



Your reference: n/a

Our reference: FOI_24_0338

E-mail: FOI

@gloucestershire.police.uk

Direct dial: 01452 754304

Postal Address: As above

Date: 22/04/2024

Dear

Gloucestershire Constabulary Freedom of Information request FOI_24_0338

On 22/03/2024 you sent an email constituting a request under the Freedom of Information Act asking the following:

I am writing to politely request the following data under the terms of the Freedom of Information Act 2000 (FOIA) on cyber attacks affecting Gloucestershire Constabulary. Where possible please provide data broken down by calendar year or failing that, by relevant 12-month period (e.g. 2021/22 2022/23 etc.) for which data is available.

1. How many times has your organisation experienced an attempted cyber-attack in the last two financial years?
2. Have you ever reported any cyber-related incidents to the NCSC and if so, how many in the last two financial years?
3. Thinking about cyber-attacks where the criminal was able to obtain data or disable systems, how much have these cost the organisation?
4. How much of the organisation's total annual budget is spent on cyber support, protection and computer systems?
5. How many people are employed by the organisation to oversee cyber support and programmes?

With regard to questions 1, 2 and 3:

Section 1 of the Freedom of Information Act 2000 (FOIA) places two duties on public authorities. Unless exemptions apply, the first duty at Section 1(1)(a) is to confirm or deny whether the information specified in a request is held. The second duty at Section 1(1)(b) is to disclose information that has been confirmed as being held. Where exemptions are relied upon s17 of FOIA requires that we provide the applicant with a notice which: a)

states that fact b) specifies the exemption(s) in question and c) states (if that would not otherwise be apparent) why the exemption applies.

Gloucestershire Constabulary can neither confirm nor deny that it holds any information in relation to systems used for intelligence purposes 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 23(5) Information supplied by, or concerning certain security bodies
Section 24(2) National Security
Section 31(3) Law enforcement;

Section 23 is an absolute, class based exemption and therefore neither a harm test nor a public interest test.

Section 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 that the information is held as well as carrying out a public interest test.

Harm in Confirming or Denying that Information is held

To confirm or deny whether any information is held in respect of successful or attempted cyber-attacks resulting in Data Breaches would provide actual knowledge of where an attempt has been made, it if 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.

To confirm or deny whether information is held in respect of any leaked data as a result of an attack would, in effect, confirm that there had been successful cyber-attacks made against the force, which would present harm as detailed above.

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 Considerations

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 causing Data Breaches 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 whether any cyber-attacks have been successful would highlight to terrorists and individuals intent on carrying out criminal activity vulnerabilities within the 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 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 our opinion that for these issues the balance test favours neither confirming nor denying that information is held.

With regard to questions 4 and 5:

Under the Freedom of Information Act 2000 s1, I can confirm that Gloucestershire Constabulary holds some relevant information.

Section 17 of the Freedom of Information Act 2000 requires Gloucestershire Constabulary, when refusing to provide information (because the information is exempt) to provide you the applicant with a notice which: (a) states the fact, (b) specifies the exemption in question and (c) states (if not otherwise apparent) why the exemption applies.

The following exemptions apply:

Section 24(1) – National Security
Section 31(1) – Law Enforcement

The exemptions above are qualified and prejudice based therefore both a Public Interest Test and Harm Test are required.

Harm Test

Modern-day policing is intelligence led, and intelligence changes on a day-by-day basis. Disclosures under the Freedom of Information Act are disclosures to the world, not just to the individual making the request.

Any response that has the potential to undermine ongoing and future operations to protect the security of the United Kingdom would significantly increase the risk of harm to the community at large.

Whilst the release of information regarding the total annual cyber security budget for a particular department does not pose a cyber-security risk in and of itself, it may allow requesters to deduce sensitive information regarding the forces expenditure and as such should be withheld. If it was to show limited investment this could provide an indication of the departments lack of understanding of cyber security threats.

Similarly confirming the number of people who oversee cyber support would provide an indication of the Constabulary's understanding of cyber security threat, risk appetite and activity. If this was considered low or high it could indicate to offenders whether their current endeavours are working or where they should concentrate their efforts if mapping this information over the whole country.

Any such assistance by providing this information to those intent on criminal activity would only serve to increase the risk of harm to the public.

Public Interest Test

Section 24

Factors favouring disclosure

Confirming the budget and number of staff involved in this area of policing for Gloucestershire Constabulary which could also safeguard matters of national security would improve public confidence in the work of the police and reassure them that they are adequately resourced.

Factors against disclosure

It is not in the public interest to disclose the capabilities of the police service and other UK authorities and the intelligence held that may be used to safeguard the country. As detailed in the harm above, confirming the budget and number of staff involved in this area of policing would provide assistance to those intent on disrupting the police service.

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

Section 31

Factors favouring disclosure

Confirming this information would satisfy the public need to know how well the Constabulary is equipped to deal with cyber security. It would also show how public funds are being used to fight crime.

Factors against disclosure

Confirming the budget and number of people involved in cyber security for the Constabulary would highlight whether this area of policing is potentially under or over-funded. This would provide useful intelligence to those intent on disrupting the police service as to where they should focus their efforts. This would clearly affect the safety of the public and therefore any such disclosure would put the public at risk.

If this information were mapped across the country this would also provide useful intelligence to criminals as which forces may be more or less funded and would allow them to target specific forces.

Balance Test

Whilst there is public interest in disclosing the requested information which would provide reassurance to the public that the Police Service are appropriately funded and equipped to deal with such offences, there is a stronger public interest in safeguarding national security.

The Police Service is charged with enforcing the law, preventing and detecting crime and protecting the communities we serve. Any disclosure of information that could adversely affect this purpose would by its very nature put the public at risk.

It is for this reason, the balance test for or against disclosure favours non-disclosure.

If you are not satisfied with this response or any actions taken in dealing with your request, you have the right to ask that we review your case under our internal procedure. Please note that a request for an internal review must be made within 20 working days of the response to your original request.

If you decide to request that such a review is undertaken and following this process you are still unsatisfied, you then have the right to direct your complaint to the Information Commissioner for consideration.

The Information Commissioner can be contacted via the following means:

Website - <https://ico.org.uk/>

Call their helpline - 0303 123 1113

Email - casework@ico.org.uk

Post –

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

Yours sincerely,

Disclosure Officer
Gloucestershire Constabulary