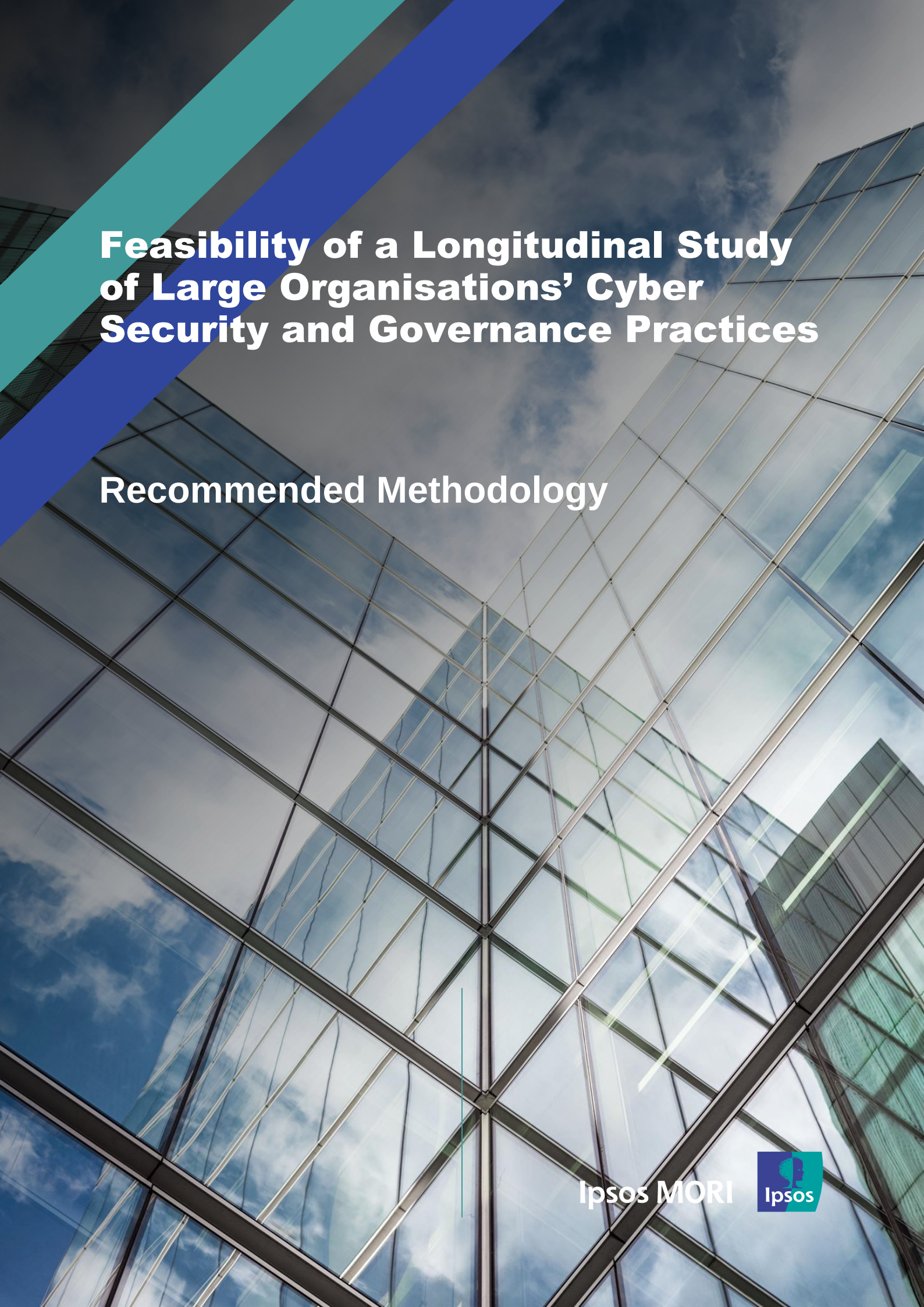

Feasibility of a Longitudinal Study of Large Organisations' Cyber Security and Governance Practices

Recommended Methodology

Ipsos MORI

Contents

1 Background and policy context

In November 2016, HM Government launched its National Cyber Security Strategy which sets out the Government's approach to ensuring the UK is secure and resilient to cyber threats, prosperous and confident in the digital world. The strategy is underpinned by the National Cyber Security Programme (NCSP), which supports economic prosperity, protects national security and safeguards the public's way of life by building a more trusted and resilient digital environment.

The Department for Digital, Culture, Media and Sport (DCMS) works to deliver many of the strategy's objectives, particularly under the 'develop' strand of the NCSS which aims to improve the resilience of the UK economy to cyber-attacks. This includes work to ensure that UK organisations are able to appropriately manage their cyber risks, that there is a sufficient supply of cyber security professionals and skills, and that innovative new companies are being supported to address real world issues.

In 2013, HMG launched The FTSE 350 Cyber Governance Health Check (FTSE 350) which assesses the extent to which boards and audit committees of FTSE 350 businesses understand and oversee risk management measures that address cyber security threats to their businesses. In 2015, DCMS commissioned the Cyber Security Breaches Survey (CSBS) an annual survey of UK businesses and charities as part of the National Cyber Security Programme. The findings help to understand the nature and significance of the cyber security threats organisations face, and what organisations are doing to stay secure. It also supports the Government to understand changes to cyber security and risk across the UK and helps shape future policy in this area in line with the National Cyber Security Strategy.

DCMS wish to investigate the feasibility of creating a new longitudinal study of large organisations' (250+ employees for businesses; £500k+ income for charities) cyber security and governance practices. This study would be intended to allow DCMS to conduct 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. This potential longitudinal study would build upon the insights generated from the FTSE 350 and CSBS.

Ipsos MORI was commissioned by DCMS to undertake a study to determine the feasibility of conducting a longitudinal survey of large organisations' cyber security and governance practices. This report provides a recommended methodology for a longitudinal study of large organisations' cyber security and governance practices. The report draws on the findings from the various strands of the feasibility study, including consultations with government and industry stakeholders, consultations with commissioners of UK business panel surveys in Government Departments, depth interviews with large organisations and a review of existing surveys and literature, including existing DCMS research and relevant research commissioned by other organisations.

2 Project aims and methods

2.1 Aims of the feasibility study

The purpose of the study is to determine the feasibility and appropriateness of a longitudinal survey of large organisations' cyber security and governance practices. The study would be intended to allow DCMS to conduct analysis around the links between large organisations' cyber security behaviours and the extent to which they influence the impact and likelihood of experiencing a breach over time. The study should build on and improve upon the insights already available from the FTSE 350 Health Check and CSBS, by providing a better understanding of the causal relationship between cyber security controls, and breaches or attacks, and their impact.

The specific aims of the study are to:

- review the feasibility of creating a longitudinal study of large organisations' cyber security and governance practices; and
- based on the assessment of feasibility, produce insight into the optimal approach for conducting a longitudinal study of large organisations' cyber security and governance practices.

This report covers the second aim, with a recommended design for a longitudinal study of large organisations' cyber security and governance practices.

2.2 Summary of methods and sources used

A multi-stage approach was used to assess the feasibility of conducting of a new longitudinal study of large organisations' cyber security and governance practices and a recommended design for the survey.

This **initial assessment** involved a review of the existing cyber security questionnaires and datasets held by DCMS to collate information on response rates and recontact rates among large organisations on the subject matter, identify gaps in the evidence base relative to what stakeholders want to see covered, highlight the question areas that could provide better insights via a longitudinal approach and identify the questions that cannot be included in a longitudinal survey as they would suffer from conditioning of respondents. The CSBS and FTSE 350 were reviewed as part of the initial assessment, as well as additional studies exploring cyber security issues carried out on behalf of DCMS and other organisations. The output from this stage was a summary table identifying topics currently covered quantitatively in existing data, and the strengths and weaknesses of these for a longitudinal survey (see Annex 1).

