discribe
IMAGINING SECURE DIGITAL FUTURES

INDUSTRIAL STRATEGY

UKRI Economic and Social Research Council

Call for Scoping Reviews

ESRC Digital Security by Design Social Science Hub+

The DiScriBe Digital Security by Design Social Science Hub+ is an ESRC-funded Hub+ that forms part of the wider Industrial Strategy Challenge Fund (ISCF) "Digital Security by Design" programme. The Hub+ supports the wider DSbD challenge by applying social and economic science to core questions around the adoption of new secure technologies, the readiness of different sectors (and roles) to adopt new secure hardware, the regulatory and policy environment and how that might influence the adoption of DSbD Tech, and what social and cultural factors might influence the success of the wider DSbD ecosystem. Our goal is to support the widespread adoption at scale of DSbD technologies.

DiScriBe was established in September 2020 with funding from the ESRC, and is a consortium of four academic institutions: the Universities of Bath, Bristol and Cardiff, and Royal Holloway, University of London. More information is available at: https://www.discribehub.org

This commissioning call is for scoping activities around our four key topic areas, with the goal to understand the current state of knowledge and current areas with no evidence base. We expect submissions to be in the form of systematic literature reviews, meta-analyses, evidence gap analyses or systems approaches to summarising connections between events but would welcome other creative methods that would address the topics and questions outlined below. The total funding for this call is £200,000 (at 100% fEC), of which 80% will be funded by the Hub+.

Deadline: Submissions by 4pm on the 3rd Dec 2020 at: https://easychair.org/conferences/?conf=discribe2020

Funding panel meeting: 11th January 2021.

Decisions communicated: 15th January 2021

All funded projects must be completed, with all deliverables, by **31 July 2021.**

CALL TOPIC AREAS:

1) Economics of security hardware adoption: quantifying costs and benefits

Under this call topic area, we are seeking a review of existing methods for identifying and quantifying the costs and benefits of adoption of new security hardware and practices. The identification should be done under a broad scope, for instance the benefits should encompass reducing the expected loss in terms of direct and indirect costs of cybersecurity failure, and importantly, in addition to private costs, externalities should also be considered and analysed. Finally, in addition to objective assessments spanning all relevant dimensions and areas (i.e. markets for vulnerabilities, insurance markets, impact of cyber events on organizations' concurrent operations and on performance over the years, cost of stock price fluctuations, loss of consumers and cost of PR fallouts, etc.), the scoping should also comprehensively consider subjective perceptions and biases.

Indicative approaches / methods

We expect a combination of desk research (e.g. literature review) and interviews with relevant experts from a spectrum of relevant fields and industries (e.g. digital security, insurance markets, PR). Given the interdisciplinarity and diversity of prior research methods and focus, to maximize the value of these scoping activities, we would expect to see as a deliverable a database that enables every piece of research to be defined by a set of attributes, i.e. assumptions, methods, metrics, group of interest, type of cost/benefit, results, limitations and indicated directions of future research. Detailed structure should be described in the proposal.

This database should be designed to allow for the identification of best practices, groups and profiles of actors relevant to the adoption decision-making process, research gaps, areas of methodological consensus, and directions for future research. To maximize its usefulness, comparability in terms of unit of account is key, and where possible the relevant data sources should be listed. Marginal cost and benefit approach should be applied where possible. Finally, we welcome proposals that additionally include other approaches and attributes as value added (for instance, by illustrating via case studies).

Indicative Deliverables

1. Methodological report describing the approach used and its limitations.
2. Anonymised transcribed dataset from the interviews.
3. Structured database of existing methods for identifying and quantifying the costs and benefits for adoption of new security hardware and practices, including all the attributes mentioned above and where possible actual quantities (cost and benefit values, examples).
4. Recommendations on best practices and directions for future research.

2) Understanding secure and insecure practices across consumer chains of hardware security advances

Under this topic area, we require a systematic mapping of the consumer chains that will potentially utilise hardware security advances. The focus of the scoping research should be on understanding how secure (or insecure) practices currently manifest across the complex intersections inherent in these consumer chains. These consumer chains encompass infrastructure developers who aggregate a range of hardware and software services to deliver critical systems, e.g., smart city environments, smart grids, intelligent transportation, etc. as well as those who deliver consumer goods ranging from personal computers and devices to Internet of Things (IoT). An equally important aspect is developers and distributors of software and software-based services as well as end users who consume the functionalities offered by the infrastructures, devices and software. Hardware security advances are not a panacea for all insecure practices that manifest across the chain and we are aiming to establish where these may be best leveraged to mitigate insecure practices or enhance existing practices against the increasing sophistication of attacks.

