discribe
IMAGINING SECURE DIGITAL FUTURES

Assessing Organisational DSbD Awareness and Readiness

Prof. Steven Furnell

Dr. Maria Bada

June 2023

University of Nottingham
UK | CHINA | MALAYSIA

Queen Mary
University of London

The Discribe Hub+ is funded by UKRI through ESRC
Grant no: ES/V003666/1
For more information about the Hub+ please visit
www.discribehub.org

UK Research and Innovation

Table of Contents

1 Introduction

Many attacks and exploits are possible because security has not been recognized and built into the system from the outset. This applies in both hardware and software contexts, and if such insecure components are then further incorporated into other products, then this can render the wider product vulnerable as well. With this in mind, it is increasingly recognized that security features and capabilities need to be built-in (by design) and they need to be the standard operating mode (by default). At the same time, and despite the potential advantages, organizations can face difficulties in terms of decision-making around the adoption of secure hardware (Tomlinson et al. 2022).

Security by design is a paradigm in which a system is designed with security in mind from the start, as opposed to taking an insecure system and plugging the holes, and is particularly relevant to the hardware context. However, one of the notable findings from prior stakeholder engagement (Benson et al., 2021) was that the awareness of hardware security was fuzzy in at least parts of the industry, which has implications for the readiness to adopt DSbD. At present, unless decisions happen to fall to people who are DSbD-aware, the benefit has potential to be missed or misunderstood. Moreover, even conceptual understanding was not sufficient to persuade stakeholders of the case for investment. As such, many potential beneficiaries require more specific evidence of the applicability to their context.

Although many executives and decision-makers are becoming aware of the significance of cyber security, decisions are often not proactive enough. Incentives can drive managers to protect organizational assets in the short-term at the expense of planning for the long-term (Srinidhi et al., 2015). A manager's perception of risk is driven by their organizational and information system environment, as well as individual characteristics (Straub & Welke, 1998). Therefore, the intuitive assessment of probability is often based on perceptual quantities that can often be biased (Tversky & Kahneman, 1974). Therefore, this can lead to the dangerous illusion of strong security. Although device-centric security is receiving relevant further attention in new legislative proposals (UK Parliament, 2022), it is falling short of requiring products to be based on DSbD principles. At the same time, while stronger forms of regulation would potentially force uptake, this could also generate resistance and impede innovation, and still does not assist adopters in understanding their own needs. What is preferable is for adoption of DSbD-based solutions to become part of a wider culture and mindset, integrating it within the processes and practices of a business.

For DSbD to be adopted in an informed manner requires related awareness and expertise from the organization. As such, a business considering the adoption of (and investment in) DSbD solutions faces two important questions: is the investment needed and is it going to work? While the former depends upon the nature of the security requirement, the latter will ultimately be affected by the organizational context and culture.

1.1 Project aims and deliverable focus

The key contributions of the overall project were originally proposed to address:

- Insights into the awareness, understanding and perception of DSbD amongst relevant potential adopters and beneficiaries. In particular, the work will seek to identify key factors and linkages that potentially make the difference between organisations/environments that are DSbD-ready and those that are not. In broad terms, this will provide insights around the level of 'security awareness' an organisation needs in order to embrace DSbD.

- The design, implementation and initial evaluation of a prototype Self-Assessment Tool that enables organisations to assess their own DSbD readiness. The value here will be in offering them an insight into their own position, including the level of related alignment between different parties, and ultimately helping to address the questions of whether the related investment is needed and will work. It is envisaged that the tool will be a tangible output that is already useful in its own right, but which also provides a likely foundation for further work.

Addressing these issues requires related consultation with organizational stakeholders, in order to inform the design and implementation of an approach that enables them to assess DSbD awareness and readiness in their own environments.

The work presented in this report addresses the first of these items and contributes toward the direction that has been adopted for the second. The first step in the work has focused upon data collection to establish organizations' current awareness of DSbD as a concept, and the related appetite that may exist to adopt related technologies.

2 Background

To quote the UK's National Cyber Security Centre (NCSC), the concept of being Secure by Default is motivated as follows (NCSC, 2018):

> *"To be truly effective, security needs to be built-in from the ground up. Hardware needs to be designed to resist physical attacks, and provide secure storage to other components. Operating systems need to take advantage of hardware security features, and applications need to use the right operating system security features.*
>
> *Secure by Default is about taking a holistic approach to solving security problems at root cause rather than treating the symptoms; acting at scale to reduce the overall harm to a particular system or type of component. Secure by Default covers the long-term technical effort to ensure that the right security primitives are built in to software and hardware. It also covers the equally demanding task of ensuring that those primitives are available and usable in such a way that the market can readily adopt them."*

The concept is further supported by a series of eight related principles, listed as follows (NCSC, 2018):

- Security should be built into products from the beginning, it can't be added in later;
- Security should be added to treat the root cause of a problem, not its symptoms;
- Security is never a goal in and of itself, it is a process – and it must continue throughout the lifetime of the product;
- Security should never compromise usability – products need to be secure enough, then maximize usability;
- Security should not require extensive configuration to work, and should just work reliably where implemented;
- Security should constantly evolve to meet and defeat the latest threats – new security features should take longer to defeat than they take to build;
- Security through obscurity should be avoided;
- Security should not require specific technical understanding or non-obvious behaviour from the user.

Levine (2021) offers the view that "trust starts in silicon," highlighting the fundamental nature of hardware security as an underpinning basis upon which other security efforts will typically be based. As he goes on to state, one cannot design a secure system on a compromised base, and flags that unlike with software (where vulnerabilities can be patched) there is no opportunity to retrofit a fix to compromised hardware. Affected devices would instead need to be replaced.

In the UK, the Digital Security by Design (DSbD) initiative is funded by the UK Industrial Strategy Challenge Fund, with £70m of government funding matched by £117m of industry co-investment. Its vision is to “radically update the foundation of the insecure digital computing infrastructure by creating a new, more secure hardware and software ecosystem” (DSbD, 2023).