Alongside the initial assessment, a series of **telephone consultations were carried out with industry stakeholders** and a **workshop was held with government stakeholders**[1] to clarify the data and insights that DCMS and other stakeholders want from a large business survey. The government stakeholders included DCMS, Cabinet Office, Home Office, Information Commissioners Office (ICO) National Cyber Security Centre (NCSC), Department for Business, Energy and Industrial Strategy (BEIS) and Her Majesty's Treasury (HMT). The industry stakeholders included Confederation of British Industry (CBI), Institute of Chartered Accountants in England and Wales (ICAEW), Association of British Insurers (ABI) and Tech UK. The topics covered with stakeholders included perceived gaps in the existing data and priorities for a new survey, the types of organisations that should be covered, expectations for

[1] Government stakeholders that were unable to attend the workshop provided separate feedback.

subgroup analysis, the relative importance of comparability with existing surveys (including the CSBS and FTSE 350) and the frequency of data collection (based on the needs of policy).

These two stages culminated in a **statement of data requirements**, including the rationale behind these (i.e. a gap in existing datasets or a priority topic for certain stakeholders). The statement of data requirements also summarised the discussion from the stakeholder workshop and telephone interviews.

Nine **telephone interviews with large organisations** were also undertaken to establish if large organisations hold the data identified in the statement of data requirements, the format it is held in, who it is held by and whether it is easily retrievable. The interviews also explored whether organisations would be willing to disclose the data required and any concerns they have with the longitudinal element. The interviews were recruited from the recontact sample from CSBS 2020 and leads provided by DCMS. Annex 2 outlines the types of large organisations that were consulted.

In parallel with the other stages discussed above, a **systematic review of academic literature on longitudinal business surveys** and the **technical performance of large business surveys** was undertaken. This covered the types of data that have been collected, the sampling and data collection methods, approaches used to maximise response rates and minimise attrition, frequency of data collection and response rates obtained; Annex 3 contains a summary of the main surveys referenced in the report, and Annex 4 has a complete list of studies and sources.

The stages above were brought together in a report which focus on an overall assessment of the feasibility of a longitudinal study of large organisations' cyber security and governance practices. Following this assessment, a meeting was held with DCMS to discuss key issues to cover in the recommended design.

2.3 Contribution of this review to the overall study

This document provides a recommended methodology for a longitudinal survey of large organisations' cyber security and governance practices (including suitable sampling frame, optimal sample design, suitable data collection mode(s), questionnaire design approach, how to maximise response rates and minimise attrition, and recommendations for weighting) based upon key issues discussed as part of the feasibility assessment (which is provided as a separate summary of findings).

3 Recommended survey design

3.1 Overview

In order to achieve its objectives, the proposed survey will need to be based on a robust design which will achieve a good response rate.

3.2 Sample population

In any survey it is important to define the target population. In surveys of organisations, this will include consideration of the inclusion or exclusion of businesses in terms of size, organisational level, industry sector and ownership (public, private and charity sector).

Surveys of organisations are based on different populations. The first distinction is between surveys of **enterprises** (whole organisations) and **establishments** (individual sites/workplaces). CSBS and the Cyber Skills Survey (CSS) are sampled at the enterprise level; this reflects that multi-site organisations will typically have connected cyber security infrastructure and will therefore deal with cyber security centrally. Other surveys, including the main UK longitudinal surveys Longitudinal Small Business Survey (LSBS) and Large Business Survey (LBS) are also sampled at the enterprise level. We have therefore assumed that the proposed survey would sample organisations at the enterprise level, in line with these surveys.

The survey population also needs to be defined in terms of **sector**. All of the most relevant DCMS studies on cyber security and governance (CSBS, CSS and FTSE 350) include private sector businesses; CSBS and CSS also include non-profit organisations and CSS includes most of the public sector. **Government stakeholders** felt that larger charities (by income rather than number of employees) should be considered for inclusion, although noted that questions may need to be adapted as in CSBS.

Reflecting the views of government stakeholders, and following discussions with DCMS, the survey should include **private sector business and charities**, but not public sector organisations (defined as SIC 2007 category O[2]).

In CSBS and CSS, organisations with no IT capacity or online presence are deemed ineligible, which has led to a small number of specific sectors (agriculture, forestry and fishing) being excluded. However, this issue should not apply to this survey given that it will cover larger organisations only. Therefore, we have assumed that (other than the exclusion of all public sector organisations) there will be no other exclusions by sector or type of organisation.

As noted above, this report covers two options: the first based on **large organisations only**, and the second including both **medium-sized and large organisations**. Surveys usually define large organisations as those with 250 or more employees, and medium-sized organisations as those with 50-249 employees. Charities are usually defined in relation to annual income. The population figures for businesses and charities are shown below.

[2] This category includes activities of a governmental nature, normally carried out by the public administration. This includes the enactment and judicial interpretation of laws and their pursuant regulation, as well as the administration of programmes based on them, legislative activities, taxation, national defence, public order and safety, immigration services, foreign affairs and the administration of government programmes.

Table 4.1: ONS population data for UK private sector businesses[3]

	Number of organisations				
Number of employees	**UK**	**England**	**Wales**	**Scotland**	**Northern Ireland**
50-249	**35,585**	**30,715**	**1,330**	**2,510**	**1,030**
- 50-99	23,530	20,325	895	1,635	675
- 100-199	10,000	8,640	360	705	295
- 200-249	2,055	1,750	75	170	60
250+	**7,685**	**6,805**	**225**	**495**	**160**
- 250-499	3,915	3,445	125	260	85
- 500 or more	3,770	3,360	100	235	75

Table 4.2: Charity population data (from charity regulator databases)

	Number of organisations			
Annual income	**UK**	**England and Wales**	**Scotland**	**Northern Ireland**
Unknown	9,550	7,714	1,836	2,788
£0 to under £10,000	78,820	66,971	9,061	1,946
£10,000 to under £100,000	69,165	58,793	8,426	1,066
£100,000 to under £500,000	27,366	23,068	3,232	326
£500,000 to under £5 million	11,337	9,541	1,470	39
£5 million or more	3,045	2,351	655	365
High-income charities (£500,000 or more)	**14,382**	**11,892**	**2,125**	**2,788**

In making a final decision over the inclusion of medium-sized organisations, there are several issues to consider:

- Firstly, it is important to assess the relevance of medium-sized businesses to the proposed topic coverage. Government stakeholders saw value in including medium-sized businesses, given that they share some characteristics with large businesses (e.g. central IT department, digital footprint) and the population tends to be more stable than among smaller organisations.

- From a technical perspective, the inclusion of medium-sized businesses would add a dimension to the design of the survey. The total sample size will need to be larger, to allow separate analysis of the two groups, and the sample design would need to ensure sufficient numbers in each group, while minimising any resulting weighting. It is worth noting that, even with the inclusion of medium-sized businesses, the sample design of the proposed survey is likely to be more 'efficient' than surveys that include organisations of all sizes[4].

- At the same time, the inclusion of medium-sized businesses would provide a larger number of businesses in the population that could be sampled. There are limited numbers of large

[3] Business population estimates 2019 (published January 2020) https://www.gov.uk/government/collections/business-population-estimates#history

[4] Surveys which include small, medium-sized and large businesses tend to over-sample large businesses (and under-sample small businesses) for analysis purposes. This is because the vast majority of businesses in the population are very small, and a random sample without any disproportionate sampling would produce a sample with very few large businesses. As a result, sample designs often lead to large weighting factors and a reduction in the effective sample size of the total sample. A sample based only on large businesses (or both medium-sized and large businesses) will inevitably be more 'efficient', because it does not need to under-sample the huge numbers of small businesses.

organisations in the UK and, given likely response rates, this may be barely sufficient for the sample size that is likely to be required (these issues are discussed further below).

3.3 Number and frequency of survey waves

There are no hard and fast rules on the time gap between waves in a longitudinal survey. The gap between waves, and the overall time span of the panel, needs to be long enough to observe change in behaviour (e.g. cyber security policies and practices).

Existing cross-sectional surveys (CSBS, CSS and FTSE 350) have been conducted annually, and some large changes can result from one year to another.

This suggests that the proposed survey should also take place **annually**. This proposed time interval is long enough to observe sustained changes over time between waves while not over-burdening organisations. A more frequent survey would represent a larger burden on organisations, would cost more and would result in greater sample attrition; while a less frequent survey may be less able to record accurate timing of events (e.g. instances of breaches), may result in too great a level of change between waves and will offer less frequent reporting.

