



**HEDDLU  
GOGLEDD CYMRU  
NORTH WALES  
POLICE**

Response Date: 15/04/2024

### **2024/333 - Cyber Security**

In response to your recent request for information regarding;

**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?**

North Wales Police can neither confirm nor deny whether we hold any further information in relation to your request as the duty in Section 1(1)(a) of the Freedom of Information Act 2000 (the Act) does not apply by virtue of the following exemptions:

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

#### **Harm in Confirming or Denying that Information is held**

To confirm or deny whether any further 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, 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.

## **2. Have you ever reported any cyber-related incidents to the NCSC and if so, how many in the last two financial years?**

Please see the answer the question 1 and in addition;

North Wales Police can neither confirm nor deny that it holds any other information with regard to an exempt body 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 23 is a class based absolute exemption and there is no requirement to consider the public interest in this case.

Confirming or denying the existence of whether any other information is held would contravene the constrictions laid out within Section 23 in that this stipulates a generic bar on disclosure of any information applied by, or concerning, certain Security Bodies.

Therefore, in accordance with the Freedom of Information Act 2000, this letter acts as a Refusal Notice under section 17 (1) of the legislation.

**3. Thinking about cyber-attacks where the criminal was able to obtain data or disable systems, how much have these cost the organisation?**

Please see the answer the question 1

**4. How much of the organisation's total annual budget is spent on cyber support, protection and computer systems?**

We do not hold a budget for cyber support and protection. These services and solutions are included in broader contracts and agreements covering more than cyber security.

**5. How many people are employed by the organisation to oversee cyber support and programmes?**

Concerns have been raised in relation to disclosing the number of people who oversee cyber support and programmes. Therefore, a Public Interest Test has been carried out to weigh up the reasons for and against disclosure; to ensure the release is in the interest of the public as a whole and not just the applicant.

The Public Interest Test has considered the following exemptions;

Section 24(1) National Security

Section 31(1) Law Enforcement

Sections 24 and 31 being prejudice based qualified exemptions, both evidence of harm and public interest considerations need to be articulated to the applicant.

**Evidence of Harm**

Any disclosure under FOI is a release to the public at large. Whilst not questioning the motives of the applicant, to disclose how many people are employed by North Wales Police to oversee cyber support and programmes into the public domain as a provide an indication of departments understanding of cyber security threat, risk appetite and activity and could leave a department vulnerable to attack if there is limited resources.

## **Public Interest Considerations**

### **Section 24(1) National Security**

#### Factors favouring disclosure

The public are entitled to know how public funds are spent and how resources are distributed within an area of policing. To disclose information regarding how many people are employed by the organisation to oversee cyber support would show our commitment to stop cyber attacks and our capability of that.

#### Factors against disclosure

Security measures are put in place to protect the community we serve. As evidenced within the harm to disclose information held would highlight to terrorists and individuals intent on carrying out criminal activity capabilities/vulnerabilities within North Wales Police.

Taking into account the current security climate within the United Kingdom, disclosure of such information may aid terrorist activity. 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(1) Law Enforcement**

#### Factors favouring disclosure:

Disclosing information relevant to this request would lead to a better informed public which may encourage individuals to provide intelligence in order to reduce the risk of attacks .

#### Factors against disclosure:

Disclosing information in this case would effect North Wales Police ability to protect its systems and information.

### **Balancing Test**

The points above highlight the merits of non-disclosure regarding requested information. 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.

Disclosing our capability and resources in a particular area specifically cyber support can provide data to criminals, specifically those involved in terrorist activity and would place the security of the country at an increased level of danger.

Anything that places 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 non disclosure.

Therefore, in accordance with the Freedom of Information Act 2000, this letter acts as a Refusal Notice under section 17 (1) of the legislation

THIS INFORMATION HAS BEEN PROVIDED IN RESPONSE TO A REQUEST  
UNDER THE FREEDOM OF INFORMATION ACT 2000, AND IS CORRECT AS AT 11/04/2024