Cyber Security Breaches Survey: Public Consultation

Background

The Department for Digital, Culture, Media and Sport (DCMS) is consulting on the [Cyber Security Breaches Survey](#) (CSBS) publication. The CSBS is an annual Official Statistics publication published by the DCMS Cyber Security team for the past 5 years. The latest release was published in April 2019 ([available here](#)), with the next publication due to be published on 25 March 2020.

The findings of this survey of UK businesses and charities help organisations to understand the nature and significance of the cyber security threats they face, and what others are doing to stay secure. This research supports the Government to shape future policy in this area and to work with industry to make the UK one of the most secure places to do business online.

The survey is representative of UK organisations, and surveys both businesses and charities. In 2019, Ipsos MORI conducted a telephone survey of 1,566 businesses and 514 charities, and in depth follow up interviews with 50 organisations. In 2020, the survey has also been extended to include educational institutions.

DCMS continuously looks for ways to improve the survey and the CSBS has evolved over time in accordance with policy priorities and best practice for surveys. The questions in the survey are updated on an annual basis (including changes to the question wording and adding/removing of questions) to reflect user and policy requirements. Survey results are published in accordance with the Code of Practice for Statistics, which states that users should be informed of survey developments and continuously seek feedback on the relevance and use of the survey.

DCMS are considering how the Cyber Security Breaches Survey should continue in future and how its findings are being applied to our policy development. In a recent review of the survey, we identified a number of limitations, including that:
- Year-on-year comparisons are not true indicators of causality due to the changing sample population
- Organisations tend to under-estimate the total cost and impact of breaches.

To mitigate these limitations we are currently undertaking scoping research into:
- The feasibility of establishing a longitudinal survey of large organisations (250+ employees)

- ○ If feasible, this survey would look at organisations' cyber security and governance practices and allow analysis around the link between large organisations' cyber security behaviours and the extent to which they influence the impact and likelihood of experiencing a breach over time. If we proceed with this research, potential users would be consulted on what they would like from the study.
- Developing a more accurate way to estimate the total costs of breaches
  - ○ This research will produce analysis on the possible definitions of cost categories and considerations that will allow government, organisations and market actors (e.g. insurers, cyber consultancies, risk management consultancies) to better estimate the total cost of a cyber incident.

While any potential changes to the CSBS publication are subject to the outcomes of the research outlined above, we are considering four main options for how to proceed with the CSBS from 2021:

1. Retain the CSBS in its current format (including an annual update to the questions to meet user needs)
2. Retain the CSBS in its current format and introduce a separate longitudinal large business survey to try to identify causal links between organisational behaviours and breaches
3. Retain the CSBS and incorporate an additional longitudinal element to the study to try to identify causal links between organisational behaviours and breaches
4. Discontinue the CSBS, to be replaced by a longitudinal survey or other survey measures

As we consider options for the future, we are keen to understand how any changes to the CSBS official statistics would impact users. As such, this consultation seeks feedback on the CSBS publication, specifically why you use the data, what information is used and how frequently you use the information, as well as how any potential changes would impact on this usage.

Users are welcome to respond only to those questions they consider relevant to them. The consultation also provides an opportunity for you to comment on any aspect of the CSBS publication.

This consultation is open to everyone, including members of the public. DCMS aims to continuously improve our statistical outputs as well as ensuring that they continue to meet user needs and make the most effective use of resources available.

Key questions we would like you to consider

Current usage of CSBS
1. Please describe how and why you use these statistics. Please be as specific as possible; for example, if you use the statistics to provide briefing and further analysis to others, it would be helpful to know what the end use is.
2. Which elements of the survey do you use in your work?
3. How frequently do you use the information?

Future CSBS, questions and topic coverage
4. Are there any questions or topic areas you would like to see included in future?
5. Are you currently doing any research on cyber breaches or are you aware of any other research, that may conflict with/ duplicate any of the proposed approaches?
6. Would you be negatively impacted if CSBS were discontinued in its current format?
7. If yes to Q6, please specify which statistics you use and how you will be impacted if comparable figures are no longer available in the future.
8. Would you use a potential longitudinal survey of large organisations' cyber security and governance practices?
9. If yes to Q8, what questions or topic areas would you like to see included?
10. If yes to Q8, how do you envisage that you would use these statistics?

Other comments and re-contact
11. Do you have any other comments, not covered by the questions above?
12. May we contact you to discuss your response to this consultation? This may be to follow up on any specific points we need to clarify.

How to respond

Responses can be submitted via our online survey. If you would prefer, you can also respond to this consultation via email. Please send emails to cyber.survey@culture.gov.uk

This consultation closes at 23:59 on **23 March 2020.**

Further information

All DCMS statistical releases are pre-announced in our statistical release calendar.
You can also keep up to date on our releases and other developments by following us on Twitter @DCMSInsight

We are always interested in feedback from our users so if you have any comments about DCMS statistical releases after the closing date for this consultation, please send these to evidence@culture.gov.uk.

Privacy Notice

The following is to explain your rights and give you the information you are entitled to under the Data Protection Act 2018 and the General Data Protection Regulation ("the Data Protection Legislation"). This notice only refers to your personal data (e.g. your name, email address, and anything that could be used to identify you personally) not the content of your response to the survey.

1. The identity of the data controller and contact details of our Data Protection Officer

The Department for Digital, Culture, Media and Sport ("DCMS") is the data controller. The Data Protection Officer can be contacted at dcmsdataprotection@culture.gov.uk.

You can find out more here:
https://www.gov.uk/government/organisations/department-for-digital-culture-media-sport/about/personal-information-charter

2. Why we are collecting your personal data

Your personal data is being collected as an essential part of the consultation process, so that we can contact you regarding your response and for statistical purposes such as to ensure individuals cannot complete the survey more than once.

3. Our legal basis for processing your personal data

The Data Protection Legislation states that, as a government department, the department may process personal data as necessary for the effective performance of a task carried out in the public interest. i.e. a consultation.

4. With whom we will be sharing your personal data

Copies of responses may be published after the survey closes. If we do so, we will ensure that neither you nor the organisation you represent are identifiable, and any responses used to illustrate findings will be anonymised.

Qualtrics is the online survey platform used to conduct this survey. They will store the data in accordance with DCMS instructions and their privacy policy can be found here:
https://www.qualtrics.com/privacy-statement/

If you want the information that you provide to be treated as confidential, please be aware that, under the FOIA, there is statutory Code of Practice with which public authorities must comply and which deals, amongst other things, with obligations of confidence. In view of this, it would be helpful if you could explain to us why you regard the information you have provided as

confidential. If we receive a request for disclosure of the information, we will take full account of your explanation, but we cannot give an assurance that confidentiality can be maintained in all circumstances. An automatic confidentiality disclaimer generated by your IT system will not, of itself, be regarded as binding on the Department.

5. For how long we will keep your personal data, or criteria used to determine the retention period.

Your personal data will be held for two years after the survey is closed. This is so that the department is able to contact you regarding the result of the survey following analysis of the responses.

6. Your rights, e.g. access, rectification, erasure

The data we are collecting is your personal data, and you have considerable say over what happens to it. You have the right:

- to see what data we have about you
- to ask us to stop using your data, but keep it on record
- to have all or some of your data deleted or corrected
- to lodge a complaint with the independent Information Commissioner (ICO) if you think we are
  not handling your data fairly or in accordance with the law.

You can contact the ICO athttps://ico.org.uk/, or telephone 0303 123 1113. ICO, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF.

7. Your personal data will not be sent overseas.

8. Your personal data will not be used for any automated decision making.

9. Your personal data will be stored in a secure government IT system.