In terms of the full time span of the survey, a **three-year time period** should be long enough to observe meaningful change. LSBS and LBPS have both been organised and commissioned on a three-yearly basis (three annual surveys), although they have been extended beyond the initial three-year period (LSBS is now in year 5).

For the survey as a whole, the use of panel refreshment can maintain the total sample size over many years. However, for longitudinal analysis it is likely to be impractical to maintain a large enough panel sample for more than three years (for example, in LBPS the wave 1 sample of 1,770 produced 378 cases that were interviewed at each of waves 1-4).

3.4 Sample design

Surveys of organisations tend to have quite complex sample designs, as they aim to achieve several (sometimes competing) objectives:

- Achieving a representative sample of the population;
- Ensuring sufficiently large sample sizes in sub-groups of interest;
- Minimising the design effect attached to the weighting (larger weighting factors result in larger design effects, which reduce the ‘effective sample size’ for statistical calculations).

In the **initial sample design** (i.e. before wave 1), surveys of organisations usually adopt a detailed stratification strategy, to ensure that sufficient numbers of organisations are interviewed in key groups of interest. This can involve complex assumptions in longitudinal surveys, as the original sample design needs to predict likely numbers of interviews (overall and in specific sub-groups) in future waves.

We have assumed that separate samples of businesses and charities will be drawn, and that they will be analysed separately. A detailed sampling specification can be agreed at the start of the survey. At this stage, we have set out a summary of a possible approach:

- The business sample will be proportionately stratified by region and sector, and disproportionately stratified by size, to ensure sufficient numbers of interviews in different size bands: medium-

sized/50-249 employees (if included in the survey), 250-499 employees, and 500+ employees. It will also be possible to disproportionately stratify by sector, depending on the likely distribution by sector and analysis needs.

- The charity sample will be proportionately stratified by country and disproportionately stratified by income band, again for analysis purposes.

The sample stratification will take into account the expected variation in response rates by size and sector. An additional factor for sub-group response rates is 'slippage' from one group to another. This can happen when comparing size band or sector in the sample frame (e.g. Inter-Departmental Business Register[5], IDBR) with the survey responses, or (in the case of size band) the change from one wave to another.

After the first wave of the survey, subsequent survey waves typically adopt a hybrid approach. For the longitudinal sample, it is important to interview as many organisations as possible that took part in previous waves, in order to maximise the sample size. As well as contacting those who were interviewed in the previous wave, the sample could be extended to include those who did not participate in the previous wave, but who are eligible and did not refuse outright. This is particularly relevant at the third or later waves (e.g. wave 1 respondents who dropped out at wave 2 can potentially be re-integrated into the survey at wave 3).

The design also includes 'panel refreshment', using a fresh or 'top-up' sample at waves 2 and 3. This is in line with most longitudinal surveys of organisations. This approach is necessary if the sample at later waves is to remain representative of the full population, given that new businesses will become eligible over time (new start-ups and those reaching the eligible size threshold). Panel refreshment will also increase the total sample size, in response to sample attrition.

The design of the survey also needs to accommodate the ways that **organisations change over time**.

Where organisations change their structure (e.g. in the event of a merger or take-over), surveys have different rules for dealing with this issue. For surveys of workplaces/establishments, this can be a complex process, although it should be more straightforward in this survey, given the focus on whole organisations/enterprises.

3.5 Sample size and sub-groups

The interview numbers proposed for the survey reflect a balance between practicalities (specifically, the limited population of large businesses) and cost-effectiveness (producing a high level of statistical confidence relative to costs). Specifically:

- The interview numbers for large businesses are the maximum that are likely to be feasible, even by sampling all available cases.

- The interview numbers for other groups (charities and medium-sized businesses) have been chosen to produce a sufficient level of statistical confidence. The numbers in these groups are designed to be broadly in line with or slightly lower than the sample of large businesses; we assume that large businesses will be the key group of interest in the survey (irrespective of the actual design and population definition).

[5] https://www.ons.gov.uk/aboutus/whatwedo/paidservices/interdepartmentalbusinessregisteridbr

- These sample sizes will allow for sub-group analysis (e.g. by business size and charity income, broad sector); this is discussed further below.

Specific details of interview numbers are shown in the section on response rates, including assumptions for sample attrition and non-response. In summary:

Option 1 (large organisations only):

- Wave 1: 1,550 interviews - 780 large businesses and 770 charities
- Wave 2: 1,215 interviews (630 businesses, 585 charities) - 780 longitudinal (390 businesses, 390 charities), 335 new (240 businesses,195 charities)
- Wave 3: 895 interviews (445 businesses, 450 charities) – 390 full longitudinal (all 3 waves) (195 businesses, 195 charities); 315 other longitudinal (wave 3 plus at least one previous wave) (145 businesses, 170 charities), 190 new (105 businesses, 85 charities).

Option 2 (large and medium-sized organisations):

- Wave 1: 2,095 interviews – 1,320 businesses (780 large, 540 medium) and 775 charities
- Wave 2: 1,735 interviews (1,165 businesses, 570 charities):
  - 1,045 longitudinal: 660 businesses (390 large, 270 medium), 385 charities
  - 690 new: 505 businesses (240 large, 265 medium), 185 charities
- Wave 3: 1,305 interviews (865 businesses, 440 charities):
  - 525 full longitudinal (all 3 waves): 330 businesses (195 large, 135 medium), 195 charities
  - 470 other longitudinal (wave 3 plus at least one previous wave): 305 businesses (145 large, 60 medium), 165 charities
  - 310 new: 230 businesses (105 large, 125 medium), 80 charities.

3.6 Statistical confidence

When analysing change over time, longitudinal datasets have statistical advantages – that is, statistically significant levels of change across waves can generally be identified from smaller sample sizes with longitudinal studies than with cross-sectional studies. In other words, longitudinal surveys are generally more sensitive to change than independent cross-sectional samples of the same size.

An example is shown below, taken from the LBS. For the longitudinal sample, this assumes a sample size of 1,000 interviews at both waves, and a result of 43% very satisfied at wave one; and that 550 of the wave 2 respondents were also interviewed at wave 1, while 450 were not interviewed at wave 1.

Example of statistical confidence: cross-sectional v refreshed panel sample

Q Approximately how often, if at all, are your organisation's [IF BUSINESS: directors/IF CHARITY: trustees/IF EDUCATION: governors] or senior management given an update on any actions taken around cyber security? Is it …?

	Percentage point increase needed at wave 2 for statistical significance (95% level)
Cross-sectional	4.4
Panel	3.3[6]

To look at this another way, in a completely cross-sectional survey, a sample size of around 1,750 at each wave would be needed to achieve similar levels of statistical confidence, compared with a partly longitudinal sample of 1,000 at each wave (as in the example above).

When considering sub-groups, a longitudinal survey has advantages for sub-group samples when comparing change over time.

3.7 Sample frame

The **Inter-Departmental Business Register (IDBR)** is the most common sample frame for surveys covering medium and/or large organisations, such as the Workplace Employment Relations Study (WERS) and the Commercial Victimisation Survey (CVS).[7] CSBS and CSS have also used IDBR for the sample of private sector businesses while, for charities, the sample frames were the charity regulator databases in each UK country.

For charities, the preferred option would be to replicate the approach used in CSBS and CSS and to use **charity regulator databases** for England and Wales, Scotland and Northern Ireland.

One complication for this survey is the focus on larger organisations. This is straightforward for private sector businesses, as the definition of small, medium-sized and large businesses is well defined (in terms of number of employees) and is compatible with the information held on IDBR.

The definitions are less well established for charities. Firstly, it is problematic to classify charities in relation to number of employees, given that charities also have trustees and volunteers in addition to paid employees (some large charities have very few paid employees). In any case, the charity regulator database does not include information on the number of employees, so this would be problematic in practical terms. CSBS defines charity size in terms of annual income, specifically low income (less than £100,000), medium (£100,000-£500,000) and large (£500,000 or more).