The foundation of the approach is the Capability Hardware Enhanced RISC Instructions (CHERI), an architecture designed by the University of Cambridge and SRI International (Woodruff et al., 2014). CHERI extends the CPU instruction set to enable it to access memory using *capabilities* instead of machine-word pointers, providing fine-grained hardware-enforced access protection of objects in memory. A program using capabilities is generally incapable of making out-of-bounds accesses, which means bugs can be caught and fixed instead of exploited. When applied to existing languages that lack memory safety (e.g. C and C++) it can address memory safety issues without the overhead of software runtime checks, and can be applied to legacy C/C++ programs with minimal change. A practical realization of the CHERI approach is offered by Arm’s Morello program (see www.arm.com/architecture/cpu/morello), a prototype system-on-chip (SoC) and a development board, which enables industry and academic partners in the DSbD initiative to test the new architecture in real-world use cases.

Although it delivers a feasible technical foundation, it is also recognized that the approach represents a significant departure for technology developers and manufacturers. As such, there is no guarantee that providing a viable DSbD solution is a sufficient basis to ensure that others will adopt it. With this in mind, a further initiative within the DSbD programme is the Digital Security by Design Social Science Hub+ (Discribe – see www.discribehub.org), which is applying social and economic science to a series of 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 technologies;
- what social and cultural factors might influence the success of the wider DSbD ecosystem

The current project contributes toward these aims by investigating aspects of existing organisational awareness, with a view towards supporting the design and development of the proposed tool to enable organisations to assess their own readiness.

3 Investigating organisational awareness

The initial phase of data collection was conducted via a survey-based approach, in order to provide some baseline insights that could then be used as a foundation for further qualitative data collection at a later stage (with both phases then feeding into the requirements capture for the later tool development phase of the project). Survey respondents were advised that the questionnaire was seeking to explore organisations':

- attitude towards cyber security and experience of incidents
- prioritization of cyber security during IT procurement and deployment
- awareness of DSbD issues and principles.

They were further advised that the findings would be used to support the development of a Self-Assessment Tool for organisations, enabling them to profile their awareness of DSbD and potential opportunities for incorporating it. The resulting survey included a total of 39 questions, spread across the thematic areas listed in Table 1. A copy of the full questionnaire (including the participant briefing material) is presented in Appendix A.

Survey theme	Issues explored
Background (4 questions)	• Sector and size of the organization • Respondent's role
Attitude towards cyber security and experience of incidents (7 questions)	• Cyber security knowledge and commitment of the respondent and their organization • Recognition of risks and experience of incidents
Prioritization of cyber security during IT procurement and deployment (15 questions)	• Importance of the NCSC's Secure by Default principles • Use of Internet of Things (IoT) / smart devices and recognition/prioritization of security when procuring or producing products. • Approval process for technology adoption • Tracking the security status of deployed devices
Awareness of DSbD issues and principles (10 questions)	• Awareness of DSbD-related initiatives • Willingness to invest in DSbD-based technologies • Incentives and barriers to DSbD adoption

Table 1 : Topic coverage within the awareness and readiness survey

The survey also included two distraction / attention-check questions, firstly at around the midpoint (with Q21 asking respondents to choose the main problem with completing online surveys from 5 light-hearted options, one of being that they generally lack pictures of kittens) and then toward the end of the survey (with Q37 asking them to select a favourite from a picture of three kittens). The final question was then an optional open comments box, inviting respondents to offer any further thoughts or add context to any of their earlier responses.

The survey was open from July to December 2022 and attempts were made to promote it to UK-based organizations via a variety of routes during this period, including:

- emails to the Corporate Partners of the Chartered Institute of Information Security (CIISec)
- Emailing to members of the DSbD and Sprite+ mailing lists
- Distribution of flyers at face-to-face events (CIISec Live in September 2022 and DSbD All-Hands in October 2022, both with in excess of 150 attendees)
- Promotion via the Federation of Small Business in the East Midlands region in November 2022
- Inclusion in the DCMS Cyber Security Newsletter in December 2022
- A number of accompanying LinkedIn and Twitter postings during the period.

Despite this, the overall response level was lower than originally desired, with 76 usable responses in total and only 67% of these being classed as fully completed. Of the responses received, 64% came from large organizations (500+ employees) and 14% from those of medium size (50-499). Respondents came from a broad range of sectors, including Finance and insurance (8%), Publication administration (8%), and Health and social work (8%). However, the main areas represented were Information and communication (18%), Professional, scientific and technical activities (14%) and Education (17%). In terms of the staff backgrounds represented, 39% were in specifically cyber-security roles, and 12% were in wider IT roles. The other significant area of representation was staff in senior management roles (28%). Only 3% came from procurement (an area that was of potential interest in relation to purchasing of secure devices) and 18% were from other staff groups (which were largely the academic respondents).

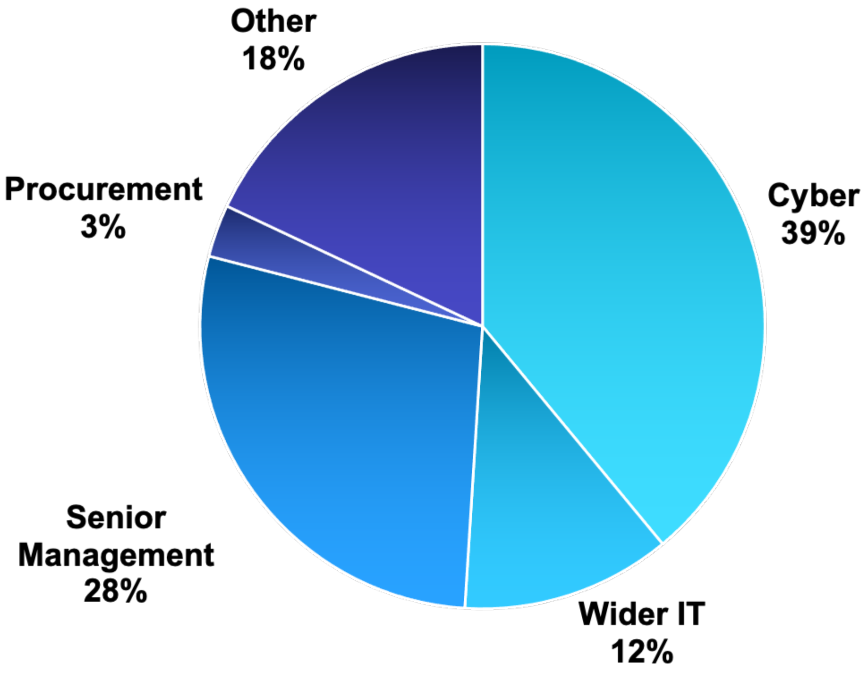


Figure 1 : Breakdown of survey respondents

It is considered that the specialized nature of the survey was a likely limiting factor on the number of respondents that considered themselves interested and eligible, and the length of the exercise was also a likely a disincentive for some (i.e. although it was stated that the activity would take around 15 minutes, it was also indicated that the total number of questions was 39, including optional comments). Meanwhile, the dropout rate was ultimately linked to the overall length of the survey and the depth of questioning. The survey tool reported an estimated time to complete of 17 minutes (in practice the average completion time was 10 minutes, likely allowing for those respondents that only completed a subset of the questions). It is recognized that this may have had a resultant effect upon the final respondent group, insofar as it may have caused a skew toward those who were truly interested in the topic and/or committed to security rather than a more representative sample of what organizations in general are likely to think.

