1) How many officers do you have within your constabulary across full time, part time and volunteers

This information is available on the following website

https://www.west-midlands.police.uk/keeping-you-safe/about-us/our-structure/index.aspx

2) How many devices are connected to central data services from outside of official government buildings? These would use Wifi/Home Broadband/LTE networks for example.

5,163 as at 27 February 2017

3) What is the breakdown of these devices (Laptops/Smartphones/Tablets etc)

Laptops: 1,263
Smartphones: 3,129
BlackBerry: 771

4) How many recorded cyber attacks have you had 2015 and 2016

West Midlands Police can neither confirm nor deny that information is held relevant to question 4 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 31(3) Law Enforcement

Please see attached covering letter for further explanation

5) How much cost has been recorded against cyber defence (Prevention, Detection and Response) in the 2015 and then 2016

No additional cost as this is part of existing services

6) How many of these devices use only SSL (or derivative) security to encrypt data in motion to cloud and other data sources

This information is exempt by virtue of section 31(1)(a).Law enforcement please see our reasoning why below.

PUBLIC INTEREST TEST

Section 31 (1) (a)

Harm

The Freedom of Information Act makes it a legal requirement that an authority has a duty to provide information, unless it is exempt, However to disclosure information in relation security encryption data would confirm the ability, or otherwise, of WMP to utilise specific technology.

Release via the Freedom of Information Act is deemed release into the public domain. Therefore to disclose such information would allow criminals to accurately evaluate the capability of WMP to deploy specific technology. This is information, with other pieces in the public domain, could undermine each forces ability to protect the data on remote devices

Considerations that favour Disclosure

Disclosing information about technologies used by police would provide a greater transparency in their actions and ensure that they operate effectively and efficiently. It is clear that there is a public interest in public authorities operating in as transparent a manner as possible, as this should allow the public to understand how the force spends public money.

Considerations that favour non-Disclosure

Where current or future law enforcement role of the force may be compromised by the release of information, then this is unlikely to be in the interest of the public.

Indicating the availability, or otherwise, of specific techniques would provide detailed intelligence to criminals regarding WMP capabilities.

Knowledge of the technologies, encryption details, available to WMP would allow criminals to judge, what information WMP have access to, the methods / software we use could offer those with intentions to unencrypt footage if they had a chance of doing so. This would compromise the future prevention and detection of crime.

Balancing Test

The issues of transparency and awareness are noted. However, on balance it is considered that the public interest in providing the information is outweighed by the potential impact release would have on future law enforcement activities.

Releasing information by the public authority might provide a greater transparency regarding the techniques and storage utilised by the Force. However there are already a number of checks and balances on police forces which ensure that appropriate technologies are used in a proportionate and lawful manner.

There are legislative requirements placed on the police, such as the Police and Criminal Evidence Act and the Regulation of Investigatory Powers Act. Police activity is monitored by independent bodies such as Her Majesty's Inspectorate of Constabulary, the Independent Police Complaints Commission, The Interception of Communications Commissioners Office and the Office of the Surveillance Commissioner. There are, therefore, already a number of mechanisms in place to ensure that the police act in a lawful and appropriate manner.

Providing information in relation to software and encryption details in this case would place into the public domain, information that would allow criminals to avoid detection and target their activities. To undermine the police's ability to prevent and detect crime would not be in the public interest. The wider public interest lies in protecting the ability of the police to utilise these techniques effectively and in a proportionate manner, given that there are already a number of independent mechanisms in place to ensure that the technology is used fairly and lawfully.

Having considered the arguments for and against, the public interest test favours non-disclosure of this information. West Midlands Police will not disclose information that could compromise the future law enforcement role of the force.