Number of employees, volunteers & trustees	Medium-income charities (income £100k-£500k) (n=51)	High-income charities (income £500k+) (n=143)
	%	%
0-9	46	3

[6] Assuming 35% 'monthly' at each wave, 8% 'monthly' at wave 1 but not wave 2, 11% 'monthly' at wave 2 but not wave 1.
[7] The Inter-Departmental Business Register (IDBR) is a comprehensive list of UK businesses used by government for statistical purposes. It is fully compliant with the European Union regulation on harmonisation of business registers for statistical purposes (EC No 177/2008); https://www.ons.gov.uk/aboutus/whatwedo/paidservices/interdepartmentalbusinessregisteridbr

10-49	42	37
50-249	4	33
250+	6	23

3.8 Data collection method

The most common method of data collection for surveys of organisations is by **telephone**, using computer-assisted telephone interviewing (CATI). For example, this is used in CSBS and Cyber Skills Survey (CSS), LBPS/LBS, LSBS, ESS and the HMRC Mid-size business customer survey (i.e. most of the studies that are particularly relevant to the proposed survey). CATI offers the advantages of interviewer-administered interviewing (usually achieving higher response rates than self-completion surveys) while being significantly cheaper than a face-to-face approach.

Some surveys offer **online** questionnaire completion as an alternative or supplement to the main CATI interview.

3.9 Questionnaire design and interview length

Interview length

In order to minimise survey non-response, it is generally recommended that telephone interviews should take no longer than 25 minutes to complete (Hales and O'Connor, 2008). In many of the telephone surveys covered in this review, **the interview length is around 20 minutes** on average. For example, the interview length in the LBS and LBPS has averaged 20 minutes each year, while the LSBS initially used a longer questionnaire length (30 minutes at wave 1), although this has fallen over subsequent waves, down to 18 minutes on average among panel respondents at wave 4.

Both LBS and LSBS have used a **modular approach** to the questionnaire design, in which certain questions are only asked of a random sub-set of the total sample. This allows for a greater number of questions to be included without extending the interview length. The main disadvantage of a modular approach is that it reduces the sample size for the questions included in the modules.

Questionnaire coverage

A questionnaire for the longitudinal survey has not yet been developed. However, in order to assess feasibility, initial work has been undertaken as part of this project, to examine question areas that could potentially be covered in the survey.

At the start of the project, DCMS outlined their expectations for the survey coverage, for areas such as: measures organisations have taken regarding cyber security, cyber security policies, governance and risk management arrangements, cyber security breaches experienced and the impact and cost to organisations that have experienced a cyber security breach.

This project confirmed that existing DCMS surveys (CSBS, CSS and FTSE 350) include coverage of all of these broad topics. As a result, the questionnaires from these surveys will provide a solid basis for the questionnaire design. A review of existing questions also found that many are suitable for use in a

longitudinal survey. Objective questions that focus on specific aspects of behaviour are likely to be more effective than those that are more subjective or general.

Overall, stakeholders were positive about creating a new longitudinal study of large organisations' cyber security and governance practices. In particular, stakeholders valued the ability to conduct analysis around the link between large organisations' cyber security behaviours and the extent to which this influences the impact and likelihood of experiencing a breach over time. In broad terms, stakeholder needs were consistent with the aims of the proposed survey – and the coverage in existing surveys. Stakeholders also identified some topics, notably the supply chain and investment in cyber security, as priority areas that are not currently covered in great detail in existing surveys.

Some stakeholders felt that attackers were more frequently targeting weak points within a supply chain widening the impact of a breach on organisations. This was particularly the case if the end recipient of a breach was part of Critical National Infrastructure. They wanted to address a hypothesis whereby organisations more stringently monitoring the risks of suppliers and supply chains were less susceptible to a costly cyber breach. It was suggested that questions could include the extent to which organisations monitor supplier and supply chain risks and this could be mapped against experiences of high impact breaches over time. However, it was also noted that the term 'supply chain' needs a specific and objective definition, to avoid confusion and multiple interpretations of what the term means.

In terms of investment, stakeholders were interested in how much was being invested in cyber security and governance measures, and the specific investment priorities of large organisations. It was suggested that questions could cover the amount spent on investment, the products and measures organisations were investing in (e.g. technology to identify breaches, cyber insurance), their motivations for investing in cyber security and the trade-offs related to investment. This could be used to understand the attitudes, strategies, measures and products which have the greatest impact on cyber resilience.

Key issues for questionnaire design

In order to examine trends over time, longitudinal surveys need to **maintain consistent question wording over time**. This has to be balanced against the need to amend or update the questionnaire, and to reflect changing priorities or new developments. The LSBS technical reports discuss this issue, referring to consultation that was carried out prior to all waves of the survey to "balance stakeholder needs with the longitudinal tracking objective". **Stakeholders** agreed that consistency in question wording was very important, while also wishing to see some flexibility to seek organisations' reactions towards policy changes and to consider new topics.

Keeping consistent question wording on some issues may be difficult for the proposed survey, given the changing nature of cyber security. Large businesses raised concerns in this area, suggesting that questions asked in the first wave may become irrelevant by the time of the final wave. Therefore, for some questions (e.g. related to the evolving nature of threats), questions and response codes may need to be updated accordingly.

A key issue for the questionnaire design will be to ensure questions are focused on **larger organisations**, by extending areas which are particularly relevant to large organisations such as the influence of the Board, the wider supply chain, cyber investment and insurance. Some specific challenges were also raised by stakeholders, including monitoring the threats large organisations face, as cyber is seen to constantly evolve.

One useful approach in longitudinal surveys is the option of **pre-populating** questionnaires or using 'dependent interviewing'. With this approach, data can be merged into the interview, either from sample data or answers given at previous waves of the panel. This approach can save time in the interview and also help to reduce 'seam bias', which is the over-estimation of the degree of change between waves because of reasons such as a change of respondents or poor questionnaire wording.

Cognitive interviewing and piloting

It will be important to include cognitive interviewing and a pilot in advance of each survey wave. This is in line with other longitudinal surveys, including LBPS/LBS and LSBS.

4 Fieldwork and survey management

4.1 Sample selection and management

After selecting the initial sample, there will be a process of **sample cleaning and editing** before issuing sample records for fieldwork. Specifically, cases will be removed as follows:

- Removing duplicates, for example either because they were businesses that belonged to a larger enterprise group, or because there was duplication on business name or by telephone number.
- Telephone number searches: Only a proportion of sample records available from IDBR contain a telephone number. Telephone number searches (both automated and manual) can be carried out to boost the number containing a valid telephone number. This approach typically results in more than 80% of sample records having a valid telephone number (either from the original IDBR record or from the search process), and therefore being available for fieldwork.
- Removing cases used for cognitive interviewing and piloting: as noted above, it is possible that pilot interviews can be retained in the analysis, provided that there are minimal changes to the questionnaire.
- Removing cases sampled in concurrent surveys on similar subjects (which target the same individuals).

4.2 Fieldwork procedures

Survey respondent

In CSBS and CSS, interviewers aim to speak to the ‘senior member of staff who has the most knowledge or responsibility when it comes to cyber security’.

Longitudinal surveys normally aim to interview the same individual each time the survey takes place. According to Forth (2008), a change of respondent can have a negative impact on response rates and on data quality, particularly for attitudinal data.

Length of fieldwork

Most surveys of organisations have lengthy fieldwork periods, and this applies particularly to longitudinal surveys, where there is often a large sample at wave 1.

4.3 Expected response rates

It will be important for the survey to achieve the highest possible response rate and to minimise response bias. As noted above, the population of large businesses is limited, and a low response rate may result in insufficient numbers of interviews, even if all eligible cases are selected from the population.

Drawing together the evidence reviewed for this project, we have set out likely response rate assumptions and numbers of interviews.

