Summary of responses to the Call for Views on the ICO's Data security incident trends

Introduction

In April 2022, the ICO published a Call for Views on our publication of information about self-reported breaches on our website. We sought input on what additional data, if any, should be included on the dashboard. We would like to thank all those organisations and individuals who took the time to give us their views.

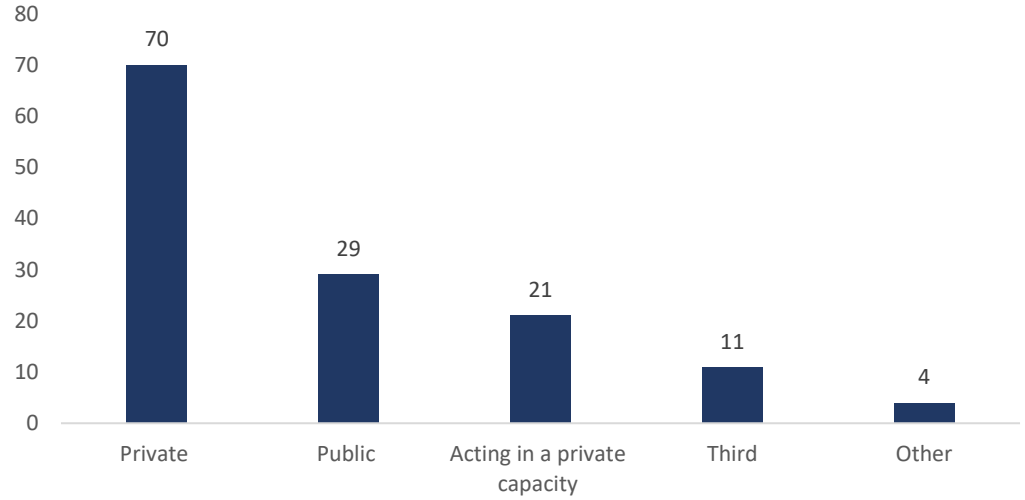
We have carefully considered all of the comments, which are a useful indicator of the interests and experiences of organisations and individuals that might engage with our data, and these have been invaluable in considering what the next iteration of the dashboard should look like.

When designing the new dashboard, we also took into account the technical and legal challenges that would arise from publishing certain categories of data. Therefore, we have not published all information that was requested. We have set out our reasoning within this document in order to provide clarity. However, if you have any questions please let us know by emailing BreachInsights@ico.org.uk.

Respondents

Overall, we received 137 responses to our Call for Views, which are broken down in Figure 1 below. The largest proportion of responses received (70) was from the private sector, with smaller numbers of responses from those operating in other sectors. This question was not answered in two cases.

Figure 1: Types of organsiations that responded



Source: Responses to question A4 of the Call for Views.

We also spoke to four organisations that did not respond to the Call for Views and had follow-up conversations with a small number of organisations who indicated as part of the survey that they would be happy to speak with us.[1] We have incorporated the comments made in these conversations into the opinions highlighted below, however they are not included as part of any charts or numbers presented.

Usefulness of current data

As part of the Call for Views we asked if those responding had used the current dashboard and, if so, how useful they found it. Of those that responded to the survey, 85 (62%) said they had used the data, with the overwhelming majority, 98 (71%)[2] saying they found it 'useful' or 'very useful'.

Those that have used the data said they used it for a variety of reasons, including:

- education;
- training;
- internal updates;
- analysis; and
- monitoring.

Those that said they found it useful highlighted that the dashboard helps in several ways. These include the following:

- It shows what types of breaches have been identified.

[1] We do not provide specific breakdowns from these organisations to ensure anonymity.
[2] We assume this figure is higher than those that had used the dashboard as some went on to look at the dashboard before answering whether it was useful or not.

- It highlights need for care, as there are a number of cases involving human error.
- It can help identify cyber trends, which helps prepare against potential attacks.
- It can be used to compare breach reports across sectors.

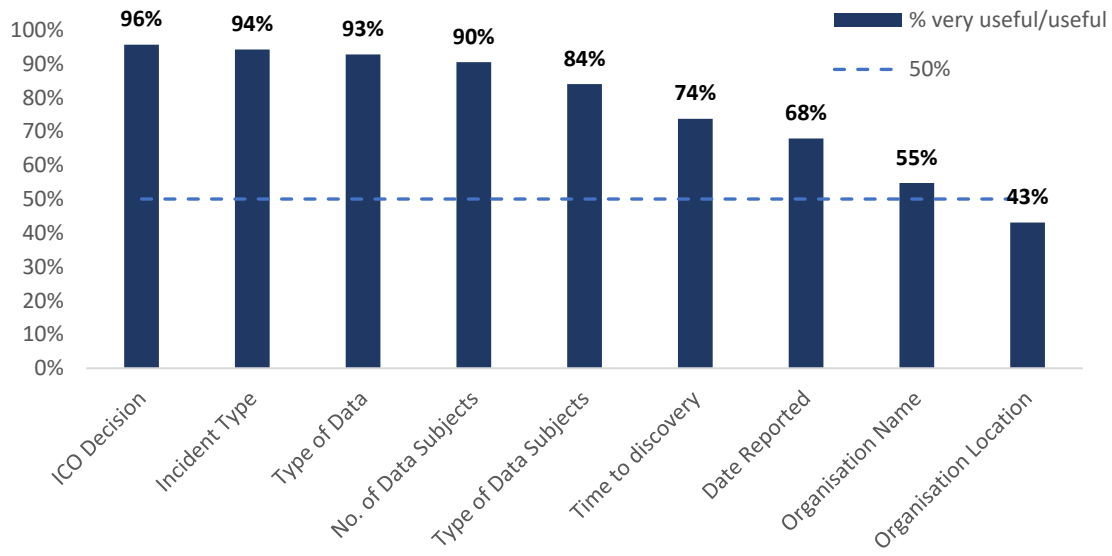
However, there were some areas that people felt could be improved. These included:

- That some of the categories used (eg for the sectors) were too broad.
- More context required to ensure data is interpreted correctly to aid with tasks such as risk assessment.
- The definitions given are not clear enough.
- More filters would help, for example the ability to filter by size of organisation.

