8 November2021

Case Reference IC-66648-D3F4

Your request

You asked us for the following: [numbers added]

"1. *The number of ICO employees who have one or more years of experience of working in cyber security roles outside of the ICO.*

2. The number of ICO employees who hold recognised technical cyber security qualifications.

3. The number of ICO employees who do not meet the above criteria, but who work in cyber security roles (including providing cyber security expertise to investigations).

4. The job titles currently held by people with cyber security experience or qualifications.

5. Any internal minutes, strategies or records of discussion relating to cyber security capacity and capabilities within the ICO.

6. Any discussions or documented concerns relating to the potential impact on investigatory capabilities and/or on the integrity of investigations, and the risk of investigatory conclusions being subject to challenge, due to lack of cyber security SMEs.

7. Details of any expense incurred to utilise external cyber security expertise for ICO investigations, or to support the ICO's own security programme"

Where your questions satisfy the criteria of a valid information request, we have considered your request under the Freedom of Information Act 2000 (FOIA). We have considered the information as of today, as we reason that this would be more helpful to you than historic information.

Our response

The actual level of experience, employment history, or qualification of our staff would constitute their personal data which would not be fair or appropriate to disclose, and it is therefore exempt under section 40(2) of

then FOIA. However, I can offer the following in response to questions 1-4:

Please find attached the Job Descriptions of all 14 members of staff in our Cyber Incident Response and Investigation Team (CIRIT) as well as those for our internal Cyber Security team. The size of our internal security team is exempt from disclosure to you under section 31(1)(a) of the FOIA, as it could make the ICO more vulnerable to crime.

Regarding the responses to your requests 5-7:

I can confirm that the ICO holds information in relation to each of the questions. However, this information is exempt from disclosure to you under section 31(1)(a) and 31(1)(g) of the FOIA.

In relation to question 7, you can find ICO expenditure, including IT expenditure, on our website. However, these reports will not specify spending specifically on covering weaknesses in our security.

I shall now explain my application of section 31 and perform both the prejudice and public interest tests.

The FOIA says:

Information is exempt if it's disclosure would *"likely prejudice:*

(a) The prevention or detection of a crime,

…

(g) … the exercise by any public authority of its functions for any of the purposes specified in subsection (2)."

In this case the relevant purposes contained in subsection 31(2) are 31(2)(a) and 31(2)(c) which state:

"(a) the purpose of ascertaining whether any person has failed to comply with the law" and
"(c) the purpose of ascertaining whether circumstances which would justify regulatory action in pursuance of any enactment exist or may arise …"

Clearly the ICO's capacity to defend itself from cyber attack relates to the purposes of crime prevention and thus s31(a) applies.
Turning now to our CIRIT. Clearly the purposes described above under s31(2) apply as CIRIT exists to perform these functions.

The exemption at section 31 is not absolute, and we must therefore consider the prejudice or harm which may be caused by disclosure of the information you have sought, as well as applying a public interest test by weighing up the factors in favour of disclosure against those in favour of maintaining the exemption.

Were the ICO to disclose the relative strengths and weaknesses of its internal security, either in its human resources or technical deficiencies or otherwise, it is likely that malicious parties could use the information to attack the ICO. Indeed, given the ICO's knowledge of the prevalence of malicious attacks on data controllers, it is confident in asserting that suck attacks would be the outcome of the disclosure of its relative strengths and weaknesses.

Were the ICO to disclose the relative strengths and weaknesses of its capacity to investigate security breaches or incidents of other data controllers, it is likely that certain parties, be it investigated parties or malicious third parties, could use such intelligence to prejudice our investigations by playing to the weaknesses of the ICO's capacity when being engaged, or indeed to commit crimes (as malicious third parties) that would be difficult to detect, investigate, and even prosecute.

With this in mind, we have then considered the public interest test for and against disclosure.

In this case the public interest factors in disclosing the information are –

- Increased transparency regarding the functions and operations of the ICO. Especially its own limitations.

The factors in withholding the information are –

- the public interest in maintaining the ICO's ability to defend itself from attack and thus continue to perform its public functions.

- the public interest in the ICO's ability to investigate other data controllers without such investigations being prejudiced by the manipulation or utilisation of the ICO's investigative weaknesses, should any exist.

- the public interest in the ICO's demonstrating good practice in not unduly facilitating the committing of crimes against it by maintaining its own security and systemic integrity.

Having considered all of these factors we have taken the decision that the public interest in withholding the information outweighs the public interest in disclosing it.

This concludes our response.

I hope you find this information helpful.