Table 4.1: Large organisations only

	Businesses	Charities
Initial sample	7,685	2,400
Issued for fieldwork[8]	6,530	2,040
Wave 1 interviews[9]	780 (12% of issued)	770 (38% of issued)
Sample available for wave 2[10]	4,250	1,595
Wave 2 interviews		
▪ longitudinal[11]	390	390
▪ other[12]	240	195
▪ Total	630	585
Sample available for wave 3[13]	2105	1040
Wave 3 interviews		
▪ longitudinal[14]	340	365
▪ other[15]	105	85
▪ Total	445	450

[8] For all groups, assumes 85% of initial sample are issued for fieldwork (after cleaning and telephone number search).
[9] Response rates based on latest CSBS figures.
[10] Includes: wave 1 interviews (for all groups, assumes 85% gave permission for re-contact), fresh sample (385 for businesses and 100 for charities) and cases that were unproductive at wave 1 but still eligible for contact (based on latest CSBS figures).
[11] For all groups, assumes 50% of wave 1 respondents are also interviewed at wave 2.
[12] For fresh sample, response rates based on latest CSBS figures. For unproductive cases at wave 1, assume response rate is half of that obtained at wave 1.
[13] Includes: wave 2 interviews (for all groups, assumes 85% gave permission for re-contact), fresh sample (385 for businesses and 100 for charities) and cases that were unproductive at wave 1 but still eligible for contact (based on various assumptions based on outcomes at previous waves).
[14] This comprises respondents interviewed at all 3 waves (195 businesses and 195 charities) and those interviewed at wave 3 plus one previous wave (145 businesses and 170 charities). For all groups, assumes 50% of wave 2 respondents are also interviewed at wave 3.
[15] For fresh sample, response rates based on latest CSBS figures. For unproductive cases at wave 2, assume response rate is half of that obtained at wave 2.

Table 4.2: Large and medium-sized organisations

	Large businesses	Medium-sized businesses	All businesses	Charities
Initial sample	7,685	3,000	10,685	2,400
Issued for fieldwork[16]	6,530	2,550	9,080	2,040
Wave 1 interviews[17]	780	540	1,320	775
Sample available for wave 2[18]	4,250	2,355	6,605	1,535
Wave 2 interviews				
▪ longitudinal[19]	390	270	660	385
▪ other[20]	240	265	505	185
▪ Total	630	535	1,165	570
Sample available for wave 3[21]	2,105	1,515	3,620	1,015
Wave 3 interviews				
▪ longitudinal[22]	340	295	635	360
▪ other[23]	105	125	230	80
▪ total	445	420	865	440

[16] For all groups, assumes 85% of initial sample are issued for fieldwork (after cleaning and telephone number search)

[17] Response rates based on latest CSBS figures.

[18] Includes: wave 1 interviews (for all groups, assumes 85% gave permission for re-contact), fresh sample (1,084 for businesses and 100 for charities) and cases that were unproductive at wave 1 but still eligible for contact (based on latest CSBS figures).

[19] For all groups, assumes 50% of wave 1 respondents are also interviewed at wave 2.

[20] For fresh sample, response rates based on latest CSBS figures. For unproductive cases at wave 1, assume response rate is half of that obtained at wave 1.

[21] Includes: wave 2 interviews (for all groups, assumes 85% gave permission for re-contact), fresh sample (685 for businesses and 100 for charities) and cases that were unproductive at wave 1 but still eligible for contact (based on various assumptions based on outcomes at previous waves)

[22] This comprises respondents interviewed at all 3 waves (330 businesses and 195 charities) and those interviewed at wave 3 plus one previous wave (305 businesses and 165 charities). For all groups, assumes 50% of wave 2 respondents are also interviewed at wave 3.

[23] For fresh sample, response rates based on latest CSBS figures. For unproductive cases at wave 2, assume response rate is half of that obtained at wave 2

4.4 Confidentiality and data security

Although there is much scope for sharing commercially sensitive information in a longitudinal cyber security survey, **large organisations** interviewed did not have huge concerns about sharing information on costs, employment, or investment in cyber security. However, there was recognition that some organisations might be hesitant around disclosing the number of breaches they've had due to commercial sensitivity.

There were some concerns expressed relating to granular detail on cyber security controls, particularly relating to how they are implemented and configured. An example of this would be sharing results of penetration testing, or how organisations implement patching. This was because they felt attackers obtaining the information could potentially use it to target weaknesses.

A Methodological Review of Research with Large Businesses, conducted for HMRC in 2008, noted that greater care is needed in longitudinal surveys to avoid the risk of disclosure. This is because "an intruder may be able to piece together information on a business from more than one wave of the survey: so-called 'residual disclosure'. It may be the case that no single wave of data offers a substantive risk of disclosure, but that the waves of data can be considered to pose a risk in combination. This means that more extensive efforts are required to protect the anonymity of respondents and the confidentiality of data in a longitudinal study" (Forth, 2008). This is particularly important given the focus on large businesses. For example, as there are small numbers of large businesses in certain sectors, sector analysis may risk disclosure of some organisations.

This has implications for the **storage of and access to the data**, as well as procedures for ensuring anonymity in the data (e.g. by suppressing certain variables and providing banded/rounded figures rather than actual figures).

4.5 Quality assurance measures

As Lynn (2009) has pointed out, 'longitudinal surveys are often not as good as cross-sectional surveys at providing cross-sectional estimates' [24] because the sample may become **less representative over time**.

For this survey, a number of other measures can be taken:

- With a refreshed sample, **panel conditioning** could be explored (and possibly quantified) by comparing the answers of the longitudinal sample with the top-up sample.
- Another type of measurement error that may affect longitudinal surveys is 'seam bias', whereby panel surveys tend to obtain over-estimates of the degree of change between waves. This is a particular concern where the individual respondent changes but can be an issue even when the respondent is the same. This can be addressed through 'dependent questioning', e.g. "According to our records, when we last interviewed you on ….. [last year], you mentioned that you have a specific cyber security insurance policy. Is that correct?).

4.6 Weighting

Weights will be required to remove biases in the sample caused by purposively sampling larger organisations relative to smaller ones, and to address the impact of sample attrition.

[24] Peter Lynn, 'Methods from Longitudinal Surveys' in Methodology of Longitudinal Surveys (ed. Peter Lynn) (2009), p. 8.

The Methodological Review of Research with Large Businesses (Forth, 2008: page 18) comments on weighting techniques in panel surveys, including the use of both cross-sectional and longitudinal weights to correct for unequal probabilities of selection and observed non-response biases. Cross-sectional weights ensure that the sample at any time point is representative of the known population at that time (including new births, etc.), while longitudinal weights seek to adjust the sub-set of respondents who have responded at each wave to the sample of responding organisations at time 'zero'.

For example, in WERS, separate sets of weights were devised for the panel sample and the combined sample, the latter being cross-sectionally representative of all workplaces, whilst the former were used for analysing change over time.

Design weights will be generated as the inverse of the selection probability for each business. A number of techniques are available for generating non-response weights. WERS used a combination of non-response modelling, where response behaviour is modelled using logistic regression (for example) and the weights generated directly by the model, and post-stratification, where adjustments are made to the sample to ensure the profile of the sample matches that of a set of external population estimates for a set of key characteristics. The specific approach used will depend on the amount of information available for responding and non-responding organisations; modelling approaches are only suitable where business-level information is available for both responding and non-responding organisations, such information is usually taken from the sampling frame.

Design effects

The design effects will be affected by the weights (design and non-response weights) applied to the survey data and (where applicable) any clustering of the sample.

In the design outlined above, the design effects due to design weights at wave 1 for large businesses only would be equal to 1.00, implying the effective sample size is the same as the actual sample size. This is because, within each size band and business type, the sampling fractions (and therefore the design weights) are constant, since the sample is drawn proportional to sector and region.

The design effects due to design weights increase if the sample includes both medium and large businesses and these are combined during analysis. This is because the sampling fractions, and therefore design weights, vary by size. For wave 1 the design effects due to design weights for the combined sample of large and medium businesses is equal to 2.45, implying an effective sample size of 537 (41% of the actual sample size of 1,319). However, if conducting analysis within each size band, the design effects due to design weights will be equal to one.

4.7 Survey outputs and reporting

In the consultations, it was generally felt that a range of outputs would be helpful to meet the needs of different stakeholders and data users, including data tables and cleaned data files (including SPSS formats), summary and detailed written reports and infographics. Large organisations felt that benchmark style reports or infographics would help maintain their interest in the study, and potentially help them to enact best practice.

