| Police Scotland logo | Freedom of Information ResponseOur reference: FOI 24-0819Responded to: 22 April 2024 |
| --- | --- |

Your recent request for information is replicated below, together with our response.

## I am writing to politely request the following data under the terms of the Freedom of Information Act 2000 (FOIA) on cyber attacks affecting  Police Scotland. Where possible please provide data broken down by calendar year or failing that, by relevant 12-month period (e.g. 2021/22 2022/23 etc.) for which data is available.

## How many times has your organisation experienced an attempted cyber-attack in the last two financial years?

## Have you ever reported any cyber-related incidents to the NCSC and if so, how many in the last two financial years?

## Thinking about cyber-attacks where the criminal was able to obtain data or disable systems, how much have these cost the organisation?

Having considered your request in terms of the Freedom of Information (Scotland) Act 2002, I am refusing to confirm or deny whether the information sought exists or is held by Police Scotland in terms of section 18 of the Act.

Section 18 applies where the following two conditions are met:

* It would be contrary to the public interest to reveal whether the information is held

Whilst we accept that you may have a particular personal interest in being informed as to whether or not the information sought is held, the overwhelming public interest to lies in protecting the ability of Police Scotland to defend against security breaches and maintain the integrity of the data it holds.

Ifthe information was held, it would be exempt from disclosure in terms of one or more of the exemptions set out in sections 28 to 35, 38, 39(1) or 41 of the Act

In this instance, Section 35(1)(a) of the Act applies – Law Enforcement

**Section 35(1)(a) – Law Enforcement**

Information is exempt information if its disclosure under this Act, would or would be likely to prejudice substantially the prevention or detection of crime.

It is not exceptional for individuals to enquire as to the information technology in use in Police Scotland or hacking attempts made against it. Nonetheless, there is concern that the release of such data could provide attack opportunities.

The requested information could be used by a hostile party to plan and execute an attack on the Service’s systems or to indicate that such an attack had gone undetected. Such attacks could take the form of data theft, denial of service or other deliberate disruptions. This could not help but have the effect of reducing the ability of the police to undertake relevant activities.

This is a non-absolute exemption and requires the application of the public interest test.

**Public Interest Test**

The public interest factors favouring disclosure of the information surround the Service’s accountability for public funds in terms of the cost to the public purse and any in informing the public of vulnerabilities within Police systems and the subsequent safety of their data.

Those favouring retention of the information surround the adverse effect on the efficiency of the Service. Disclosure would provide those intent on disrupting police activities with enough information to plan and execute a targeted attack or indicate to them that such an attack had been detected or gone unnoticed. Where systems are compromised, there is also the potential for sensitive information such as personal data, security information and other data to be made public, therefore, in this instance the factors favouring retention of the data outweigh those of disclosure.

## How much of the organisation’s total annual budget is spent on cyber support, protection and computer systems?

## How many people are employed by the organisation to oversee cyber support and programmes?

The requested information is considered to be exempt in terms of the Freedom of Information (Scotland) Act 2002 (the Act). Section 16 of the Act requires Police Scotland to provide you with a notice which:

(a) states that it holds the information,

(b) states that it is claiming an exemption,

(c) specifies the exemption in question and

(d) states, if that would not be otherwise apparent, why the exemption applies.

Where information is considered to be exempt, this letter serves as a Refusal Notice that information is held and an explanation of the appropriate exemption is provided.

The exemptions that I consider to be applicable to the information requested by you are:

**Section 35 (1) (a) & (b) – Law Enforcement**

The information requested is exempt, as its disclosure would or would be likely to prejudice substantially the prevention or detection of crime and apprehension or prosecution of offenders. If the details of Police Scotland’s cybercrime resourcing was disclosed, experience has shown that it would allow those intent on committing crime or causing disorder to gauge the likelihood of detection or to take measures to negate the likelihood of detection. It would allow criminals to plan how best to engage or occupy existing police resources in an effort to maximise their chances of committing serious crime, therefore harming the efficient and effective conduct of the service.

Such information would prove extremely useful information for persons involved in criminality as they would be able to plan and conduct their activities to avoid detection. It would confirm the resources available in a specialised area of policing, which would allow those intent on wrong doing to judge the police response to a variety of incidents. In turn this would prejudice substantially the ability for our officers to prevent and detect crime and apprehend or prosecute offenders.

Disclosure would have an adverse impact on the ability of the Police to carry out its law enforcement role effectively, and thereby prejudice substantially the prevention and detection of crime.

This is a non-absolute exemption and requires the application of the public interest test.

**Section 39(1) – Health, safety and the environment**Disclosure of the information requested would prove extremely useful for criminals and those intent on wrongdoing, to estimate the level of cybercrime resources deployed by the Police and would assist them in circumventing the efficient and effective provision of law enforcement by the police service, which in turn would have an adverse impact on the safety of the officers involved and the general public.

This would increase the risk to the personal safety of individuals and also the safety of the police officers responding to incidents.

This is a non-absolute exemption and requires the application of the public interest test.

**Public Interest Test**As you will be aware, the two exemptions detailed above are non-absolute and require the application of the public interest test. Public awareness would favour a disclosure as it would contribute to the public debate surrounding the use and deployment of this specialist unit.

That said, I would contend that the efficient/effective conduct of the service and public safety favours retention of the information as it cannot be in the public interest to release information that would prejudice law enforcement or which is likely to have an adverse impact upon public safety.

If you require any further assistance, please contact us quoting the reference above.

You can request a review of this response within the next 40 working days by email or by letter (Information Management - FOI, Police Scotland, Clyde Gateway, 2 French Street, Dalmarnock, G40 4EH). Requests must include the reason for your dissatisfaction.

If you remain dissatisfied following our review response, you can appeal to the Office of the Scottish Information Commissioner (OSIC) within 6 months - [online](http://www.itspublicknowledge.info/Appeal), by email or by letter (OSIC, Kinburn Castle, Doubledykes Road, St Andrews, KY16 9DS).

Following an OSIC appeal, you can appeal to the Court of Session on a point of law only.

This response will be added to our [Disclosure Log](http://www.scotland.police.uk/access-to-information/freedom-of-information/disclosure-log) in seven days' time.

Every effort has been taken to ensure our response is as accessible as possible. If you require this response to be provided in an alternative format, please let us know.