Indicative approaches / methods

We anticipate that the mapping will take the form of both desk-based review of existing literature and case studies as well as interviews (10-20) and focus groups (at least 3) with stakeholders in the consumer chain. We anticipate a qualitative research methodology that leads to a rich understanding of current practices and where the Hub+ activities will provide the biggest value in terms of improving secure practices across the consumer chain. Applicants are welcome to propose alternative methodologies with clear justification of how these will deliver the expected deliverables.

Indicative Deliverables

- A report incorporating the literature review and case study descriptions and a full bibliography (in Bibtex) of the literature studied.
- Anonymised transcribed dataset from the interviews and focus groups.

- Report incorporating findings from the analysis of the data (literature review, case studies, interviews and focus groups) including the analysis methodology used and its limitations.

3) Regulation, Policy and Cybersecurity

We are seeking to commission research on the regulatory landscape within the UK digital security sector. The focus should be on the design and use of hardware security as part of digital products and services. The regulatory landscape encompasses legislation, standards and regulation.

In particular, the research should:

1. Outline the regulatory frameworks for the development and adoption of hardware security in the UK and discuss related regulatory challenges and opportunities (around equality, expectations, investments) as well as barriers and enablers of their adoption in both the inter-organisational (e.g. supply-chain) and intra-organisational contexts.
2. Review academic research on regulatory frameworks related to hardware security within the UK and beyond to identify key researchers, main thematic focus and the significant scholarship contributions to relevant regulatory frameworks and approaches.
3. Contrast and compare different regulatory frameworks   that may exist in hardware security and in digital security more generally , e.g. centralised vs decentralised (devolved). Illustrate these with specific cases as appropriate. SWOT analysis may be applied to carry out the analysis and evaluation of specific frameworks.
4. Examine whether there are different regulatory frameworks and approaches in different organisations taking account of different sectors (e.g. public vs private), size (e.g. large vs SME) and extent of digitalisation (e.g. born digital vs pre-digital).
5. Explore (using focus groups) how and in what ways key stakeholders think that the Digital Security by Design_might impact digital security's regulatory landscape.

Indicative approaches / methods

Both secondary (literature review) and primary data are expected to be used for this research. The latter may comprise interviews and/or focus groups with different stakeholders across different sectors (e.g. commercial, education, financial)

Indicative Deliverables

Deliverables: Initial project plan to show the different activities and the timings of the outputs

Deliverables: Mid-term project report.

Deliverables: 3-5 key stakeholder workshops to map the regulatory space relevant to digital security and evaluate the potential impacts of Digital Security by Design on that regulatory space.

Deliverables: Short write-ups from each workshop.

Deliverable: Report that provides an overview of the regulatory landscape, identifies the key regulatory stakeholders and actors and that summarises the core regulation documentation relevant to digital security.

4) Social and Cultural Differences in the Adoption of Security Technologies

We intend to conduct a survey to understand the difference between social, cultural and commercial barriers to adoption of secure tech (i.e. CHERI and associated hardware/software) between sectors. In preparation we need to identify the potential adopters of secure technology – from manufacturers and open source communities, to end users (private, public and third sectors). Specifically, given we cannot survey all sectors, we aim to identify which to focus on through a scoping exercise to determine those that will likely achieve the highest impact from secure technology adoption.

Indicative approaches / methods

We anticipate a combination of desk-based research (e.g. literature reviews or rapid evidence assessments) and qualitative interviews (e.g. semi-structured or focus groups) will be needed to identify the sectors most likely to benefit from the implementation of secure technologies. We anticipate the development of a framework to determine risk reduction potential. We would expect some qualitative interviews with highest / lowest impact sector industries to take place in order to validate their position in the ranking.

Indicative Deliverables

Report detailing a list of sectors, the forums they engage with online and offline to discuss and guide their decisions on the adoption of new tech, and a ranked risk assessment based on potential value-added by adopting secure technologies. Interview transcripts should be provided.

