The ICO exists to empower you through information.

Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF
T. 0303 123 1113
ico.org.uk

Date: 11 March 2025

IC-365416-J2F7

Request

You asked us:

"Do you have a richer data set such as:

1. Company name
2. Two or Four digit NAICA code
3. Number of people in Company
4. Company turnover per year

Where an "Incident Category" is Cyber, any relevant details such as:
1. *Date of attack date*
2. *Threat actor e.g internal or external (suspected name of group)"*

Your question is in relation to the data security incident trends that we publish here: Data security incident trends | ICO.

We received your request on 13 February 2025. We have handled your request under the Freedom of Information Act 2000 (the FOIA).

Our response

The Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004 states that the 'appropriate limit' for the ICO is £450. We have determined that £450 would equate to 18 hours work.

While I can confirm that we do hold a company names when organisations makes a report to us, I consider that conducting the searches necessary to confirm if we hold the other information you have asked for would exceed the cost limit set out by section 12 of the Freedom of Information Act 2000 (FOIA).

When organisations report data breaches to us, we do not ask for NAICA codes. Further, we do not ask for a specific number of people at the company, the company's turnover, or the threat actor. This information may have been provided voluntarily by the company, but because it is not information we normally need for our purposes, it is not stored in an electronic format that can be automatically and easily extracted via a report. To locate whether we hold this information at all, we would have to manually search of thousands of cases. Specifically, according to the dashboard, 3159 cases.

Even if I was to assume that each check only took 1 minute – and to be clear, I think is unrealistic, but I have selected a low number to demonstrate a point – the total time taken would be 52 hours of manual searches which would clearly exceed 18 hours, triggering the provisions of section 12 of the FOIA.

I would estimate, based on my experience handling similar requests, that each check would more realistically take 3-5 minutes per case given that we may have to search through the original data breach report as well as any associated documentation in the event that the information is held in one of those documents.

With the above in mind, we are refusing to respond to this request relying on section 12 of the FOIA. I have provided advice and assistance below in the event that you wish to make a further request.

Advice and assistance

Ordinarily when providing advice and assistance, a public authority will try to recommend ways that you can refine your request such that it has a better prospect of success. However, for reasons you may not be aware of and which I will explain in this letter, I suspect that you may never be able to access some of the specific information you are looking for because I suspect it is in fact exempt.

The Commissioner and his staff are under a duty of confidentiality. This duty arises from section 132 of the Data Protection Act 2018, and reads as follows:

"(1) A person who is or has been the Commissioner, or a member of the Commissioner's staff or an agent of the Commissioner, must not disclose information which –

> *(a) has been obtained by, or provided to, the Commissioner in the course of, or for the purposes of, the discharging of the Commissioner's functions,*
> *(b) relates to an identified or identifiable individual or business, and*

(c) is not available to the public from other sources at the time of the disclosure and has not previously been available to the public from other sources,

unless the disclosure is made with lawful authority."

When an organisation reports a personal data breach (PDB) to us, it is caught under this duty. This is because such information has been provided to the Commissioner for the purposes of discharging our functions, relates to an identified business, and is in almost all cases not available to the public from other sources.

You will have noticed that our data security incident trends dashboards is anonymised given that part of your request is for the names of companies whom the incidents relate to. However, the reason the dashboard is anonymised is so that we can release information about incident security trends without falling foul of section 132. This is because by removing the companies names or other identifying information, section 132(1)(b) no longer applies and therefore the duty falls away.

To provide you with the company name would mean that the companies would once again be identifiable and would therefore be covered by the duty. Therefore, although we have not formally exempted the information for this reason in this response, if you were to make such a request under FOIA, it would in my view not result in the information being disclosed to you. However, I want to emphasise that this should not discourage you from making that request if you so wish because you are still entitled to a formal response that says as such.

We do publish various data sets which do contain the company name, but these data sets are limited so as not to reveal information that is protected by section 132. You can find these data sets here: Complaints and concerns data sets | ICO.

In relation to the other parts of your request, specifically the requests for:

- The two or four digit NAICA code;
- Company turnover per year;
- Threat actor; and
- Number of people in the company.

We do not routinely ask for NAICA codes, company turnover, or threat actor when organisations report PDBs. We also do not ask for a specific number of people that work at the company (although the form does ask for organisation

size stated as either "Under 250" or "251 or more"). In either case, this information, if held at all, is not stored in such a way that can be easily and automatically extracted and would necessitate manual searches of all PDBs that fall within the range of your enquiry. As you will note, we handle a significant amount of enquiries, so even shortening the date range significantly is unlikely to result in us being able to answer effectively.

Even if shortening the data set would make it possible for us to answer the request within the cost limit, it is entirely possible that the information is so severely limited that it is no longer useful to you or representative of the wider data set.

We would also need to be mindful that the provision of extra data such as this may also lead to identification of individual companies, such as through the 'Mosaic effect', where lots of small pieces of unrelated information add up to allow identification. It is possible that this may also mean that more detailed information is also itself exempt by virtue of section 132. However, that is a matter that would have to be analysed in a request, should you choose to progress with a shorter date range.

In closing, I appreciate that I have not painted a positive picture of your prospects of success of other possible requests. It is not my intention to discourage you to seek further information, but it is important that I provide you with an candid advice concerning the reasons why we have anonymised our security incident trends dashboards, the limits of our data, and how that may affect future requests so you can make an informed choice about your next steps.

Next steps

You can ask us to review our response. Please let us know in writing if you want us to carry out a review. Please do so within 40 working days.

You can read a copy of our full review procedure on our website.

If we perform a review but you are still dissatisfied, you can complain to the ICO as regulator of the FOIA. This complaint will be handled just like a complaint made to the ICO about any other public authority.

You can raise a complaint through our website.

Your information

Our privacy notice explains what we do with the personal data you provide to us, and sets out your rights. Our Retention and Disposal Policy details how long we keep information.

Yours sincerely

Information Access Team
Strategic Planning and Transformation
Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF
ico.org.uk twitter.com/iconews
Please consider the environment before printing this email
For information about what we do with personal data see our privacy notice