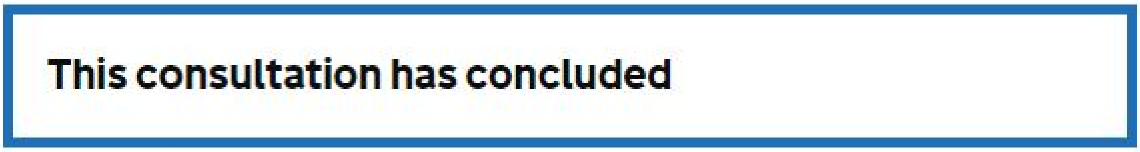
Cyber Security Breaches Survey: Consultation response - May 2020



This consultation has concluded

Detail of outcome

Cyber Security Breaches Survey: Consultation response

The Department for Digital, Culture, Media and Sport conducted a consultation on how the proposed changes to the Cyber Security Breaches Survey, as laid out in the consultation document, would impact users. The Department for Digital, Culture, Media and Sport also hoped to understand what data in the current Cyber Security Breaches Survey respondents used, how frequently it is used and how any potential changes would impact on this usage.

The four options for how to proceed with Cyber Security Breaches Survey from 2021 as stated in the consultation were

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

The public consultation ran from 28th January 2020 to 23rd March 2020.

Consultation response

Following the feedback we have received, the Department for Digital, Culture, Media and Sport will retain the Cyber Security Breaches Survey in its current format. When designing and constructing the Cyber Security Breaches Survey, the Department for Digital, Culture, Media and Sport will continue to engage with the sector to incorporate and revise the question areas highlighted by respondents in this consultation. The Department for Digital, Culture, Media and Sport will continue to explore the feasibility of introducing a separate longitudinal business survey to try to identify causal links between organisational behaviours and breaches.

Consultation feedback

The Department for Digital, Culture, Media and Sport received 17 responses to the consultation. Responses were received from government departments and agencies, academia, professional bodies and industry. The feedback summary below has been structured to reflect the headings under which views were sought in the consultation.

Current usage of the Cyber Security Breaches Survey

- Respondents identified that they used the Cyber Security Breaches Survey to identify and track trends regarding cyber security breaches over time and that these were then used to understand the scale and nature of the cyber security threat that organisations in the UK faced.
- The survey was also used by respondents to help them understand the broader cyber security environment within which they work and different organisational attitudes towards cyber security threats. In particular, respondents mentioned the findings were often used to provide context for academic papers and in grant applications for cyber security research projects.
- It was highlighted that it has been used by the insurance industry to feed into their risk models looking at the cost of a cyber attack.
- Frequency of using the survey findings and data varied by respondent with some highlighting they use it once a month while others use it once a year when the new results are published. The most common answer from respondents was that they used it a couple of times a year.
- The importance and usefulness of including charities and SMEs in the survey was also highlighted.
- Respondents emphasised that they appreciated being able to access the raw data from the survey.

Most used areas of the survey

- Sections of the survey that respondents used most were questions regarding awareness and attitudes, approaches to cyber security, incident and impacts of breaches and attacks and dealing with breaches and attacks.
- Understanding the level of compliance with 10 Steps to Cyber Security and questions regarding the number of organisations who outsource their cyber security were also mentioned as topic areas used by respondents.
- The effectiveness of cyber security measures to prevent cyber attacks amongst businesses and charities was also raised as an area of interest.

Future cyber security breaches survey, questions and topic coverage

- The majority of respondents (seven out of the eight responses to this question) stated that they were not aware of any research that conflicted with or duplicated the proposed approaches. However, one respondent did flag the need to reach out to the ICO to understand how or if they are looking at the cost of breaches.
- Of those who answered the question (five respondents), all respondents stated that they would be negatively impacted if Cyber Security Breaches Survey was discontinued in its current format. They highlighted that it would affect their own work, ability to monitor cyber security trends in the UK and highlighted the importance of the Cyber Security Breaches Survey due to it being a representative survey of the whole business population. Its use to help support and inform key performance indicators in the UK National Cyber Security Strategy was also mentioned.

Future topic areas for inclusion in the survey

Questions and topic areas that respondents would like to see included in any future Cyber Security Breaches Survey included:

- Organisations' attitudes toward cyber security insurance as a substitute for risk management.
- More detail and/or the ability to be able to distinguish between cyber dependent crimes and cyber enabled breaches and crimes.
- Geographical regions to be presented at a more granular level rather than at regional or national level only.
- Greater exploration of the reasons and drivers that lead to organisations changing their cyber security behaviours.
- Whether any of the organisations surveyed have received advice regarding cyber security from law enforcement and if so what.
- What cyber security qualifications are held by those working in cyber security within UK businesses.

Respondents also mentioned:

- The need for any future survey to be clear on the distinction between attacks (which may not succeed) and breaches (successful attacks) was highlighted particularly as respondents felt currently some of the questions merge them.
- Greater clarity in the report regarding the individual who is completing the survey on behalf of the organisation for example their job role was also raised.
- It was also suggested it would be useful if the survey could determine whether a breach was in fact a "crime" by using the Home Office Counting Rules or aligning it with the Home Office costs of crime methodology.

Feedback on the proposed longitudinal survey

Of those who responded to the question (nine respondents), the majority stated that they would use and see benefit in a potential longitudinal survey of large organisations' cyber security and governance practices. They felt it would strengthen the overall evidence and could be used to identify new research opportunities. In particular respondents felt that the following topics would be useful to explore in a longitudinal study:

- Ability to look at cyber security attitudes and whether these change over time. For example if an organisation experiences a breach, do their attitudes and practices consequently then differ compared to those that do not experience a breach, and are these differences statistically significant.
- Respondents also expressed an interest in how long it takes organisations to return to business as usual after the breach.
- Questions that would allow an understanding of the actions and practices organisations undertake as a result of a breach, including actions and attitudes towards cyber security insurance and risk management practices for their organisation.
- Questions that would allow an understanding of how many breaches are considered and reported as a crime by the organisation and exploration of the actions that organisations undertake as a consequence.
- Perceptions of the risk from different threat actors over time.
- Cost/benefits of cyber security qualifications.

There was some resistance for a longitudinal survey if this meant that the Cyber Security Breaches Survey was discontinued.

Additional points raised by respondents during the consultation

- Respondents stressed that they did not wish to lose the ability to track trends over time which they are currently able to do with the Cyber Security Breaches Survey. In particular, they felt that the publication of data tables alongside the Cyber Security Breaches Survey report would allow for these changes over time to be more easily identified.
- There was a desire to keep the existing sample. However, respondents mentioned the wish to be able to have more granular income categories for charities which may require more charities to be included in the sample.
- It was requested for a distinction to be made in the survey between when attacks are cyber dependent or cyber enabled and/or where computer misuse is being used to facilitate another type of crime.
- It was mentioned the possibility of a fifth option for the future of the Cyber Security Breaches Survey which would be to retain the Cyber Security Breaches Survey as it currently is but amend the qualitative element, so that the same organisations were interviewed to see if there were any changes over time and why.

- A one day seminar was suggested where academics and other stakeholders who used the Cyber Security Breaches Survey could present their projects and share insights.
- Respondents mentioned the following as other useful sources of information regarding the topic but felt that there was still a place for the Cyber Security Breaches Survey:
    - Hiscox Cyber Readiness Index
    - Ponemon Institute annual study looking at cyber resilience.