One of the advantages of a longitudinal design is that it will enable DCMS to accurately track real change in behaviour over time. Analytical techniques can be used for the longitudinal data, for example showing firm-level change in large organisations' cyber security behaviours and the experience of a breach over time. One of the dangers of a longitudinal survey is the risk of panel conditioning, where

those interviewed become less like the population they are supposed to represent purely because of their participation in the survey.

In any reporting and analysis undertaken, care will need to be taken to avoid the risk of disclosure, especially given the focus on large businesses as there are small numbers in certain sectors.

5 Qualitative research

Alongside the quantitative longitudinal survey, it may be useful to include a small qualitative component, in order to probe specific issues in more depth. This would help to enhance the quantitative analysis by helping to understand the reasons behind organisations' policies and practices. As such, it could help to support or explain the analysis of causality that will be core to the longitudinal survey.

Qualitative interviews would be conducted with organisations that took part in the longitudinal survey, for example one to two months after the end of the quantitative fieldwork. Issues raised by stakeholders that could be covered qualitatively include: how organisations have developed cyber security practices and governance over time; how organisations are currently managing cyber security breaches and why they have implemented specific policies and practices; and facilitators and barriers of behaviour change (e.g. decision-making in relation to investment to improve cyber security). The qualitative interviews would have the flexibility to focus on particular topics of interest each year or surprising findings from the survey.

A disadvantage of this qualitative component is the additional burden on respondents which may affect participation in subsequent waves of the survey. However, given the small numbers concerned this would have very little impact on the overall response.

Annex 1: Questionnaire coverage in existing surveys

The table below identifies the topics currently covered quantitatively in existing data, and the strengths and weaknesses of these (e.g. in being able to explain changes over time), as well as their practicality.

Topic area	Survey	Detail	Overlap	Suitability for longitudinal survey
Organisation's online exposure	CSBS	Q6: Use of online systems, payment.		Potentially useful to monitor change over time, and how they relate to other measures (e.g. adoption of security practices; experiences of incidents/breaches).
Outsourcing of cyber security	CSS	Q7/13/14. - aspects of cyber security outsourced; functions outsourced.		Extent of outsourcing could be useful for analysis. Also, a longitudinal survey of large organisations may allow a deeper exploration of certain topics, e.g. what functions are outsourced, as well as other topics such as what is on policies (CSBS), what is included in training (cyber skills), incident response actions (CSBS), type of board involvement (FTSE 350). At the same time, the current CSS questions contain a lot of detail, so may need to be selective if included in a new survey.
Nature of cyber security strategy	FTSE350	Q4/7: Presence of cyber security strategy, extent to which this is aligned with business objectives, and how strategy is formalised/ communicated.	CSBS covers this in more detail (see 'Governance and planning')	In the last FTSE 350, almost all businesses had a strategy, so any future questions will need to focus on nature of strategy/what it covers. CSBS questions (see below under 'Governance and planning') are related but more detailed/specific.
Governance and planning	CSBS	Q29 - governance or risk management arrangements in place. Q30 – actions taken to identify risks. (checks, assessments, audits). Q31 – rules or controls in place. Q32 – aspects of policy.		Coverage of these issues is likely to be important as they may link with experience of breaches (CSBS report notes this possibility, although analysis is inconclusive).

Topic area	Survey	Detail	Overlap	Suitability for longitudinal survey
		Q33a – when practices last reviewed.		In CSBS, analysing correlations with breaches is not very successful, e.g. larger businesses are more likely to have identified breaches. This is possibly because larger businesses have more sophisticated alert systems, not because they have more breaches. Larger businesses also tend to take more action. This ends up meaning that the ones most likely to identify breaches are the ones that take more action to defend themselves – which is counterintuitive. So this is an example of where a longitudinal approach ought to provide more robust analysis than is possible through cross sectional survey. Note also that, at present, most large businesses already do all of the more basic things in CSBS, so a questionnaire focusing on larger businesses may need to focus on more sophisticated actions, in order to discern differences in behaviour. CSBS has included these types of activity at some point (although the low incidence in the business population as a whole means they haven't always been reported individually). Examples include use of threat intelligence, security monitoring, penetration testing, etc[25]. Q32 and Q33 may be more problematic as they will depend on respondent's knowledge/recall and (to some extent) interpretation.

[25] Note that the Deloitte 'Future of cyber survey 2019' also includes coverage of detailed procedures that businesses may carry out.

Topic area	Survey	Detail	Overlap	Suitability for longitudinal survey
Importance of cyber security among senior management	CSBS and FTSE 350	CSBS Q9: Cyber security priority for senior management. FTSE 350 Q8: Significance or importance to the board of the risk of cyber threats (in comparison to all risks the company faces).	Similar questions in CSBS and FTSE 350	These questions are important in the current surveys. Responses are subjective and may vary depending on the identity of the survey respondent (e.g. the answer given in FTSE350 by a member of the board may differ from the answer in CSBS given by a cyber security specialist).
Level of understanding among senior management	FTSE 350 and CSS	FTSE 350 Q5: Board's understanding of the company's critical information, data assets and systems. FTSE 350 Q6: Board's understanding of potential impacts from the loss of/ disruption to critical information, data assets and systems? FTSE 350 Q15: Understanding among individual Board members of how cyber risk relates to their personal legal and fiduciary duties. CSS Q32 – Understanding of issues among senior management (risks, requirements, etc).	FTSE350 Q6 similar to CSS Q32.	As above, responses may vary depending on the identity of the respondent. Possible issue of panel conditioning for these questions, as they are asking about awareness and understanding which may increase during a respondent's repeated participation in the survey. Questions are currently quite detailed; may be useful to simplify or select a key aspect of Board's understanding (i.e. if a specific aspect can be shown to have a bearing on other issues). The FTSE 350 report notes link between level of Board understanding and implementation of cyber governance measures but notes that "firm conclusions cannot be drawn about causality".
Communication with senior management	CSBS and FTSE 350	CSBS Q11: How often are senior management given an update on any actions taken around cyber security. FTSE 350 Q12: To whom in the company does the Chief Information Security Officer regularly report?	CSBS and FTSE 350 both cover this issue but focus of questions is different	CSBS question is potentially useful - CSBS report notes a strong positive relationship between prioritisation of cyber security and updates to the board. This is also a more objective and grounded question, which may be more robust in

Topic area	Survey	Detail	Overlap	Suitability for longitudinal survey
		Q13: Rating of information provided to the Board (related to cyber risk profile and management). Q14: Extent to which board challenges/approves information. Q22: How Board obtains assurance that cyber security strategy and procedures are fit for purpose		measuring trends over time (compared with more general, subjective questions). FTSE 350 Q14 also potentially useful – more grounded and objective, with discrete response options. Other FTSE 350 questions less suitable; e.g. any change over time at Q12 may reflect internal changes as opposed to meaningful change in cyber security procedures; Q13 is very subjective and answers are likely to vary depending on respondent identity; Q22 is an open ended question - hard to use for longitudinal analysis in current format. However, FTSE 350 report mentions link between whether board receives comprehensive information x whether CISO reports to them directly but notes that it cannot determine causality.
Awareness and behaviour among staff generally	CSS and CSBS	CSS Q34 – understanding of cyber security issues among core staff CSBS Q8 - staff use of personal devices for work.		CSS Q34 - potentially useful although currently quite a detailed question – may need to include selected items only. CSBS Q8 – also potentially useful for analysis.
Insurance policy	CSBS	Q23x/y - Insurance policy and what covered. Q23b – any insurance claims made.		Question would transfer successfully to longitudinal survey but depends on relevance to core objectives/needs. Note that a longitudinal survey of large organisations may be effective at measuring low incidence behaviour (e.g. insurance claims).