Overview of categories of data requested

Overall, respondents indicated that they would like to see more data published on our dashboard. We asked about the possibility of publishing a number of additional categories of data and, in every case but one, more than 50% of respondents said they would find the information 'useful' or 'very useful'. The proportion answering 'useful' or 'very useful' for each question is shown below.

Figure 2: Usefulness of categories of data



Source: Responses to questions C1-C10 of the Call for Views.

Level of detail provided for each category of data

For some categories of data we asked about in the Call for Views, we also asked about the level of detail that respondents would like. These questions were asked about:

- The date the breach report was received;
- The types of data involved in the breach;
- The types of data subject affected by the breach; and
- The decision taken in a case.

For the date, type of data and type of data subject the majority of respondents said they wanted high level detail only. For example, the most popular response for the date was for the month the breach was reported, not the full date.

Responses stated that reporting the month a breach was reported was sufficient for analysis, and would give enough detail to identify trends such as breaches linked to larger external events (eg Covid). However, the full date a breach was reported would be less useful than the date a breach happened, since breaches aren't necessarily identified immediately.

Again, for the types of data and data subject, respondents were keen to get some detail for training, education and analysis purposes. However, it was felt that too much detail may identify individuals or cause increased anxiety for those involved in the breach.

However, respondents were keener to see the full details of the decision reached in a case. They felt that these details could help understand what makes a breach reportable, and can act as the basis for examples for training and presenting to boards. They also thought this could help them understand ICO's decision process so they can prioritise and train effectively.

Justifications

There were several responses that recurred when we asked respondents to explain why they had chosen how useful they would find different categories of data. The more positive (ie why 'useful' or 'very useful') themes covered the ways people used the data. They included the following:

- Education & Training
- General monitoring, risk and trend analysis
- Benchmarking
- Comparison with similar organisations and other sectors
- Resource planning
- Case studies for discussions with upper management/boards

- Identification of vulnerabilities
- Look at impact of large external events (Covid, Ukraine, etc)
- Helps establish which incidents are reportable

Of these, the key areas for those that responded centred around training, analysis, monitoring, and discussions with senior management.

It was felt that the use of real world examples and statistics can help drive home the importance of security to those being trained. It is also useful for explaining to senior management why additional resources are required in specific areas. For example, additional security may be required if analysis and monitoring indicates that there has been an increase in breaches within their sector.

Concerns raised

There were also some common responses for not wanting additional data published. These included:

- It's not relevant or doesn't add value; and
- It may discourage reporting.

Of these, the concern that additional data may discourage reporting appeared most often within the responses. There were comments that publishing too much data about a breach may lead to an organisation being identified (particularly if we chose to publish the name of the organisation that reported the breach). This could make an organisation less likely to report the breach, as they may worry about any reputational damage this may cause.

We also asked in the survey whether there were general concerns people had about the publication of our breach reporting data. Some of the responses are highlighted below.

- Some sectors are more likely to report than others and this can skew data. For example NHS organisations have strict policies in place for reporting breaches, and this may lead to them being overrepresented in the data.
- Some sectors are more likely to collect special category data than others. If these sectors suffer a breach, there is a chance that special category data could be involved. We should highlight this.
- Some were concerned that publishing these statistics could show hackers and cyber criminals where vulnerabilities can be exploited.
- There were some concerns that data could be exploited by law firms, who could use information published to try and encourage affected data subjects to sue.
- There were concerns that publishing data about cases that did not reach the threshold for reporting would not be in the public interest.

Additional comments

As well as asking about specific categories of data within the survey, we also asked if there was any additional information that people would like to see. Although it may not be technically possible to add this data to this next version of the dashboard, these are things we will consider when developing our data in the future.

Additional information suggested in response to this question included:

- Whether it was necessary to report the breach to us in each case;
- Whether the organisation involved had reported other breaches within the previous five years;
- The time between when the breach occurred and the discovery of the breach by the organisation;
- Whether the individuals affected by the breach have been informed; and
- Whether the organisation had taken mitigating steps and what our views on those steps were.

Finally, we asked if there were any additional comments about the dashboard. Key comments were as follows:

- The summary page should be updated to include links to guidance relating to trending breaches, case studies, ways of preventing breaches etc.
- We should define certain terms used within the data.
- We should highlight that the data shows just main cause of breach listed in some cases, and that there may be more than one breach type per incident.
- We need to ensure dashboard isn't overcomplicated. For example the current summary slide contains a lot of information.
- Finally, people like having access to data in other formats. It's currently available in CSV format, but some have asked if we can make it available in other formats also.

If you have any further comments or questions, please get in touch using the email address BreachInsights@ico.org.uk.