| Police Scotland logo | Freedom of Information ResponseOur reference: FOI 23-2606Responded to: 25 October 2023 |
| --- | --- |

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

## To ask, in the past five years, on how many occasions Police Scotland have become aware of attempted cyber attacks on its computer systems and networks.

## Could this be broken down by year, whether or not the attempt was successful, and from which country the source of the attack was considered to be.

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.

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.