Topic area	Survey	Detail	Overlap	Suitability for longitudinal survey
Information sources	CSBS and FTSE 350	FTSE 350 Q16: Sources of advice and guidance used by company in managing cyber risk? CSBS Q24- sources of information used. Q24B – usefulness of govt information. Q24C – awareness of Cyberaware. Q24D – awareness of Govt schemes.	FTSE 350 Q16 and CSBS Q24 are similar	Questions on sources of information may vary depending on identity of survey respondent. Specific sources of information may become less relevant over time/list may need updating – so may be difficult to detect meaningful change over time. CSBS awareness questions may be less suitable for longitudinal survey (risk of conditioning).
Risk associated with software	FTSE 350	Q11: Whether Board recognises the risks associated with software.		Question asks about awareness, so risk of conditioning. Also, current question is very broad (yes/no), so may need to be revised.
Supply chain	CSBS and FTSE 350	CSBS Q45B – any work done to formally review risks of supply chain. FTSE 350 Q9 - Recognition of risk among board Q10: Tools used to enforce cyber security in supply chain.	FTSE350 and CSBS both cover this issue but focus of questions is different	CSBS question is potentially useful and is an objective, fact-based question. FTSE350 Q9 is quite broad (yes/no) and subjective. Also a risk of panel conditioning for this question. FTSE Q10 may be useful, although list of specific tools is likely to change, so may be difficult to detect meaningful change over time.
Impact of GDPR	FTSE350	Q17: Impact of GDPR on how the Board manages cyber risk.		Question linked to introduction of GDPR, so trends over time in future may become less useful.
Experience of breaches or attacks	CSBS and FTSE 350	CSBS Q53A – any breaches/attacks, including type, in last 12 months. Q54 – frequency. Q56A – outcomes of breaches. Q57 – impact of breaches. Q59 – cost of breaches. FTSE 350 Q18: Has the company experienced a major cyber-attack or	CSBS Q53a is a more detailed version of FTSE 250 Q18	Key issue, relevant for longitudinal survey. In a longitudinal survey, respondent recall is particularly important - need to place any attacks in the correct timescale. Number/frequency of incidents is likely to be important, as longitudinal survey will be able to assess how this has changed over time, e.g. whether certain types of organisation

Topic area	Survey	Detail	Overlap	Suitability for longitudinal survey
		incident in the last 12 months?		appear to be getting targeted more/less often. Cost of breaches (and of the most disruptive breach – see below) can be examined more robustly in a longitudinal survey than is currently possible in CSBS - it's very difficult for a cross-section survey to actually say if costs are going up or down over time and/or link this to actions taken.
Most disruptive breach or attack	CSBS	Q64A - What kind of breach was this? Q65 – how was it identified? Q71 – how long to restore to normal? Q75A – cost of direct results. Q75C – cost of recovery. Q75E – cost of long-term effect. Q75G – senior management aware of breach? Q76 – reported outside the organisation? if so, who to. Q78 – what is done to prevent further breaches.		Questions are potentially useful, but current questions include a lot of detail which may be outside scope of a new survey.
Response planning	CSBS and FTSE 350	CSBS Q63A – items in place for when breach is experienced. FTSE 350 - Q19 – whether response plan in place. Q20 How often test plans. Q21- board participation in crisis simulation.	FTSE 350 and CSBS both cover this issue – CSBS covers response plan in more detail	These questions are potentially useful, for analysis against experience of attacks/breaches. CSBS Q63a has more detail than FTSE 350 Q19 which is a broad yes/no question – so may be more sensitive to change over time.
Profile of staff involved in cyber security	CSS	Q16a/17 - Job role and team, numbers involved in cybersecurity. Q18a/b/c. pathway – entry into role. Q19 & Q20 – profile / characteristics of people working in cyber security. Q22-24 - cyber security-related qualifications or training.		Questions on number of staff involved in cyber security and overall figure for presence of qualifications/training may be useful for analysis. Other questions are very detailed, may be outside scope of a new survey.

Topic area	Survey	Detail	Overlap	Suitability for longitudinal survey
Role of cyber security staff and skills	CSS	Q26/Q27 – formal/informal role and cover arrangements. Q28 – importance of skills. Q29 – confidence in carrying out technical tasks. Q30 – confidence in communication or managerial tasks (e.g. risk assessment). Q31 – knowledge.		Q30 may be useful if it can include selected items only/simplified. Otherwise, questions are likely to be too detailed and specific for a new survey.
Training and upskilling	CSS	Q35 – Understanding of cyber security training and skills needs. Q36 - formal analysis of organisation's cyber security skills or training needs. Q37a/b – training carried out and type. Q42 - How much current training meets overall training and skills needs.		As above, questions are likely to be too detailed and specific for a new survey.
Recruitment and retention	CSS	Q43 – Recruitment of staff to fill any cyber skills needs Q44 – recruitment methods used Q45 – vacancies in cyber security roles Q46/47 – hard to fill vacancies and reasons Q47a – any changes to recruitment processes		As above, questions are likely to be too detailed and specific for a new survey.

Summary of questionnaire coverage in other existing Cyber Security Surveys

There are two additional existing studies that explore cyber security issues: Hiscox Cyber Readiness Report (2019); and Deloitte Future of Cyber Survey (2019).

The **Hiscox Cyber Readiness Report** is a survey of businesses in seven countries, which includes coverage of the following issues, which may be of relevance to the proposed survey:

- **Supply chain**: whether cyber-attacks are a result of a weak link in their supply chain; inclusion of cyber KPIs in their contracts with suppliers; and how often they evaluate the security of their supplier networks.
- **Costs of cyber-crime** to the business (over 1 year period), cost per incident. Overall spending on IT.

- **Cyber readiness model** – this measures how closely firms match up to what counts as best practice. Respondents are asked a series of questions covering their approach in four areas – strategy, oversight and resourcing on the one hand and technology and process on the other. They are invited to say how closely their way of doing things aligns with a well-structured, rigorous and effective approach.

The **Deloitte Future of Cyber Survey** captures cyber reporting practices of FTSE 100 companies, as well as board ownership of cyber security matters. The report provides relatively general data on boards' specialist expertise on cyber, the share of companies having contingency, recovery and mitigation plans, as well as some statistics on the number of companies suffering from breaches.

Coverage is as follows (underlined points are potentially most relevant for the proposed survey):

- Top ranked digital transformation initiatives for the next 12 months
- Most challenging aspects of cybersecurity management across enterprise infrastructure (Shadow IT, Cyber transformation, Cyber hygiene, Hybrid IT)
- Average percentage of time spent addressing various cyber domains (e.g. Cyber monitoring and operations, Cybersecurity governance, Cyber resilience)
- Organizations' cyber budget (% on items e.g. Data security, Infrastructure security, Cyber transformation)
- What is the most challenging aspect of cyber security management across your organization? (e.g. Data management complexities, Better prioritization of cyber risks across the enterprise, Rapid IT changes, Lack of skilled cyber professionals, Lack of management alignment on priorities, Lack of adequate funding, Inadequate governance across organization)
- How frequently cybersecurity issues are on board's agenda (similar to FTSE 350)
- How cyber investment decisions are evaluated (e.g. risk quantitative tools; the experience of their cyber leadership or cyber maturity assessments).
- To whom does the CISO typically report in your organization? (Overlap with FTSE 350)
- Nature of Cyber department's interaction with other business units (e.g. Through security assessments or audits; Through security steering committees that work with businesses; Through separate security organizations within each business; Through security liaisons/champions within each business).
- What percentage of their workforce supporting cybersecurity are full-time employees versus contractors and consultants
- Percentage of outsourced cybersecurity operations

- Type of Cybersecurity functions outsourced to third parties
- Greatest challenge managing application security risks (Lack of appropriate organizational structure to enable the integration of security into application development life cycle, Lack of prioritization/awareness of cyber risks that could impact the solutions being developed, Lack of tools or solutions that test and analyze software vulnerabilities)
- Organizational approach to agile/DevOps (We have fully adopted Agile/DevOps ,We have adopted in a limited capacity, We continue to leverage traditional waterfall approach to software development and deployment)
- Top ranked cyber defence priorities and investment areas among total participants (Security orchestration and automation, AI-driven threat assessment/identification, Scaled cybersolutions, Zero trust networks, Technical resilience, DevSecOps)
- Top criteria used to assess potential infrastructure management and cyber risk management partners (e.g. Opportunities to outsource foundational cyber defence capabilities)
- Top ranked internal/enterprise identity security initiatives (e.g. Privileged identity/ privileged access management (PAM))
- Preferred way to procure, implement, and provide ongoing delivery of identity capabilities (e.g. On-premise implementation with in-house/ contractor resources)
- Top three ranked most concerning cyber threats among total participants (Data integrity, Actions of well-meaning employees, Technical vulnerabilities)
- Number of sensitive production data disclosures within test and development environment in the last 12 months
- Timing of most recent cyber incident or breach among total participants (last year, 1-2 years, longer ago)
- Biggest impacts of cyber incidents or breaches on organizations (e.g. Loss of revenue due to operational disruption)
- Methods for reviewing and testing cyber incident response processes and procedures (e.g. Annually review and update response and business continuity procedures)
- Whether plan to leverage their incident response (IR) processes to handle data destruction attacks that use advanced tactics.

