Request Reference: 1267A/21

West Midlands police can neither confirm nor deny that information is held relevant to your request 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 31 (3) Law Enforcement

Sections 24 and 31 being prejudice based qualified exemptions 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 in confirming or denying that information is held

To confirm or deny whether a cyber-crime has been successful and provide further information relating to such attacks would allow criminals to understand weaknesses within forces would identify vulnerable computer systems and provide actual knowledge, or not, that these incidents have taken place. 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 criminal activities. 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 any specific details of breaches of information technology, security and vulnerabilities in technology would be extremely useful to those involved in terrorist activity as it would enable them to map vulnerable information security databases.

Confirming or denying that attacks have been successful would assist potential attackers by indicating that an attack had gone undetected. By understanding where attacks have been successful, and possible weaknesses exist, attackers may be able tailor their methods to increase the chance of success. This would increase the risk of successful attacks on police forces IT infrastructure which would ultimately prevent the force from undertaking its primary function of preventing and detecting crime and apprehending offenders.

Confirming or denying information was held in relation to how forces may or may not have investigated and acted upon successful attacks would provide valuable information to attackers about the success of any such attacks and further, how forces have specifically investigated and dealt with such attacks.

Public Interest Considerations
Section 24 (2) National Security - Factors favouring complying with Section 1 (1) (a) confirming 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 where information security breaches have occurred or to highlight vulnerabilities would enable the general public to hold West Midlands Police to account ensuring all such breaches are recorded and investigated appropriately. In the current financial climate of cuts and with the call for transparency of public spending this would enable improved public debate.

Section 24 (2) National Security - Factors against complying with Section 1 (1) (a) confirming or denying that any other information is held.

Security measures are put in place to protect the community that we serve. As evidenced within the harm to confirm where specific breaches have occurred or vulnerable systems are in place would highlight to terrorists and individuals intent on carrying out criminal activities vulnerabilities within West Midlands Police. 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 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 the forces 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 worrying 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 the force area but also the country as a whole. Any incident that results from such a disclosure would by default effect National Security.

Section 31 Law Enforcement – Factors favouring complying with Section 1 (1) (a) confirming 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.

Section 31 Law Enforcement – Factors against complying with Section 1 (1) (a) neither confirm nor 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. The construction of a mosaic picture of vulnerable areas could also occur.

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 order to comply with statutory requirements and to meet NPCC expectation of the Police Service regarding the management of information security a national policy approved by the College of Policing titled National Policing Community Security Policy has been put in place. This policy has been constructed to ensure the delivery of core operational policing providing appropriate and consistent protection for the information assets of member organisations. A copy of this can be found at the below link:

http://library.college.police.uk/docs/APP-Community-Security-Policy-2014.pdf

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.