Freedom of Information Request Reference N^{o}: FOI 005269-17

I write in connection with your request for information received by Suffolk Constabulary on the 9 June 2017 in which you sought access to the following information:

1. *"Does your organisation install anti-virus software or endpoint protection on network devices?*

    a. *Yes*
    b. *No*

2. *Has your organisation suffered a ransomware attack in the last 12 months, in which an external hacker encrypted a PC or device or network within your organisation and demanded payment in order to decrypt the device?*

    a. *Yes*
    b. *No*

3. *If yes, In the past 12 months, how many ransomware attacks has your organisation had to defend against?*

    a. *1-2 attacks*
    b. *3-4 attacks*
    c. *5-6 attacks*
    d. *7-8 attacks*
    e. *9-10 attacks*
    f. *More than 10 attacks (please specify)*

4. *Do you know how the ransomware attacker gained access to your organisation's network?*

    a. *Phishing via email or social media network*
    b. *Drive-by-download caused by clicking on a compromised website*
    c. *Infection via a computer that was part of a botnet*
    d. *Other (please specify)*

5. *How far did the most successful ransomware attack get when targeting your organisation's data?*

    a. *The attacker was unable to successfully encrypt any files/data*
    b. *The attacker was able to encrypt some files/data*

6. *What type of data has been affected by ransomware attackers in the past 12 months?*

    a. *Employee information*
    b. *Inmate information*
    c. *Payroll/HR*

d. Financial data
e. All data was targeted

7. *Of the ransomware attacks your organisation has experienced in the last 12 months, has your organisation paid the ransom demanded?*

   a. Yes, my organisation paid the ransom every time
   b. Yes, my organisation has paid some ransoms but not all
   c. No ransom was paid

8. *Has your organisation been able to identify the attacker in any of the ransomware attacks on your organisation, and if so who was the attacker?*

   a. Organised cyber-criminals
   b. Opportunistic hackers (non-organised)
   c. Political hacktivists
   d. Disgruntled employees/former employees
   e. State sponsored hackers
   f. Other (please specify)

9. *Was your organization hit by the WannaCry ransomware attack in May 2017?*

   a. Yes
   b. No"

Response to your Request

The response provided below is correct as of 2 June 2017.

Norfolk and Suffolk Constabularies have considered your request for information and our response is below.

1. Yes

2 - 9

Norfolk and Suffolk Constabularies can neither confirm nor deny whether 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 23(5) Information supplied by or concerning certain Security Bodies**
- **Section 24(2) National Security**
- **Section 30(3) Investigations**
- **Section 31(3) Law Enforcement**

Section 23 is a class based absolute exemption and there is no requirement to consider the public interest.

Section 30 is a class based qualified exemption which requires a public interest to determine if neither confirming nor denying whether information is held, is the appropriate response.

Sections 24 and 31 are prejudice based qualified exemptions, this means that both the evidence of harm and the public interest test needs to be articulated.

Evidence of Harm

Policing is an information-led activity, and information assurance (which includes information security) is fundamental to how the Police Service manages the challenges faced. In order to comply with statutory requirements, the College of Policing Authorised Professional Practice (APP) for Information Assurance, has been put in place to ensure the delivery of core operational policing by providing appropriate and consistent protection for the information assets of member organisations, see link below:-

https://www.app.college.police.uk/app-content/information-management/

To confirm or deny whether any ransomware attacks have occurred would identify vulnerable computer systems and provide actual knowledge, or not, whether these incidents have taken place within individual force areas.

It is vitally important that information sharing takes place with other police forces and security bodies within the UK 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 ransomware attacks would be extremely useful to those involved in terrorist activity as it would enable those involved in such activity to map any vulnerability.

