HEDDLU GOGLEDD CYMRU
NORTH WALES POLICE

Response Date:19/08/2024

2024/720 - Networks

In response to your recent request for information regarding;

1. What network vendor(s) / service provider does your emergency service currently use for their LAN, WAN,, wireless and core network (e.g., BT, Virgin, Cisco)?
Primary Service Providers – BT, Virgin, Convergence, CGI
Primary Network Vendors – Cisco, Fortigate, Palo Alto, Juniper

2. Is the network managed / run internally, or is the network managed and/or supplied by a third party? Please specify which elements of the network are outsourced and to which companies.
All network components are outsourced. CGI are the primary contract holder for network services

3. Please may you provide an indication of the size of the network (e.g., number of switches, routers, access points etc.)?
218

4. How much money was spent on the last major network refresh (referring to replacement of the LAN / WAN / core network)?
Network replacement in 2016 £1.6M
Core Nexus upgrade 2022 £280k

5. When was the last major network refresh (month & year)?
See above

6. When is the next major network refresh likely to take place (month & year)?
This is currently underway with the current provider. Network refresh/transformation will take place over the next ~3years.

7. What frameworks are likely to be used when releasing a tender for a network refresh?
North Wales Police would not automatically use a Framework for the tender of a network refresh. We would review the market and may go out to tender direct to market ourselves.

Cyber Security
1. Which cyber security providers / vendors are used, and for what technologies (e.g., firewalls, SOC etc.)?
We operate a comprehensive, complimentary suite of cyber technology comprising of industry leading layered Firewalls, MDM, log analytics and nationally managed SOC service, all securely architected to deliver upon a defence in-depth strategy.

Harm has been identified in providing you with the details of cyber security used, therefore, Section 31 (1) (a) (b) (c) Law Enforcement and Section 24 (1) is to be considered as part of the Public Interest Test. A Public Interest Test has been carried out to weigh up the reasons for and against disclosure of the information requested, to ensure the release is in the interest of the public as a whole and not just the applicant.

Section 24 (1) – National Security
Section 31 (1) – Law Enforcement

Harm in Confirming or Denying that Information is held

To disclose details relating to cyber security providers / vendors may assist potential attackers. It would leave us vulnerable to cyber attacks as we are providing information to those intent on committing crime. This would impact our ability to carry out our policing functions and potential hinder national security too.

Public Interest Considerations

Section 24(1) National Security

Factors in favour disclosure

The public are entitled to know how public funds are spent within an area of policing. To disclose details of cyber security providers / vendors enable the general public to hold the police to account and provide confidence that data is protected. With the call for transparency of public spending this would enable improved public debate.

Factors against disclosure

Security measures are put in place to protect the community we serve. As evidenced within the harm to disclose cyber security providers / vendors would highlight to terrorists and individuals intent on carrying out criminal activity what security we use which could be exploited.

Taking into account the current security climate within the United Kingdom, no information 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.

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 and those intent on committing crime gathering information from various sources would be even more impactive when linked to other information gathered from various sources. 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 disclosure

To disclose cyber security providers / vendors would lead to a better informed public and provide confidences for Force is protected.

Factors against disclosure

As mentioned under the national security section to disclose cyber security providers / vendors would provide data to terrorists and individuals intent on carrying out criminal activity what security we use which could be exploited and hinder us carrying out our role.

Balancing Test

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 any of our security would place the Force and potentially 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 not 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.

2. When is your service due for a renewal of these technologies (month & year)?
There is no single renewal date as vendor / applications were built over a period of time. A significant portion of that service is covered by national cyber programs.

3. Is all cyber security managed in-house, or is it / parts of it outsourced to a third party? Please specify which elements are outsourced and to which companies.
Cyber security is provisioned in-house and supported / monitored externally as part of a national program overseen by Police digital services.

Command and Control
1. Which technology suppliers / vendors are used in your command and control rooms?
Hexagon
Frequentis

2. Is your command and control room managed in-house, or is it / parts of it outsourced to a third party? Please specify which elements are outsourced and to which companies.
Outsourced
HEXAGON UK system - Tier 1 and 2 support – CGI, Tier 3 support - HEXAGON
FREQUENTIS system –Tier 1 support – CGI, Tier 2 and 3 support – Frequentis

3. How much was spent on the last major command and control technology refresh (referring to the replacement of the CAD / ICCS)?
ICCS application and infrastructure 2016 £3M
CAD upgrade 2012 £380k

4. When was the last command and control technology refresh (month & year)?
See above

5. When is the next command and control technology refresh likely to take place (month & year)?
In progress

THIS INFORMATION HAS BEEN PROVIDED IN RESPONSE TO A REQUEST UNDER THE FREEDOM OF INFORMATION ACT 2000, AND IS CORRECT AS AT 09/08/2024