SSRO

Single Source
Regulations Office

Single Source Regulations Office
Finlaison House
15-17 Furnival Street
London
EC4A 1AB

[REDACTED]
By email to: request-805985-bbb6e3af@whatdotheyknow.com

T 020 3771 4767
E enquiries@ssro.gov.uk

www.gov.uk/ssro

Ref: SSRO/RFI 053

6 December 2021

Dear [REDACTED],

Subject: Freedom of Information request

I refer to your email of 11 November 2021 in which you asked for the following information to be provided, by year, in respect of the period 2018 to November 2021:

1. How many malicious emails have been successfully blocked?
2. What percentage of malicious emails were opened by staff?
3. What percentage of malicious links in the emails were clicked on by staff?
4. How many ransomware attacks were blocked by the department?
5. How many ransomware attacks were successful?

We have considered your request under the Freedom of Information Act 2000 (the FOI Act).

In response to question 1, I confirm that the SSRO does not hold this information.

For questions 2 to 5, the SSRO considers that disclosing whether we hold information concerning malicious email and ransomware attack activity would, or would be likely to, prejudice the prevention of crime. This is because confirming whether we do or do not hold information would give cyber criminals insight into vulnerabilities which may, or may not, exist and this would likely encourage attempts to illegally access the SSRO's IT systems. We are therefore relying on section 31(3) of the FOI Act, which allows us to refuse to confirm or deny if the information is held.

The exemption relied upon is a qualified exemption and is subject to a public interest test. This is a test of whether we should confirm or deny that the information is held, rather than whether the information requested should be disclosed. We have balanced the public interest in confirming or denying whether the information is held against the public interest in maintaining the exemption.

Factors in favour of confirming or denying whether the information is held are that it would support transparency of the organisation's activities, it would provide information about how effective our security systems are and could reassure people about whether our systems are vulnerable or not.

Weighed against this, confirming whether we hold the information or not would increase the likelihood of cyberattacks as it would give cyber criminals insights into the strengths of the organisation's cyber security and any potential weaknesses that may exist. If, for example, the SSRO were to state that it holds all of the information then this could demonstrate to cyber criminals that the organisation's systems are particularly vulnerable, encouraging attacks. If, conversely, the SSRO states that it holds little information, this could either demonstrate that it has poor reporting and recording procedures which will encourage an attack, or that it has robust procedures, in which case it could encourage a cyber criminal to test new attack techniques.

Having weighed these public interests, our conclusion is that the public interests in maintaining the exemption should preponderate.

If you are dissatisfied with the handling of your request, you have the right to ask for an internal review. Internal review requests should be submitted within two months of the date of receipt of our response to your request and should be addressed to: enquiries@ssro.gov.uk.

If you are not content with the outcome of the internal review, you have the right to apply directly to the Information Commissioner for a decision. The Information Commissioner can be contacted at: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF.

Please remember to quote the reference number above in any future communications.

Yours sincerely

Enquiries