RISCS Research Institute for Sociotechnical Cyber Security

Workshop Note: Optimising the use of UK Government survey data on cyber security

The Research Institute for Sociotechnical Cybersecurity (RISCS) held an online policy workshop on 22nd July 2021 with 28 participants from Government, academia, law enforcement and the cyber sector as part of the Quantification and Cyber Risk Fellowship theme led by Fellow Dr Anna Cartwright.

Context

The aim of this two-hour session was to identify policy relevant research questions which can be answered using accessible government datasets —such as the Cyber Security Breaches Survey (CSBS) and the Longitudinal Small Business Survey (LSBS) — and to understand the barriers researchers face when looking to use government datasets. The workshop was designed around several starting questions provided by the Department for Digital, Culture, Media and Sport (DCMS) and the National Cyber Security Centre (NCSC), which they had identified as priorities for this workshop.

This report summarises the workshop discussions and the next steps for the Quantification and Cyber Risk Fellowship theme.

Starting questions

1. What behaviours/ policies/ processes have the biggest impact on improving an organisation's cyber security? (i.e., reducing the likelihood of breaches and attacks. number or frequency of incidents/ impact of breaches in terms of cost, recovery time etc.). Are there key areas that government should be seeking to focus on for improvement?

2. How can we demonstrate the overall cyber risk level to the UK economy? What is the evidence base that this is a serious threat to UK industry?

3. How can we best measure the impact of government interventions on improving organisations' cyber security? What can we demonstrate about the cumulative impact of UK government's interventions on the state of organisation's cyber security so far and how can our understanding of this be improved?

4. How can we enable organisations to take data driven decisions about their cyber security?

5. How can organisations use data like that found in the CSBS and use it to inform what they do next?

6. Could data from the CSBS help us understand the efficacy and impact of cyber security measures?

7. Can we form a picture of what controls an organisation has in place and understand what this means for their outcomes and the support we can provide them?

Discussion on the starting questions

During the opening session, DCMS and NCSC colleagues explained their starting questions in more detail and provided context on their current priorities. Participants reflected on these questions before discussing as a group. The questions and ideas are grouped as follows: 1. Cyber Essentials certification; 2. organisational understanding and motivation; and 3. capabilities of the survey data.

1. Cyber Essentials Certification

The Government-backed 'Cyber Essentials' certification scheme was raised in relation to several of the starting questions around the effectiveness of interventions and policies that aim to improve cyber security.

Suggested additional questions for researchers to explore included:

- Does having Cyber Essentials lead to a change in behaviours (and reduced cyber incidents) in organisations or is it just a 'box ticking' exercise?
- Has the scheme led to a change in risk management, or compliance management?
- Is Cyber Essentials take up by organisations a good way to measure impact?
- Has there been an increase in organisations taking Cyber Essentials? And what proportion achieve the certification?
- How much better are organisations with Cyber Essentials at reducing the impact of incidents than those without it?

2. Organisational understanding and motivation

Participants suggested that studying the level of understanding that organisations have about cyber security could provide useful insights for policymakers. Research into what motivates organisations to implement cyber security measures into their business practice was also put forward in group discussions

Suggested additional questions for researchers to explore included:

- Do organisations understand the complexity and fast-moving nature of cyber security?
- Where do Small and Medium Enterprises (SMEs) turn for advice upon recognising that their organisation lacks an individual competent in cyber security?
- How do we know that people answering survey questions (e.g., CSBS) on behalf of their organisation have adequate cyber security knowledge (particularly in SMEs which may lack expertise due to their limited resources)?
- Would storytelling (such as hearing from others on their experiences of breaches, or reading news stories on breaches) be more impactful in understanding cyber security than the current 'checklist' approach?
- What motivates organisations to take steps to improve their cyber security?

3. Disaggregating the data by organisational size, type, and sector

Some participants strongly felt that it would be important to investigate effects according to organisational size, type, and sector (rather than looking at averaged results across all survey respondents) since the motivation to improve cyber security and ability to do so are likely to vary significantly according to the nature of the organisation concerned. There might also be benefits of providing assessments on a sectoral basis, so that each sector can seek to maintain alignment with peers to drive improvements.

Suggested additional questions for researchers to explore included:

- What has been the impact of government interventions by organisation size?
- Are organisations currently making use of data to inform their cyber security decision making? How does this vary according to organisational size, type, and sector?
- Alongside assessing the impact of government interventions, how can we understand impacts of a breach on an organisation? For example, these would differ greatly between a shop and a petrochemicals plant.

Barriers to researchers using government datasets

To provide context for a discussion on the challenges facing researchers using government data, participants heard from two researchers with experience of undertaking such research: Professor Steven Furnell, Professor of Cyber Security, University of Nottingham, and Professor David Wall, Chair in Criminology, University of Leeds. Professor Furnell reflected on his experiences of using CSBS data and some of the challenges in analysing self-reporting survey data. Professor Wall discussed the 'data paradox', whereby organisations recognise the need for data to inform cyber security but are reluctant to share their own data.

