Request Reference: 1038A/21

2. How many cyber attacks (that the department is aware of) have successfully breached the force's defences?

3. To the best of the force's knowledge, has any data been leaked online as a result of the attacks?

4. Has that data included personal data from people who've interacted with the police?

Applicable 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 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.

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 would enable the general public to hold West Midlands 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 above, to confirm whether any cyber attacks have been successful would highlight to terrorists and individuals intent on carrying out criminal activity vulnerabilities within West Midlands 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 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(3) – Law enforcement

Factors in favour of 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 or denying that information is held:

Confirmation or denial that information is held in this case would suggest West Midlands 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 my opinion that for these issues the balance test favours neither confirming nor denying that information is held.