WILTSHIRE POLICE

Force Disclosure Unit
Wiltshire Police HQ
London Road
Devizes
Wiltshire
SN10 2DN
Tel 101 ext 62005
www.wiltshire.police.uk
disclosure@wiltshire.pnn.police.uk

Date: 24th September 2021 Your ref: FOI Our ref: FOI 2021 / 710

Reply contact name is: Kerry Merritt

Dear ****,

I write in connection with your request for information dated 31st August 2021 concerning Ransomware incidents.

I am required by the Freedom of Information Act 2000 to handle all requests in a manner that is blind as to the identity and motives of the requestor. Any information released as a response to a request is regarded as being published and therefore in the public domain without caveat.

Your request for information has now been considered and it is not possible to meet your request in full.

You wrote:

1. In the past three years has your organisation:
a. Had any ransomware incidents? (An incident where an attacker attempted to, or successfully, encrypted a computing device within your organisation with the aim of extorting a payment or action in order to decrypt the device?)
i. If yes, how many?
b. Had any data rendered permanently inaccessible by a ransomware incident (i.e. some data was not able to be restored from back up.)
c. Had any data rendered permanently inaccessible by a systems or equipment failure (i.e. some data was not able to be restored from back up.)
d. Paid a ransom due to a ransomware incident / to obtain a decryption key or tool?
i. If yes was the decryption successful, with all files recovered?
e. Used a free decryption key or tool (e.g. from https://www.nomoreransom.org/)?
i. If yes was the decryption successful, with all files recovered?
f. Had a formal policy on ransomware payment?
i. If yes please provide, or link, to all versions relevant to the 3 year period.
g. Held meetings where policy on paying ransomware was discussed?
h. Paid consultancy fees for malware, ransomware, or system intrusion investigation
i. If yes at what cost in each year?
i. Used existing support contracts for malware, ransomware, or system intrusion investigation?
j. Requested central government support for malware, ransomware, or system intrusion investigation?
k. Paid for data recovery services?

i. If yes at what cost in each year?
l. Used existing contracts for data recovery services?
m. Replaced IT infrastructure such as servers that have been compromised by malware?
i. If yes at what cost in each year?
n. Replaced IT endpoints such as PCs, Laptops, Mobile devices that have been compromised by malware?
i. If yes at what cost in each year?
o. Lost data due to portable electronic devices being mislaid, lost or destroyed?
i. If yes how many incidents in each year?

2. Does your organisation use a cloud based office suite system such as Google Workspace (Formerly G Suite) or Microsoft's Office 365?
a. If yes is this system's data independently backed up, separately from that platform's own tools?

3. Is an offsite data back-up a system in place for the following? (Offsite backup is the replication of the data to a server which is separated geographically from the system's normal operating location site.)
a. Mobile devices such as phones and tablet computers
b. Desktop and laptop computers
c. Virtual desktops
d. Servers on premise
e. Co-located or hosted servers
f. Cloud hosted servers
g. Virtual machines
h. Data in SaaS applications
i. ERP / finance system
j. We do not use any offsite back-up systems

4. Are the services in question 3 backed up by a single system or are multiple systems used?

5. Do you have a cloud migration strategy? If so is there specific budget allocated to this?

6. How many Software as a Services (SaaS) applications are in place within your organisation?
a. How many have been adopted since January 2020?

Our response:

1. In the past three years has your organisation:

a. Had any ransomware incidents? (An incident where an attacker attempted to, or successfully, encrypted a computing device within your organisation with the aim of extorting a payment or action in order to decrypt the device?) **None**

For your questions namely b), c), d), dI), e), eI), f), fi), g), h), hI), hII), j), k), kI), kII), m), n) Wiltshire 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 Wiltshire 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 individual's intent on carrying out criminal activities vulnerabilities within Wiltshire 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 Wiltshire 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

o. Lost data due to portable electronic devices being mislaid, lost or destroyed? **No**

i. If yes how many incidents in each year? **N/A**

2. Does your organisation use a cloud based office suite system such as Google Workspace (Formerly G Suite) or Microsoft's Office 365? **Yes**

a. If yes is this system's data independently backed up, separately from that platform's own tools? **No**

3. Is an offsite data back-up a system in place for the following? (Offsite backup is the replication of the data to a server which is separated geographically from the system's normal operating location site.)

a. Mobile devices such as phones and tablet computers **Intune**
b. Desktop and laptop computers **Yes, to Microsoft Cloud services**
c. Virtual desktops **N/A**
d. Servers on premise **Yes, to a secondary site**
e. Co-located or hosted servers **Yes, to a secondary site**
f. Cloud hosted servers **No**

g. Virtual machines **Yes, to a secondary site**
h. Data in SaaS applications **Yes, for some SaaS systems.**
i. ERP / finance system **Backed up by provider.**
j. We do not use any offsite back-up systems

4. Are the services in question 3 backed up by a single system or are multiple systems used? **Multiple systems**

5. Do you have a cloud migration strategy? **Yes** If so is there specific budget allocated to this? **No**

6. How many Software as a Services (SaaS) applications are in place within your organisation? **5**
a. How many have been adopted since January 2020? **3**

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

The exemption applicable to the information requested is:

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

In accordance with section 17 of the Act, this letter represents a Refusal Notice for this particular request.

I am satisfied that all the relevant information has been passed to me and been considered in the light of your request within the time constraints applicable under the legislation.

Wiltshire Police would like to thank you for the interest that you have shown in the Force.

Yours sincerely,

Kerry Merritt
Disclosure Decision Maker

Wiltshire Police offers a re-examination of your case under its review procedure.

Force Disclosure Unit
Wiltshire Police HQ, London Road, Devizes, Wiltshire SN10 2DN
Telephone 101 ext 62005

Freedom of Information Request Appeals Procedure

1. Who Can Ask for a Review

Any person who has requested information from Wiltshire Police, which has been dealt with under the Freedom of Information Act, is entitled to complain and request an internal review, if they are dissatisfied with the response they received.

2. How to Request a Review

Requests for review of a Freedom of Information request must be made in writing to the:
Force Disclosure Unit
Wiltshire Police Headquarters,
London Road, Devizes,
Wiltshire,
SN10 2DN

Email at disclosure@wiltshire.pnn.police.uk.

The reference number, date of the request and details of why the review is being requested must be included. Requests for review should be brought to the attention of the Force Disclosure Unit within 20 working days of the Force's response to the original FoI request.

3. Review Procedure

Receipt of a request for review will be acknowledged in writing to include confirmation of the reasons for the review. The review will be conducted by another Decision Maker, who is independent from the original Decision Maker. The Force Disclosure Unit will set a target date for a response. The response will be made as soon as is practicable with the intention to complete the review within twenty working days. In more complex cases the review may take up to 40 working days.

The Independent Decision Maker will conduct a review of the handling of the request for information and of decisions taken, including decisions taken about where the public interest lies in respect of exempt information where applicable. The review enables a re-evaluation of the case, taking into account the matters raised by the complaint.

4. Conclusion of the Appeal

On completion of the review the Independent Decision Maker will reply to the complainant with the result of the review. If the complainant is still dissatisfied following the review they should contact the Information Commissioner to make an appeal. The Information Commissioner can be contacted via the following details:

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF
Tel: 01625 545 700
Fax: 01625 524 510
Email: mail@ico.gsi.gov.uk