Despite the relatively limited response, an examination of the results still proved to be useful in confirming the relevance and direction of the wider project activity.

4 Results and analysis

The results and discussion below are based upon the 76 respondents for the overall survey, but dropping to a core of 58 from the IoT questions onwards. It should be noted that there was no noticeable pattern in type of respondents that the dropped out (e.g. it was not a case that cyber security practitioners persisted while others stopped).

4.1 Cyber security awareness and experience

The overall results present a positive view of the respondents' claimed knowledge and attitude towards cyber security, and how they believe it is reflected in their organization. In terms of their own personal experience, there was a high level of confidence and claimed knowledge in relation to cyber security, with 72% claiming high or above average knowledge (and only 8% claiming to be below average). Meanwhile, looking at the position of their organization, there were some similarly positive indications:

- 57% claiming the organization's knowledge of cyber security was above average or high, with only 13% below average.
- 72% claimed their organization is committed or highly committed to cyber security, with only 8% suggesting a lack of commitment.
- In terms of the actual level of cyber security, 59% felt it was high or very high (with 11% indicating below average). Moreover, 49% felt their organization was likely to be better than others in the same sector, while only 12% felt they were likely to be worse.

Given these results, we can consider that although the response base was small it was generally coming from a set of respondents that were knowledgeable and committed in terms of cyber security. This places them in an interesting position in terms of offering their views about the desirability and feasibility of adopting DSbD-based approaches (i.e. they would be expected to be a fairly 'best case' response group, and so any issues or challenges raised from their perspective would only be likely to be amplified amongst a less committed community). Nonetheless, 42% indicated that they had experienced a security incident that they perceived to be the result of vulnerability exploitation. As such, there was a fair base of respondents that would potentially have direct experience from which to relate to the underlying issue that DSbD seeks to address.

4.2 Security in device adoption and deployment

The next stage of the questionnaire sought to more specifically explore the respondents' perspective on security in the context of adopting and using devices. This began by asking respondents to consider and rate the importance of each of the aforementioned Secure by Default principles. Ratings were provided on a 5-point scale (from very low to very high), and the main finding was that the majority of respondents rated all of the principles as being of high or very high importance. Looking more specifically, there were particularly prominent levels of agreement for:

- Security is never a goal in and of itself, it is a process – and it must continue throughout the lifetime of the product (86%)
- Security should constantly evolve to meet and defeat the latest threats – new security features should take longer to defeat than they take to build (85%)
- Security should be added to treat the root cause of a problem, not its symptoms (83%)

The principles scoring the least levels of importance (scoring neutral or below) were as follows (while of course remembering that the significant majority of responses were still rating them high importance):

- Security should never compromise usability – products need to be secure enough, then maximize usability (38%)
- Security through obscurity should be avoided (34%)
- Security should not require specific technical understanding or non-obvious behavior from the user (34%)

The principle that is arguably closest to matching the notion of security *by design* ("Security should not require extensive configuration to work, and should just work reliably where implemented") was rated important by 75%. As such, these responses help to further reinforce the impression of a positive predisposition towards security and likely buy-in to the DSbD concept.

Moving beyond the consideration of principles, attention was then given to the extent to which organizations had adopted IoT/smart devices and the extent to which they had considered security when doing so. This category of device was specifically selected because it represents a newer form of technology than traditional IT (e.g. desktops, laptops, smartphones and tablets) that organizations would likely purchase routinely, as well as being a category in which security issues have been specifically called out as requiring attention (DCMS, 2018). As such, it was expected to be an area in which respondents might more specifically be able to comment on whether security was given specific attention when determining whether it was appropriate to adopt and deploy the technologies.

66% of organizations indicated that they were using IoT/smart devices, with a notable further 14% indicating that they did not know. However, where the devices were in use, only 50% were confident that they were using business-grade devices (while 37% indicated use of consumer-grade devices). This represented the first indication of a gap between the theory and practice in the respondents' handling of security, insofar as there is a clear group of them that have adopted technologies that are not directly designed for use in organizational settings. This is not to say that the devices will not work and deliver the functionality needed (indeed the fact that they have been adopted tends to illustrate that they are serving a purpose), but rather that this is potentially happening without certain issues of more importance at the business level (e.g. security) having been given the attention that may be needed. Indeed, concern has been expressed about the level of consumer grade connected devices in use in enterprise contexts, and the resulting vulnerability that these may introduce (Ipsos, 2022).

Given the self-declared security-awareness of the respondents and their organizations, security appears to have received somewhat less attention than one might expect during the adoption of IoT/smart devices. Here 71% claimed to have done so during the selection and purchase of the devices, 53% during deployment, and 61% during use. The fact that notably fewer claimed to consider it during deployment and use seems surprising and somewhat counterintuitive if they have considered it important when selecting the devices in the first place.

Looking beyond the specific IoT/smart device context, the survey also asked some more general questions around the recognition and prioritization of security during wider technology procurement. Some key results here were as follows:

- 67% look for security assurances from suppliers when purchasing new devices / hardware;
- 65% would pay for a more secure product because of the risk of cyber breaches;
- 71% use security features as a factor when comparing between products during procurement;
- Security elements are rated with similar priority to other factors (e.g. brand reputation; features and functions, financial cost; warranty and support) when purchasing connected devices, with 76% rating it high/very high.

These broadly similar proportions all again serve to suggest that the respondent group was generally positively disposed towards security, and used it as a key factor in their adoption-related decision-making. It was also relevant to note that they tended to expect that other organizations would be similar. Of the 62% of respondents who indicated that they created products of some form, 78% believed security features to be a marketing advantage when addressing potential adopters.

