Response to open consultation on

Proposed changes to the Cyber Security Breaches Survey

On behalf of the UK Computing Research Committee, UKCRC.

Prepared by: Professor Chris Johnson,
School of Computing Science, University of Glasgow, Glasgow, G12 8RZ.
http://www.dcs.gla.ac.uk/~johnson

The UK CRC is an Expert Panel of all three UK Professional Bodies in Computing: the British Computer Society (BCS), the Institution of Engineering and Technology (IET), and the Council of Professors and Heads of Computing (CPHC). It was formed in November 2000 as a policy committee for computing research in the UK. Members of UKCRC are leading researchers who each have an established international reputation in computing. Our response thus covers UK research in computing, which is internationally strong and vigorous, and a major national asset. This response has been prepared after a widespread consultation amongst the membership of UKCRC and, as such, is an independent response on behalf of UKCRC and does not necessarily reflect the official opinion or position of the BCS or the IET.

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.

   [1.1] The UK Computing Research community uses the breach report in a number of ways. It helps to provide the context for academic papers, it is used to motivate research projects and is frequently cited in the impact sections of grant applications, it may also be used to provide a baseline for quantitative studies in reporting behaviour. Finally, it can also form part of statistical analyses used to triangulate with other forms of corroborative evidence.

   [1.2] Limitations with the annual breach report include the way in which it only provides a snapshot each year given that the participants are not the same between editions. The estimation methods are poor and governed by processes in organisations that are changing

   [1.3] Methodological concerns, noted in the consultation and [1.2], typically mean that the data in the breach report tends only to be used to illustrate general trends. It is rarely used as a primary source in research studies unless confirmed by other independent sources – including the Verizon report or those issued by DHS/NIST.

2. Which elements of the survey do you use in your work?

   [2.1] Many different sections of the breach report are used by the research community. For instance, material relating to the distribution of reported attacks across sector are used to justify further work with healthcare organisations, charities or small to medium businesses. The sections dealing with the engagement of senior management have justified research into human aspects of cyber security. Many aspects of the cyber breach report are used together with other documents published from across government – for instance the NAO reporting in the National Cyber Security Strategy, to develop further metrics and to establish methods of assessing the cyber maturity of UK organisations.

   [2.2] The broad ranging nature of the data provided in the annual breach report is useful in reminding the wider UK Computing Research Community of the socio-technical nature of many cyberattacks and also the dimensions along which it is important to engage both with policy and with industry needs.

3. How frequently do you use the information?

   [3.1] It is impossible to provide an accurate assessment of the frequency of use of data within the annual report. However, it would be rare to find a UK senior academic with an interest in cyber security who has not read the most recent edition of the report.

Future CSBS, questions and topic coverage

4. Are there any questions or topic areas you would like to see included in future?

   [4.1] Given the growing importance of the Cyber Council[1], it would be useful to have an annual reflection both on the relevant cyber security qualifications held within UK organisation but also the perceived value of the associated training.

   [4.2] The survey might also be used to identify those areas that UK organisations perceive to require further research/development.

   [4.3] It would be useful to determine the frequency of breaches that might have worst plausible consequences including safety concerns.

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?

   [5.1] The UK Computing Research community is engaged in a broad range of projects that draw from and extend the annual survey. Some such as PETRAS benefit directly from

[1] https://www.theiet.org/impact-society/uk-cyber-security-council-formation-project/

DCMS involvement. Others can be contacted either through UKCRC or via the NCSC Research Institutes and Centres of Excellence.

[5.2] These projects tend to develop new forms of automated detection; others look at specific aspects of breaches including the human factors elements or the deployment of hardware mitigations. The UK also has a leading position in the formal, mathematical analysis of breaches.

[5.3] A common theme across UK cyber security research projects is less to duplicate the breach report but to use it to inform the counter measures that make future breaches less likely or to mitigate the consequences of any future attacks.

6. Would you be negatively impacted if CSBS were discontinued in its current format?

   [6.1] Yes. Given methodological concerns over the breach report and the availability of alternate sources, discontinuing the report would have an impact more than "minimal" but no more than "significant".

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.

   [7.1] The other sources mentioned in [6.1] may be less reliable and often not derived from UK organisations. Hence there is a danger that the UK Computing Research community might mistakenly invest efforts in addressing problems that are more significant in the US or in continental Europe through lack of comparable UK statistics.

   [7.2] The NAO report into the UK National Cyber Security Strategy criticised the difficulty in identifying any KPIs that might be used to assess value for money form the significant public funds invested in this area. If the survey is discontinued then careful thought must be given to the wider issues raised by the NAO especially where they relate to the renewed national strategy.

8. Would you use a potential longitudinal survey of large organisations' cyber security and governance practices?

[8.1] Yes. Longitudinal studies provide greater assurance so long as the questions can be issued to a consistent sample of organisations and those questions are interpreted in a consistent manner. Longitudinal studies would, however, measure something quite different from a random annual snapshot and raise different concerns. Longitudinal studies might, for example, cease to be considering a representative sample over time. This is not, therefore, an either/or situation, rather it might be better to say that adding a longitudinal element would strengthen the overall methodology.

[8.2] The UK Computing Research Community is skilled in the development and, more importantly, in the validation of longitudinal surveys to address some of the methodological concerns raised in the consultation and echoed by the NAO.

9. If yes to Q8, what questions or topic areas would you like to see included?

[9.1] Perceptions of the risk from different threat actors over time.

[9.2] Cost/benefits of cyber security qualifications.

[9.3] Areas of potential research opportunity.

10. If yes to Q8, how do you envisage that you would use these statistics?

[10.1] As mentioned previously, the breach report provides important background data that is used to direct UK research projects. In many cases those projects involve close cooperation with particular UK businesses, charities and public bodies. The breach report helps to establish that their specific concerns are reflected more widely and hence are deserving of public funds to support research.

Other comments and re-contact

11. Do you have any other comments, not covered by the questions above?

[11.1] None

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.

[12.1] Yes