Annex 2: Profile of large organisations

Interviews achieved by sector

Sector	Interviews
Administration or real estate	1
Finance or insurance	1
Professional, scientific or technical	1
Education (excluding public sector)	1
Food or hospitality	1
Health, social care or social work (excluding NHS)	1
Retail or wholesale (including vehicle sales and repairs)	1
Charities	2
Total	***9***

Interviews achieved by number of employees (including volunteers and trustees for charities)

Number of employees	Interviews
More than 250, but less than 1,000	6
1,000 or more	3
Total	***9***

Annex 3: Summary of main surveys

Study	Sponsor	Years/ waves	Longitu-dinal?	Aims/coverage	Sample population
Longitudinal Small Business Survey (LSBS)	BEIS	Annual, 2015 onwards	Yes	Business characteristics and performance	UK-based enterprises with 0-249 employees
Large Business Survey (LBS) and Large Business Panel Survey (LBPS)	HMRC	Annual: LBPS 2010-2014; LBS 2015 onwards	LBPS: Yes LBS: Not explicitly	Understand large business customers' experience of dealing with HMRC	UK large businesses (defined re. HMRC customer groupings)
FTSE 350 Cyber Governance Health Check	DCMS	Annual 2013-2018	No	Board understanding and involvement in cyber security risk management measures	UK largest businesses, specifically those listed in the FTSE 350
Cyber Security Breaches Survey (CSBS)	DCMS	Annual, 2016 onwards	No	Awareness, attitudes and approaches to cyber security, nature and impact of breaches	UK private companies or non-profit organisations with more than one person on the payroll
Cyber Skills Surveys (CSS)	DCMS	2018 and 2019	No	Cyber security skills gaps and training	UK businesses, charities and public sector bodies
Workplace Employment Relations Survey (WERS)	BEIS	c. every 5 years 1980-2011	Part	Employment relations practices	workplaces in Britain with 5 or more employees
Commercial Victimisation Survey (CVS)	Home Office	Annual since 2012	No	Extent of crime against business premises	England and Wales, specific industry sectors
Mid-size business customer survey	HMRC	2015, 2016	No	Experience of dealing with HMRC	UK businesses with turnover of £10m or more and/or more than 20 employees
IAB Establishment Panel	IAB	2018	Yes	Employment development, use of technology, training	Establishments in Germany with 1+ employees

Annex 4: Surveys and publications

The review draws on the following studies and publications:

- Longitudinal Small Business Survey (LSBS) (BEIS)
- Large Business Panel Survey (LBPS)/Large Business Survey (LBS) (HMRC)
- FTSE 350 Cyber Governance Health Check (FTSE 350) (DCMS)
- Cyber Security Breaches Survey (CSBS) (DCMS)
- Cyber Skills Survey (DCMS)
- Bank of England Decision Maker Panel Survey (Bank of England)
- National Small and Medium Sized Business Survey (University of Cambridge)
- Workplace Employment Relations Study (WERS) (BIS, ESRC, Acas, UKCES, NIESR).
- Mid-size business customer survey (HMRC)
- Establishment Panel (IAB)
- Commercial Victimisation Survey (CVS) (Home Office)

References

Biewer, P, Pitts, A, Aspinwall, K. (2007) *Do Monetary Incentives Increase Business Survey Response Rates? Results from a Large-Scale Experiment*.

Cycyota, C and Harrison D. (2002) *'Enhancing survey response rates at the executive level: are employee or consumer-level techniques effective?'*, Journal of Management, 2002 vol 28 no 2

Deloitte (2019) *The Future of Cyber Survey 2019*
https://www2.deloitte.com/za/en/pages/risk/articles/2019-future-of-cyber-survey.html

Department for Business, Energy & Industrial Strategy (2020) *Business Population Estimates*, published online (accessed 30 March 2020)
https://www.gov.uk/government/collections/business-population-estimates

Department for Business, Energy and Industrial Strategy, *Small Business Survey reports* (website, accessed 30 March 2020)
https://www.gov.uk/government/collections/small-business-survey-reports#2018

Department for Business, Innovation and Skills, National Institute of Economic and Social Research, Advisory, Conciliation and Arbitration Service (2015) *Workplace Employee Relations Survey, 2011*. [data collection]. 6th Edition. UK Data Service. SN: 7226
http://doi.org/10.5255/UKDA-SN-7226-7

Department for Digital, Culture, Media & Sport (2019) *FTSE 350 Cyber Governance Health Check 2018*
https://www.gov.uk/government/publications/cyber-governance-health-check-2018

Department for Digital, Culture, Media & Sport (2019) *Cyber Security Breaches Survey 2019: Technical Annex*
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/802623/Cyber_Security_Breaches_Survey_2019_-_Technical_Annex.pdf

Department for Digital, Culture, Media & Sport (2020) *Cyber Security Breaches Survey 2020: Technical Annex*
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/874693/Technical_annex_-_Cyber_Security_Breaches_Survey_2020.pdf

European Central Bank (2019) *Survey on the access to finance of enterprises Methodological information on the survey and user guide for the anonymised micro dataset*
https://www.ecb.europa.eu/stats/pdf/surveys/sme/methodological_information_survey_and_user_guide.pdf?ecdc7494b2abc88048ce44465a60be2b

Forth, J. (2008) *Methodological Review of Research with Large Businesses, paper 6: methods for longitudinal panel surveys* (HM Revenue and Customs)

Hales, J and O'Connor W. (2008) *Methodological Review of Research with Large Businesses, paper 3: data collection* (HM Revenue and Customs)

Hiscox (2019) *Hiscox CyberReadiness Report 2019*
https://www.hiscox.co.uk/sites/uk/files/documents/2019-04/Hiscox_Cyber_Readiness_Report_2019.PDF

HM Government (2016) *National Cyber Security Strategy 2016-2021*
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf

Home Office (2019) *Crime against businesses: findings from the 2018 Commercial Victimisation Survey*
https://www.gov.uk/government/statistics/crime-against-businesses-findings-from-the-2018-commercial-victimisation-survey

IFF Research (2014) *Large Business Panel Survey 2013* (HM Revenue & Customs)

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/318936/report312.pdf

IFF Research (2016) *Large Business Survey 2015* (HM Revenue & Customs) https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/536555/Large_Business_Survey_2015.pdf

IFF Research (2018) *Employer Skills Survey 2017 Technical report*, Department for Education https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/733999/Employer_Skills_Survey-Technical_report.pdf

Ipsos MORI (2010) *Large Business Methodology Review: Stage 2 report* (HM Revenue and Customs Research Report 98) https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/344925/research-report98.pdf

Ipsos MORI (2019) *Commercial Victimisation Survey Technical Report 2018* https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/828770/commercial-victimisation-survey-technical-report-2018.pdf

Ipsos MORI (2020) *Cyber security skills in the UK labour market 2020: Technical Report* (Department for Digital, Culture, Media & Sport) https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/870107/Cyber_security_skills_in_the_UK_labour_market_2020_technical_report.pdf[26]

Kantar Public (2017) *Mid-size Business Customer Survey Wave 2: 2016*, HM Revenue and Customs Research Report 475 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/708599/Mid-Size_Business_Survey_2016_-_HMRC_Research_Report_475.pdf

Lynn, P. (2009) *'Methods for Longitudinal Surveys' in Methodology of Longitudinal Surveys*

Smith, P. and Yung, W. (2019) *A review and evaluation of the use of longitudinal approaches in business surveys* https://eprints.soton.ac.uk/432022/1/Longitudinal_approaches_in_business_surveys_AAM.pdf

[26] This is referred to in document as Cyber Skills Survey. Please follow the link for more details on CSS