In addition, there was, a slight drop in the level of attention when looking at the post-procurement stage. Here 60% claimed to track the security status of their deployed devices, with remaining respondents fairly equally split between 'no' and 'don't know' responses. Although the majority still claim to track, the fact that some do not (and that this is happening amongst security-focused respondents) gives a further indication towards the desirability of deploying secure by design technologies (i.e. on the basis that these would be more secure from the outset and so not needing the level of attention that current devices may demand in terms of security patching and updates).

4.3 DSbD-specific issues and awareness

The final segment of the survey sought to explore the specific familiarity with DSbD as a concept, and the attitude towards adopting future technologies based upon such a foundation. The first question sought to explore awareness of three notable activities in the topic area, as listed in Table 2. To briefly explain the inclusion of each, the DSbD programme is the name of the overarching UK initiative, which in turn is supported by the UK Industrial Strategy Challenge Fund. Meanwhile, as mentioned earlier in the report, CHERI is the capability architecture for more secure operations at the hardware level, and Morello is a prototype implementation of the approach. What is notable from the results is that, even amongst a more apparently security-aware and committed set of respondents, there is a relatively low level of awareness and familiarity compared to earlier findings While the DSbD initiative itself gains a reasonable level of at least name-recognition, the situation is clearly different when examining more specific familiarity and awareness of CHERI and Morello, with two thirds of respondents being *unaware* in both cases. In fairness, this could reasonably be explained on the basis that both are fairly specific areas of activity, and so may be less visible for those not involved in them. At the same time, the overall picture that emerges from this is that even amongst a security-literate audience, the issue of DSbD is not as overtly prominent as it could be.

Activity	Familiar with it	Heard about it	Unaware of it
The UK's Digital Security by Design (DSbD) programme	17%	42%	41%
The Capability Hardware Enhanced RISC Instructions (CHERI) architecture	9%	26%	65%
The ARM Morello prototype/development board	11%	24%	65%

Table 2 : Respondents' familiarity with different DSbD-related activities

The further questions sought to explore attitudes towards adopting DSbD-based technologies, with particular interest in the overall appetite to do so, and the associated challenges and incentives. One key issue that would be expected to affect willingness to adopt is of course the pricing compared to standard technologies that already do the job. With this in mind, the respondents were specifically asked whether they believed their organization would be willing to pay more for a product that is more secure by design. The question was further framed by suggesting that such a product could reduce potential vulnerabilities by at least two thirds, based on the assertion offered in much of the publicity around the DSbD initiative that the approach has “the potential to block up to two thirds of all memory related cyber attacks” (DSbD, 2022). As depicted in Figure 2, just over half indicated that they would pay more, and only a minority explicitly indicated that they would not do so. However, this left a third unsure, which is again potentially reflective of the lack of awareness or consideration of the issue.

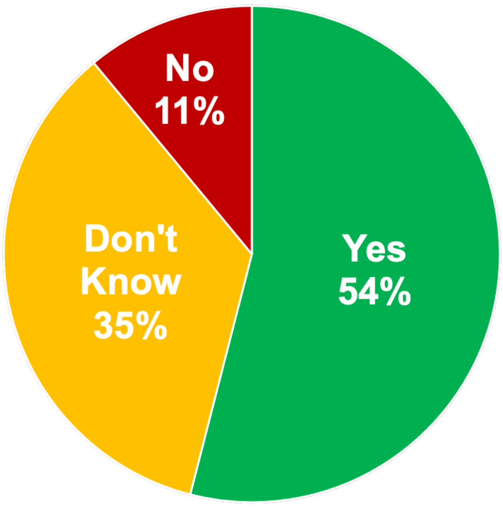


Figure 2 : Willingness to pay more for a secure by design product

Setting the issue of cost in a wider context, the respondents were found to perceive a variety of potential barriers to be overcome in adopting secure technology. They were offered 15 choices, and asked to rate each of them on a Low, Medium, High scale:

- Ambiguity, uncertainty
- Change resistance
- Competing with other priorities
- Complexity
- Financial cost
- Disruption / Inconvenience
- Lack of clarity about benefits
- Lack of compatibility
- Lack of incentive
- Lack of necessity
- Lack of skills
- Seeing losses, not gains
- Satisficing (i.e. aiming for a satisfactory or adequate result, rather than the optimal solution)
- Avoiding decision regret over the investments
- Only recognizing known risks

Of these, almost all were ranked at as least a Medium concern by at least two thirds of respondents. The only issue that was substantially away from this was 'Avoiding decision regret over the investments', where only 48% considered it a Medium or High barrier. Meanwhile, looking at the issues rated as High, 'Competing with other priorities' was ranked most prominently (67%). Issues around 'Financial cost' (54%), 'Lack of clarity around benefits' (56%) and 'Lack of compatibility' (50%) were the other issues for which at least half of the respondents selected the High category.

Set against the obstacles, and looking at potential incentives to adopt DSbD-based technologies, there was broad recognition of a range of stakeholders that would value it if the organization were to implement DSbD-based technology (see Figure 3). Customers were marginally the most prominent, and the only party where more than half the respondents anticipated that value would be perceived. Indeed, while only 6% felt that no-one would value it, there is clearly a mixed picture in the extent to which likely value is perceived from others and no single group that emerges as clearly dominant.

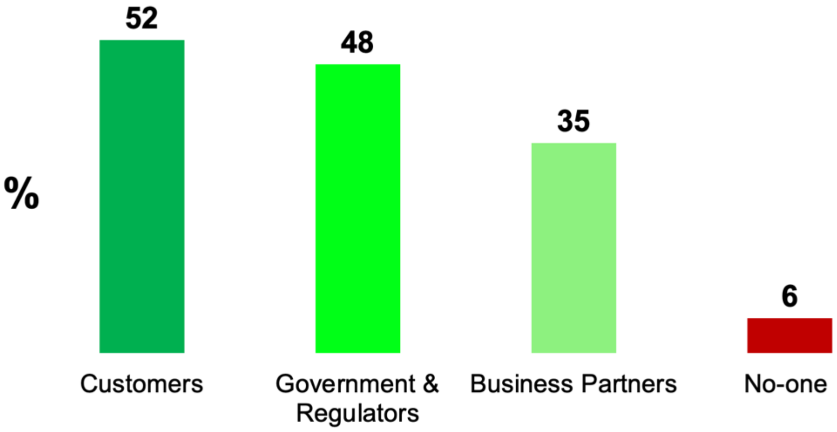


Figure 3 : Parties likely to value DSbD adoption

In terms of steps that would help organisations to adopt secure-by-design hardware, two factors were prominent: 'Pricing them competitively' (63%) and 'A clear requirement or directive that pushes towards adoption' (61%), with the latter notably aligning with the response around legal requirement to adopt. The third specific option that was offered, 'Access to expertise/advice to help understand what to look for and choose', was selected by 32%. Meanwhile, 9% felt that they did not need help as they were already adopting such hardware, and 6% felt no need for help as they did not perceive a need for such devices in their organisation (i.e. consistent with the earlier proportion that felt no-one would value it being adopted).