Public Interest Test

Section 24 – factors favouring confirmation or denial of whether 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 whether any ransomware attacks have occurred would enable the general public to hold Norfolk and Suffolk Constabularies to account, ensuring that 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 – factors against confirmation or denial of whether information is held

Security measures are put in place to protect the communities we serve. As evidenced within the harm, to confirm where ransomware attacks have occurred would highlight to those involved in criminal and terrorist activity, vulnerabilities within Norfolk and Suffolk Constabularies.

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 entrusts 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 information 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 30 – factors favouring confirmation or denial of whether information is held
Confirming or denying whether information exists relevant to this request would lead to a better informed general public by identifying that Norfolk and Suffolk Constabularies robustly investigate ransomware attacks. This fact alone may encourage individuals to provide intelligence in order to assist with investigations and would also promote public trust in providing transparency and demonstrating openness and accountability into where the police are currently focusing their investigations.

The public are also entitled to know how public funds are spent, particularly in the current economic climate.

Section 30 – factors against confirmation or denial of whether information is held
Modern-day policing is intelligence led and Norfolk and Suffolk Constabularies share information with other law enforcement agencies as part of their investigation process. To confirm or not whether Norfolk and Suffolk Constabularies has alerted other agencies of ransomware attacks could hinder the prevention and detection of crime, as well as undermine the partnership approach to investigations and enforcement.

Should offenders take evasive action to avoid detection, police resources may well be diverted from frontline duties and other areas of policing in order to locate and apprehend these individuals. In addition, the safety of individuals and victims would also be compromised.

Section 31 – factors favouring confirmation or denial of whether information is held
Confirming 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 these attacks.

Section 31 – factors against confirmation or denial of whether information is held
Confirmation or denial of whether information exists in this case would suggest that Norfolk and Suffolk Constabularies take their responsibility to protect information and information systems from unauthorised access, destruction, etc, dismissively and inappropriately.

Balance Test

The points above highlight the merits of confirming or denying whether 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 the NPCC expectation of the Police Service, with regard to 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 by providing appropriate and consistent protection for the information assets of member organisations. A copy of this can be accessed via 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 our opinion that for these reasons the balance test favours neither confirming nor denying whether information is held.

No inference should be taken from this response as to whether information does or does not exist.

Should you have any further queries concerning this request, please contact Clair Pack, FOI Decision Maker, quoting the reference number shown above.

A full copy of the Freedom of Information Act (2000) can be viewed on the 'Office of Public Sector Information' web-site;
http://www.opsi.gov.uk/

Norfolk and Suffolk Constabularies are not responsible for the content, or the reliability, of the website referenced. The Constabulary cannot guarantee that this link will work all of the time, and we have no control over the availability of the linked pages.

Your Right to Request a Review of Decisions Made Under the Terms of the Freedom of Information Act (2000).

If you are unhappy with how your request has been handled, or if you think the decision is incorrect, you have the right to ask the Norfolk and Suffolk Constabulary to review their decision.

Ask Norfolk and Suffolk Constabularies to look at the decision again.

If you are dissatisfied with the decision made by Norfolk and Suffolk Constabularies under the Freedom of Information Act (2000), regarding access to information, you must notify the Norfolk and Suffolk Constabulary that you are requesting a review within 20 days of the date of its response to your Freedom of Information request. Requests for a review should be made in writing and addressed to:

Freedom of Information Decision Maker
Information Management Department
Suffolk Constabulary
Police Headquarters
Martlesham Heath
Ipswich
Suffolk
IP5 3QS
OR
Email: information@suffolk.pnn.police.uk

In all possible circumstances Norfolk and Suffolk Constabulary will aim to respond to your request for us to look at our decision again within 20 working days of receipt of your request for an internal review.

The Information Commissioner.

After lodging a request for a review with Norfolk and Suffolk Constabulary, if you are still dissatisfied with the decision, you can apply to the Information Commissioner for a decision on whether the request for information has been dealt with in accordance with the requirements of the Act.

For information on how to make application to the Information Commissioner please visit their website at www.ico.org.uk or contact them at the address shown below:

The Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF
Telephone: 01625 545 700