measures in the fight to deprive terrorist networks of their ability to commit crime. To confirm or deny specific details of any breaches of information technology and security would be extremely useful to those involved in terrorist activity as it would enable them to map vulnerable information security databases.

Public Interest Test

Section 24(2) National Security

Factors in favour of confirming or denying that information is held

The public are entitled to know how public funds are spent and how resources are distributed within an area of policing. To confirm information is held regarding cyber breaches identified by the force would enable the general public to hold the police to account ensuring all such breaches are recorded and

investigated appropriately. With the call for transparency of public spending this would enable improved public debate.

Factors against confirming or denying that information is held

Security measures are put in place to protect the community we serve. As evidenced within the harm, to confirm or deny whether any information is held about identified cyber-breaches would highlight to terrorists and individuals' intent on carrying out criminal activity, vulnerabilities within the force which could be further exploited.

Taking into account the current security climate within the United Kingdom, no information (such as the citing of an exemption which confirms information pertinent to this request is held, or conversely, stating 'no information is held') which may aid a terrorist should be disclosed. To what extent this information may aid a terrorist is unknown, but it is clear that it will have an impact on a force's ability to monitor terrorist activity.

Irrespective of what information is or isn't held, the public entrust the Police Service to make appropriate decisions regarding their safety and protection and the only way of reducing risk is to be cautious with what is placed into the public domain.

The cumulative effect of terrorists gathering information from various sources would be even more impactive when linked to other information gathered from various sources about terrorism. The more information disclosed over time will give a more detailed account of the tactical infrastructure of not only a force area but also the country as a whole.

Any incident that results from such a disclosure would, by default, affect National Security.

Section 31 – Law Enforcement

Factors favouring confirming or denying that information is held

Confirmation that information exists relevant to this request would lead to a better-informed public which may encourage individuals to provide intelligence to reduce such cyber-security breaches.

Factors against confirming nor denying that information is held.

Confirmation or denial that information is held in this case would suggest the police take their responsibility to protect information and information systems from unauthorised access, destruction, etc., dismissively, and inappropriately.

Balancing Test

The points above highlight the merits of confirming or denying the requested information exists. The Police Service is charged with enforcing the law, preventing and detecting crime and protecting the communities we serve. As part of that policing purpose, information is gathered which can be highly sensitive relating to high profile investigative activity. Weakening the mechanisms used to monitor any type of criminal activity, and specifically terrorist activity would place the security of the country at an increased level of danger.

In addition, anything that places that confidence at risk, no matter how generic, would undermine any trust or confidence individuals have in the Police Service. Therefore, at this moment in time, it is SP's opinion that for these issues the balance test favours neither confirming nor denying that information is held.

Please note, SP are interpreting the wording of the question, i.e. cyber security "breach" to isolate only cyber security threats which have infiltrated police systems i.e. have been successful.

Please be advised that all Freedom of Information request responses are published on the SP website although personal details are not included.

Freedom of Information Request Appeals Procedure

1. **Who Can Ask for a Review**

Any person who has requested information from SP, which has been dealt with under the Freedom of Information Act, is entitled to complain and request an internal review, if they are dissatisfied with the response they received.

2. **How to Request a Review**

Requests for review of a Freedom of Information request must be made in writing within two months of the date of receipt of this email, and should be addressed to:

IAT@staffordshire.police.uk

Or by Post to:

Information Access Team
Staffordshire Police HQ
PO Box 3167
Stafford
ST16 9JZ

The reference number, date of the request and details of why the review is being requested must be included. Requests for review should be brought to the attention of the Information Access Team within two months of the Force's response to the original FOI request.

3. **Review Procedure**

Receipt of a request for review will be acknowledged in writing. The review will be conducted by a Supervisor who is independent from the original Decision Maker. The Information Access Team will set a target date for a response. The response will be made as soon as is practicable with the intention to complete the review within 20 working days. In more complex cases the review may take up to 40 working days.

The independent Supervisor will conduct a review of the handling of the request for information and of decisions taken, including decisions taken about where the public interest lies in respect of exempt information where applicable. The review enables a re-evaluation of the case, taking into account the matters raised by the complaint.

STAFFORDSHIRE POLICE

4. Conclusion of the Appeal

On completion of the review the Independent Supervisor will reply to the appellant with the result of the review. If the appellant is still dissatisfied following the review they should contact the Information Commissioner to make an appeal. The Information Commissioner can be contacted via the following link: https://ico.org.uk/make-a-complaint/foi-and-eir-complaints/foi-and-eir-complaints/

Freedom of Information
Information Access Team