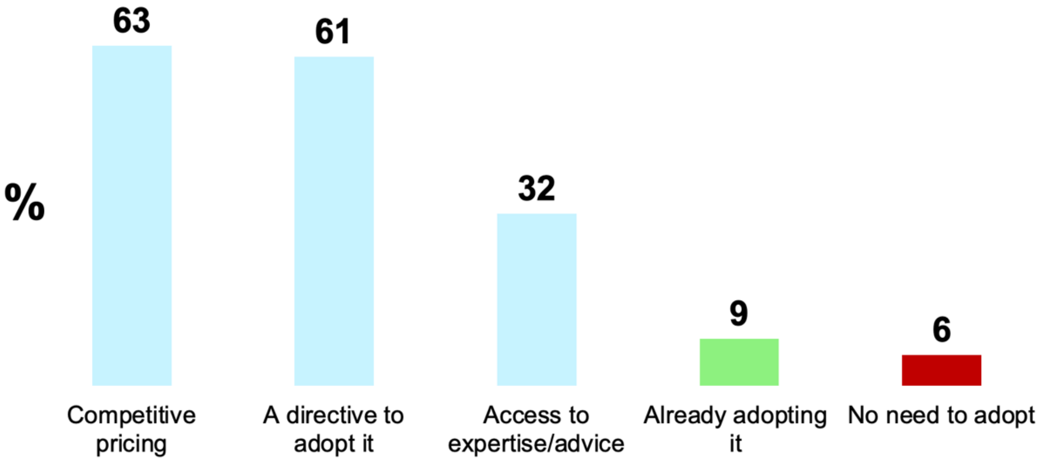


Figure 4 : Factors that would aid DSbD adoption

When asked more specifically about what would further encourage and incentivise adoption, regulatory requirement clearly emerged as the most prominent choice (see Figure 5). A series of further factors were also considered likely to have a role, with almost all respondents clearly indicating that *some* form of incentivisation would be relevant.

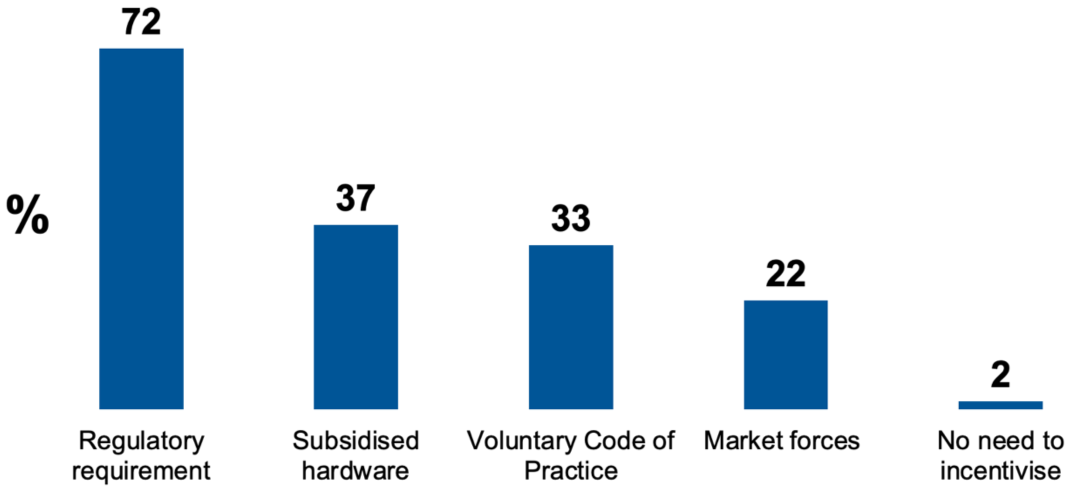


Figure 5 : Factors that would incentivise DSbD adoption

Finally, and again aligning with earlier responses around regulation, there was strong support for the introduction of legal measures to promote secure approaches. As shown in Figure 6, there is clear support for it to be legal requirement for both the providers to *produce* secure technology, and for the technology users to *adopt* it.

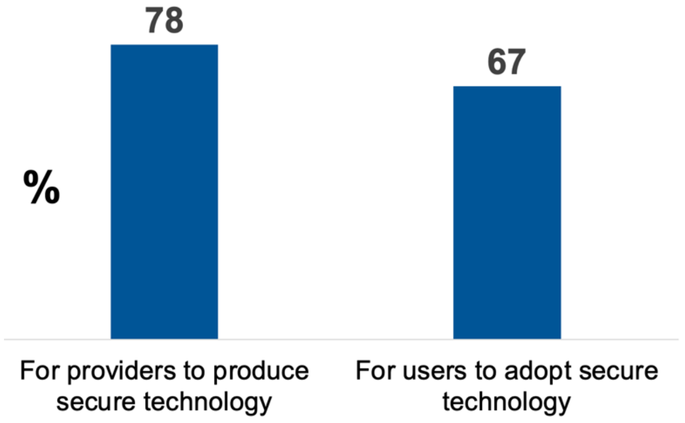


Figure 6 : Support for legal / regulatory requirements for DSbD adoption

5 Discussion

Although the response rate was ultimately lower than the project would have liked, it had the advantage of coming from a focused and informed sample group. Moreover, the significant level of agreement and consistency in the opinions of the current respondent group is strongly suggestive that the results would still have told a similar tale amongst a larger group of cyber-aware respondents. On the negative side, the survey ultimately had insufficient reach and response rate to enable us to assess potential differences between the views of CISOs and other significant players in the organization (e.g CFOs, CEOs etc).

An optional free-text comments box was offered at the end of the questionnaire, but ultimately garnered very little additional feedback. There were six responses in total, with most commenting about security more broadly than DSbD and so offering no further insights on the target theme. There was, however, one particularly notable response that is useful to consider in conjunction with the otherwise positive indications towards legal requirements for adoption:

> *"Per your question about legislation, the single biggest challenge with that is that you cannot assume many businesses are profitable at a particular level and are coping well with the skills shortage. So legislation, while appearing to be a strong stick might create major problems that would take time to emerge"*

This suggests that care would need to be taken in pushing too hard to mandate the adoption of DSbD-based technologies before the wider market is ready for it.