FUNDING

It is intended that the total amount available for this Call will be up to £200,000 at 100 per cent full Economic Cost (fEC), of which 80 per cent fEC (i.e., up to £160,000) will be made available to successful applicants. In practical terms this means that UK HEI researchers should cost their projects using the same process as they would cost a UKRI grant. All other applicants must recognise that an application to DiScriBe’s commissioning programme requires a commitment to provide the remaining 20% of full Economic Cost from their own resources. That is, DiScriBe will pay 80% of the total costs outlined within the proposal, with an expectation that the organisation covers the remaining 20%. All costs should be inclusive of VAT and/or any other applicable tax. A guide of fEC and the ESRC’s position on its payment is available at: https://www.ukri.org/files/funding/tcs/fec-questionnaire-pdf/

- The duration of work proposed under this Call should not last more than 6 months and should run between 1st February 2021 and 31st July 2021. DiScriBe will not reimburse costs associated with the development or submission of a proposal.

- All projects will be assessed on an individual basis against the Assessment Criteria outlined below.

SUBMISSION FORMAT

Please submit the proposal as a single PDF by **4pm on the 3rd December** using the form and upload system at: https://easychair.org/conferences/?conf=discribe2020. Submissions should not exceed four pages plus short CVs, comprising:

1) Your understanding of the problem (1 page max)

2) Your proposed methodology (1 page max)

3) Deliverables and timescales (1 page max)

4) Financial summary (divided into directly incurred and allocated staff costs, travel, subsistence and other costs, estates and indirect costs. (1 page max). Proposals should be costed and approved by the applicant's organisation before submission. The costings submitted should be at 100% full economic cost (fEC), but recognize that 80% of eligible costs will be funded. The costs should be in sufficient detail to allow for value for money judgements to be made.

Appendices:

Please attach short (2 page) CVs for all applicants and named researchers at the end of the proposal.

Eligibility

The Call is open to Higher Education Institutions, research organisations, charities, commercial companies, and individuals from the UK and overseas who can demonstrate a capability to deliver a high-quality programme of research. Interested partners without such experience should consider partnering with established research institutes. We strongly encourage applications from researchers in all disciplines, and encourage proposals that are interdisciplinary and that involve collaborations between stakeholders and researchers. **Researchers who have not traditionally worked in the cybersecurity domain** but believe their expertise may provide insights or new applications to the area, are particularly encouraged to apply. Eligible applicants may submit more than one proposal.

ASSESSMENT

The award of funding to proposals will be based on an independent evaluation. All proposals will be reviewed by at least three (3) expert peer reviewers, and then evaluated by a Commissioning panel comprising the DiScriBe director, a member of the DiScriBe executive team, and three external representatives drawn from academic and user groups. Members of the wider DSbD programme will be non-voting members of the panel. Applications that are not submitted in the format requested in above, or that are outside of the scope of this call, may be rejected without recourse to peer review.

Criteria

Submissions will be scored by peer reviews across four domains:

1) Understanding of the problem (weight: 1)

2) Appropriateness of proposed methodology (weight: 1.5)

3) Value for money and appropriateness of deliverables / impact plans (weight: 1.5)

4) Team track record, including inter-disciplinary nature of the team (weight 1)

Grant conditions

Successful applicants will receive an offer letter that will outline the terms of the sub-contract with DiScriBe. In the main these are standard UKRI terms and conditions, but with some minor amendments related to the source of funding and relationship with the DSbD challenge. **Applicants should make sure that these terms are acceptable to their organisation before applying to funding. The terms are not negotiable. Copies of the contract are available at:** http://www.discribehub.org/terms

Equality, Diversity and Inclusion

The long-term strength of the UK research base depends on harnessing all the available talent and the Research Councils together developed the ambitious UKRI Equality, Diversity and Inclusion Action Plan (https://www.ukri.org/files/legacy/skills/action-plan-edi-2016/).

In line with the UKRI's policies on equality, diversity and inclusion (https://www.ukri.org/about-us/policies-and-standards/equality-diversity-and-inclusion/), DiScriBe expects that equality, diversity, and inclusion are embedded at all levels and in all aspects of applicants' research proposals.

We are committed to supporting the research community in the diverse ways a research career can be built. This includes career breaks, support for people with caring responsibilities, flexible working and alternative working patterns. With this in mind, we welcome applications from researchers who job share, have a part-time contract, need flexible working arrangements or those currently committed to other longer, large existing grants.