Participants were then asked to consider barriers faced by researchers using government data sets, which concerned: the reliability of the data, challenges in analysing, sharing and anonymity of survey data responses, and the questions themselves.

1. Methodological concerns

Participants raised a number of queries relating to the methodology used to recruit participants to the surveys, including:

- How representative are the respondents?
- Are self-reported answers reliable, particularly if respondents lack awareness or understanding of cyber security data (particularly in SMEs)?

Participants also noted that the questions asked in the survey have changed each year since it was introduced, which presents challenges for examining trends over time. Participants suggested that it might be useful to create a roadmap or baseline for cyber security which provides targets for organisations to aim for.

2. Challenges presented by anonymity

Participants recognised that summarising datasets or anonymising them is attractive because assurances can be given to survey participants. However, they also argued that it could be useful to have access to a complementary data set with potentially identifiable information for use under restricted conditions like a Secure Lab. This would allow for linking across surveys as with the LSBS "Secure Access" Version.

- Is consent from respondents required for sharing any parts of the data outside of DCMS for research purposes?

3. Limitations of the survey data

As described above, the desirability of distinguishing between SMEs and large organisations, as well as between organisation type and sector in these datasets was strongly emphasised by participants. For example, the CSBS currently only provides a broad definition of the sector and more specific detail, alongside location information, would be useful.

Participants also raised questions around how much government data can tell us and suggested ideas for what other data or information might be useful to paint a fuller picture. Suggestions included:

- Conducting an annual survey to examine a change in knowledge and understanding of cyber security.
- Looking to international datasets or initiatives as additional sources or inspiration for new approaches.
- Exploring whether there are complementary data sets in the private sector that could be made available.
- Finally, the formatting of the data was highlighted as another potential barrier. Currently, data needs to be prepared for analysis (for example by combining datasets from different years or different surveys)

Final questions

- What behaviours, policies or processes have the biggest impact on improving an organisation's cyber security as measured by likelihood and impact of breaches and attacks?
- Has Cyber Essentials worked? What gaps do organisations with Cyber Essentials have? Are organizations with Cyber Essentials less likely to be attacked? Has take-up of Cyber Essentials increased?
- What can we demonstrate about the cumulative impact of UK government's interventions on the state of organization's cyber security? Does impact differ by sector or by size of organisation?
- How can organisations use data like that found in the Cyber Security Breaches Survey to inform what do they do next?
- How can we demonstrate the overall cyber risk level to the UK economy? What is the evidence base that this is a serious threat to UK industry?
- Where do organizations (SMEs) turn to for advice? Are SMEs taking up appropriate cyber security services?

to be usable by researchers and there is a lack of resource to do this. Participants questioned whether it could be possible for the Government to share analysis-ready data to minimise the burden on academic resources.

4. Challenges relating to the nature of the questions

While participants could understand the motivation behind the questions that had been posed by DCMS and NCSC, researchers also wanted to manage expectations and pointed out that it is difficult to measure the impact of policy interventions. As cyber security is fast moving with many variables, it is hard to be sure any single intervention has caused a change. It is equally challenging to measure things that aren't happening (such as cyber-attacks that have been prevented). One idea was to take inspiration from the safety literature (i.e., the Health and Safety Executive), which similarly faces these practical difficulties (for example, in estimating how many health and safety incidents have been avoided as a result of certain interventions).

Participants by organisation

- Cambridge University
- Coventry University /Oxford Brookes University
- CyberSmart
- Department for Digital, Culture, Media & Sport
- De Montfort University
- University of Kent
- IPSOS Mori
- Lloyds Register Foundation
- National Cyber Security Centre
- RISCS Advisory Board
- Royal United Services Institute
- UCL
- University of Leeds
- University of Nottingham
- West Midlands Police Regional Organised Crime Unit

Next steps

During the final activity, participants were asked to consider which of the questions would be feasible to answer with existing data sets. These views were used to finalise a list of questions (see 'final questions' box) which are the subject of a competition for PhD students and early career researchers to encourage cyber security research and analysis that addresses these questions. The competition details can be found on the RISCS website.

Successful competition entrants will have the opportunity to present their work to the RISCS community in Spring 2022. This session will provide an opportunity to assess progress and review steps to be taken to increase use of government survey data.

Contributors

This workshop and report were produced in partnership with UCL Engineering's Policy Impact Unit (PIU) as part of the Research Institute for Sociotechnical Cyber security (RISCS) Fellowship on Quantification & Cyber Risk led by Dr Anna Cartwright, Oxford Brookes University. This workshop series on the RISCS Fellowship themes is funded by the UCL EPSRC Impact Acceleration Account and by RISCS.

The team is particularly grateful for contributions from NCSC & DCMS in providing the starting questions for this workshop and engagement with the project.

Contact us

Dr Anna Cartwright, RISCS Fellow in Quantification & Cyber Risk, a.cartwright@brookes.ac.uk
Principal Lecturer in Accounting, Finance and Economics, Oxford Brookes University

For more information on the PIU, please visit https://www.ucl.ac.uk/steapp/collaborate/policy-impact-unit-1