One final point to note was that the survey also sought to set the awareness and interest in DSbD against a series of other cybersecurity-related themes that were considered topical at the time (specifically, Cloud security, Data protection, Identity management, IoT and connected devices, Securing a hybrid/remote workforce, and Zero Trust Architecture). The respondents were asked about their awareness of each, and the potential interest for their organization. In terms of recognizing the issues, the vast majority of respondents claimed to be aware of all of them. The most prominent care of unawareness was in relation to Zero Trust Architecture, with 17% not having heard of it, whereas in all other cases it was only 4-6%. However, it is also notable that even the relatively high level of unawareness around ZTA is dwarfed by the levels of unfamiliarly with any of the DSbD-related activities reported earlier. This suggests that there is still a significant task in making potential adopters aware of DSbD opportunities as the approaches mature.

Security issues	No Knowledge of this	Aware of this	Interested in this	This is a priority	N/A
Cloud security	4%	17%	29%	50%	0%
Data protection	4	6%	27%	63%	0%
Identity management	4%	10%	40%	46%	0%

Internet of Things and connected devices	6%	31%	42%	15%	6%
Securing a hybrid / remote workforce	4%	13%	33%	50%	0%
Zero Trust Architecture	17%	25%	29%	27%	2%

Table 3 : Awareness and prioritization of other topical cybersecurity issues

Meanwhile, the results in Table 3 as a whole (particularly the leaves of interest and priority expressed around certain issues) again broadly confirms is that the survey drew from security-aware and committed respondents. As such, it again suggests that the views on DSbD-related matters were being drawn from a 'favourable' audience that would be expected to be more informed and receptive to the it. In this context, it seems particularly relevant to be mindful of the concerns and barriers that they still perceive.

6 Towards an organisational Self-Assessment Tool

The survey findings help to support the case for the proposed Self-Assessment Tool (SAT). The intention of the tool and the related work as a whole is to address the following aspects:

- Establishing a measure of organizational 'DSbD readiness'. This includes the ability to assess the practical (e.g. is current staff capable of implementing it), philosophical (e.g. business culture inertia) and pragmatic (e.g. cost/benefit) barriers that may exist, so that an organization can ensure that it is positioned to adopt DSbD at the technology level.
- Providing a means for organizations to recognize and assess where DSbD is relevant to them, and the extent to which it would be cost-effective (e.g. in comparison to existing approaches and set alongside potential breach costs).

The concept of the proposed tool is outlined in Figure 7, which indicates the range of stakeholder inputs that are considered useful to acquire in order to get a sense of organisational awareness and readiness to adopt DSbD technologies. As shown, it is considered desirable to get a range of views from those in key management/leadership roles, including the chief executive, and other players whose views may influence security investment and purchasing decisions, such as chief financial and procurement officers. Alongside this, the other views of clear relevance will come from those more directly connected to the technology and security aspects of the business, such as chief technology and information security officers[1].

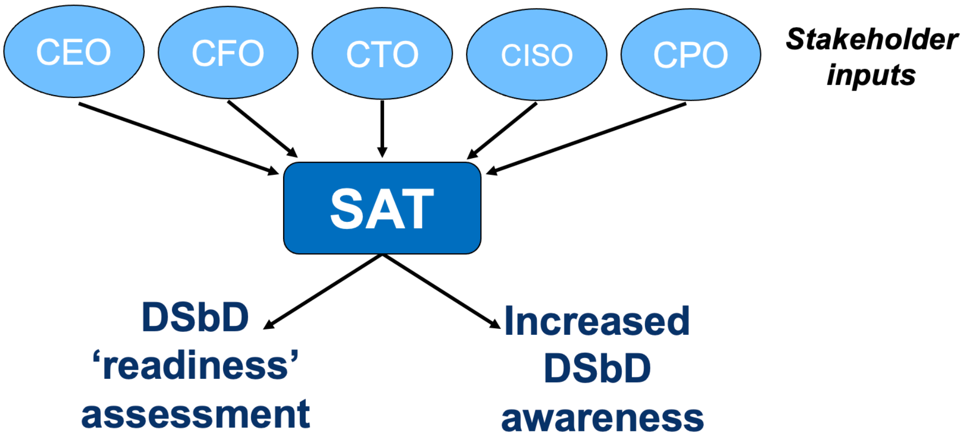


Figure 7 : The Self-Assessment Tool concept

[1] It is acknowledged these various c-suite roles and responsibilities may exist and be named differently within different organisations, and (depending upon the size of organisation concerned) various aspects may be consolidated within broader roles rather than each being represented by distinct individuals. At the same time, if there are not a sufficiently distinct set of stakeholders to involve then the expected relevance and utility of the SAT would be reduced (i.e. the tool is not envisaged as being as well suited to smaller environments in which the responsibilities may sit with 1-2 people and/or with technology management outsourced externally).

Table 4 outlines the areas around which it is envisaged that the SAT would collect data from different stakeholders, and the role that these would play within readiness assessments. In broad terms, the resulting assessment could be a function of the aggregated stakeholder *Attitude* and *Awareness* aspects set against the measure of organisational *Need*.

Data capture	Rationale	Usage
Incidents and breaches	Highlights the organisation's need for security based upon evidence of exposure, plus suggests the extent to which it already on the agenda.	Inform a 'Need' rating
Technology and data usage	The need for security based upon what the organisation is using the technology for, its dependence upon it, etc.	
Security priority and investment	Attitudes toward security in the organisation as a whole.	Inform an 'Attitude' rating
Security (in) technology adoption	More specific focus upon considerations at the technology investment level (i.e. which is more likely to affect DSbD adoption decisions).	
DSbD-specific awareness	More specifically focused on the CISO/CTO elements of the organisation to determine how well positioned they are to keep up to date with what is available to be adopted. Can also be used to *raise* awareness of DSbD.	Inform an 'Awareness' rating

Table 4 : Areas of data capture for the Self-Assessment Tool

The initial intention was to use the survey findings as a foundation for a further round of data collection via workshop / focus group sessions to discuss the SAT concept and explore associated requirements. However, despite several attempts to promote this, including coverage within a poster and an accompanying promotional flyer at the All-Hands meeting in April 2023 (see related materials in Appendix B) and an accompanying mailshot to the DSbD mailing list supported by the Discribe Hub, we were unable to secure sufficient expressions of interest from potential participants. As such, it was agreed that this activity would be put on hold with a view to revisiting it when a more comprehensive design for the SAT is available, and to promote via a more targeted group of contacts if necessary.

