18 October 2024 **FOI Ref 17291**

Request - You asked us the following:

Under the Freedom of Information Act 2000, I kindly request the following information regarding cybersecurity breaches or hacks experienced by your police force over the past three years (from 1st January 2020 to the present):

1. A chronological list of all cybersecurity breaches or hacks that have occurred within the specified time frame.
2. For each incident, please provide:
   - o Date of the breach/hack
   - o A brief description of the nature of the breach/hack
   - o Impact on operations, including any data compromised
   - o Measures taken to address the breach/hack and prevent future incidents

If providing specific details is not possible due to exemptions under the Act, please supply as much information as permissible, citing the applicable exemptions for any withheld details.

I would prefer to receive the information in electronic format via email (please reply to this email address)

I appreciate your time and assistance with this request. Please acknowledge receipt of this email, and I look forward to your response within the statutory 20 working days.

We received your request on 25/09/2024 and have processed this under the Freedom of Information Act (FOIA).

Staffordshire Police's response to your enquiry is as follows:

Staffordshire Police can neither confirm nor deny whether 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:

In accordance with Section 17(1) of the Freedom of Information Act, this letter represents a refusal notice for this particular request.

- Section 24(2) – National Security
- Section 31(3) - Law Enforcement

Sections 24 and 31 are prejudice based qualified exemptions and there is a requirement to articulate the harm that would be caused in confirming or not whether information is held as well as considering the public interest.

Harm

To confirm or deny whether information is held in respect of successful cyber-attacks would provide actual knowledge that where an attempt has been made, it has or has not 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 would enable understanding of where attacks have been

successful, and possible weaknesses 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 in order 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 successful cyber-attacks would enable the general public to hold Staffordshire 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 whether any cyber-attacks have been successful would highlight to terrorists and individuals intent on carrying out criminal activity vulnerabilities within Staffordshire Police 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 with regard to 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 impactful 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 (3) 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 in order to reduce such security breaches.

Factors against confirming nor denying that information is held

Confirmation or denial that information is held in this case would suggest Staffordshire Police take their responsibility to protect information and information systems from unauthorised access, destruction, etc., dismissively and inappropriately. Confirmation or denial that information is held would both inform and assist offenders, in turn adversely affect Staffordshire Police's ability to prevent and detect crime and apprehend and prosecute offenders. This is not in the public interest.

Balance 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 our opinion that for these issues the balance test favours neither confirming nor denying that information is held.

Please note that we have interpreted your request to be referring to the number of successful cyber-security breaches Staffordshire Police may or may not have experienced.

Next steps

You can ask us to review our response.

If you would like us to carry out a review of our response, please let us know within two months of the date of receipt of this email, review requests should be addressed to:

foi@staffordshire.police.uk

Or by Post to:

Central Disclosure Unit
Staffordshire Police HQ
PO Box 3167
Stafford
ST16 9JZ

STAFFORDSHIRE POLICE

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

Freedom of Information
Central Disclosure Unit