7 Conclusions

Secure by Design technologies have significant potential to improve standard level of security within deployed devices, and to reduce many of the vulnerabilities that have previously led to successful cyber attacks. At the same time, however, it is recognized that adoption of the resulting technology is not a simple case of 'build it and they will come', and this raises the question of how to ensure the support of potential adopters. The exploratory study presented in this report has sought to benchmark the level of awareness and potential buy-in around the topic.

The results the study clearly indicate an acceptance of the principle (which we would arguably expect to be the case anyway, given then security-focused respondent group). At the same time, however, there are a range of challenges that may need to be overcome in practice. The technology needs to be positioned appropriately in the market in terms of price-point, it needs to integrate alongside other technologies, and adopters need to feel confident that they have the skills needed to make the transition.

Moving forward, the findings are intended to inform the design and development of a web-based Self-Assessment Tool, allowing organizations to profile their current awareness of DSbD and the potential opportunities for incorporating it within their environment. The tool will obtain weighted data points from different organizational stakeholders (e.g. CISO, CFO, procurement, etc) in order to assess their respective awareness, understanding and acceptance of related security needs and investment, while at the same time also assessing the extent to which the organization may benefit from DSbD based upon its activities and prior experience of security incidence. It is anticipated that this will lead to a scorecard-based approach, where the organization is able to get a measure of its current posture and attitude, and how this may position them in terms of needs and readiness to adopt DSbD-based technology.

8 References

Benson, V., Furnell, S., Masi, D. and Muller, T. (2021). *Regulation, Policy and Cybersecurity: Hardware Security*. Final Project Report. Discribe Hub+, September 2021. https://www.discribehub.org/commissioning-reports.

DCMS. (2018). *Code of Practice for Consumer IoT Security*. Department for Digital, Culture, Media and Sport, October 2018. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/971440/Code_of_Practice_for_Consumer_IoT_Security_October_2018_V2.pdf

DSbD. (2022). "More companies across the UK join Digital Security by Design to test and learn from prototype cybersecurity technology", Press Release, Digital Security by Design, 5 December 2022. https://www.dsbd.tech/blogs/press-release-more-companies-across-the-uk-join-digital-security-by-design-to-test-and-learn-from-prototype-cybersecurity-technology/

DSbD. (2023). "About Digital Security by Design", Digital Security by Design. https://www.dsbd.tech/about/ (accessed 27 February 2023).

Ipsos. (2022). *Cyber security in enterprise connected devices*. Department for Digital, Culture, Media and Sport, 9 May 2022. https://www.gov.uk/government/publications/cyber-security-in-enterprise-connected-devices

Levine, E.V. (2021). "The Die Is Cast", *Communications of the ACM*, 64(1), pp56-60.

NCSC. (2018). "Secure by Default", National Cyber Security Centre, 7 March 2018. www.ncsc.gov.uk/information/secure-default

Srinidhi, B., Yan, J., and Tayi, G.K. (2015). "Allocation of resources to cyber-security: The effect of misalignment of interest between managers and investors", Decision Support Systems, 75, pp49- 62.

Straub, D.W. and Welke. R.J. (1998). "Coping with systems risk: Security planning models for management decision making", MIS Quarterly, 22, pp441-469.

Tomlinson, A., Parkin, S. and Shaikh, S.A. (2022). Drivers and barriers for secure hardware adoption across ecosystem stakeholders, *Journal of Cybersecurity*, Volume 8, Issue 1, https://doi.org/10.1093/cybsec/tyac009

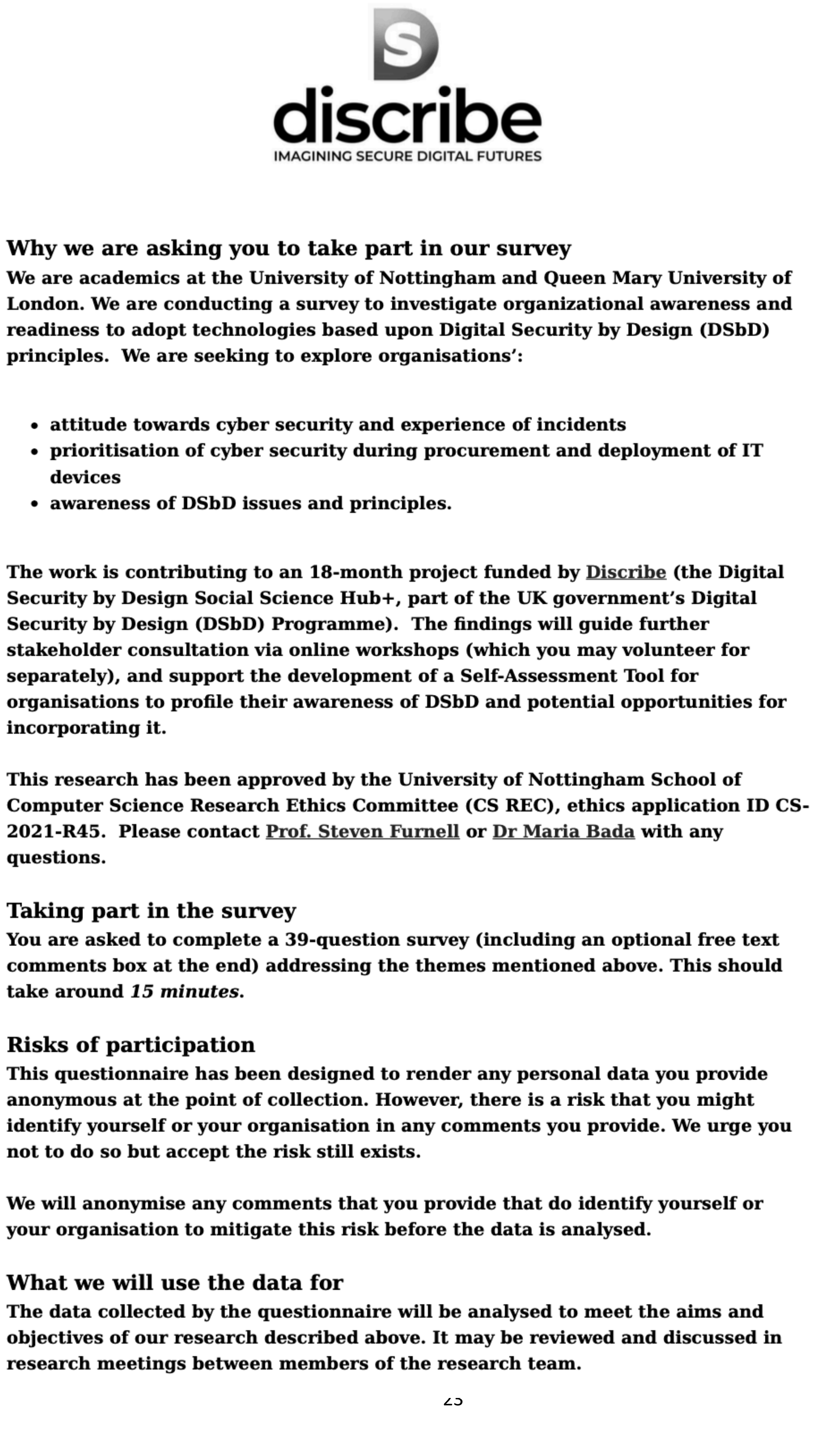
Tversky, A. and Kahneman, D. (1974). Judgment under Uncertainty: Heuristics and Biases, Science, 185, pp1124- 1131.

UK Parliament. (2022). *The Product Security and Telecommunications Infrastructure Act 2022*. 6 December 2022. https://www.legislation.gov.uk/ukpga/2022/46/pdfs/ukpga_20220046_en.pdf

Woodruff, J., Watson, R.N.M., Chisnall, D., Moore, S.W., Anderson, J., Davis, B., Laurie, B., Neumann, P.G., Norton, R., Roe, M. (2014). “The CHERI capability model: Revisiting RISC in an age of risk” https://www.cl.cam.ac.uk/research/security/ctsrd/pdfs/201406-isca2014-cheri.pdf

Appendix A – Survey

The following pages present a full copy of the survey questionnaire, as presented to participants on the SurveyMonkey website.



discribe
IMAGINING SECURE DIGITAL FUTURES

Why we are asking you to take part in our survey

We are academics at the University of Nottingham and Queen Mary University of London. We are conducting a survey to investigate organizational awareness and readiness to adopt technologies based upon Digital Security by Design (DSbD) principles. We are seeking to explore organisations':

- **attitude towards cyber security and experience of incidents**
- **prioritisation of cyber security during procurement and deployment of IT devices**
- **awareness of DSbD issues and principles.**

The work is contributing to an 18-month project funded by Discribe (the Digital Security by Design Social Science Hub+, part of the UK government's Digital Security by Design (DSbD) Programme). The findings will guide further stakeholder consultation via online workshops (which you may volunteer for separately), and support the development of a Self-Assessment Tool for organisations to profile their awareness of DSbD and potential opportunities for incorporating it.

This research has been approved by the University of Nottingham School of Computer Science Research Ethics Committee (CS REC), ethics application ID CS-2021-R45. Please contact Prof. Steven Furnell or Dr Maria Bada with any questions.

Taking part in the survey

You are asked to complete a 39-question survey (including an optional free text comments box at the end) addressing the themes mentioned above. This should take around *15 minutes*.

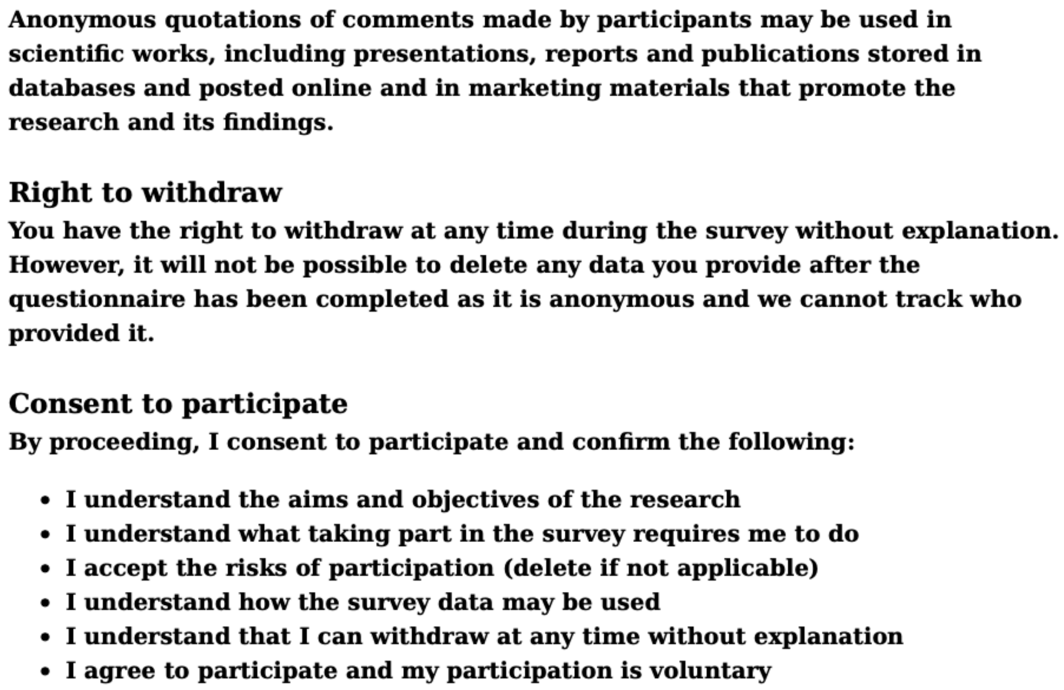
Risks of participation

This questionnaire has been designed to render any personal data you provide anonymous at the point of collection. However, there is a risk that you might identify yourself or your organisation in any comments you provide. We urge you not to do so but accept the risk still exists.

We will anonymise any comments that you provide that do identify yourself or your organisation to mitigate this risk before the data is analysed.

What we will use the data for

The data collected by the questionnaire will be analysed to meet the aims and objectives of our research described above. It may be reviewed and discussed in research meetings between members of the research team.



Anonymous quotations of comments made by participants may be used in scientific works, including presentations, reports and publications stored in databases and posted online and in marketing materials that promote the research and its findings.

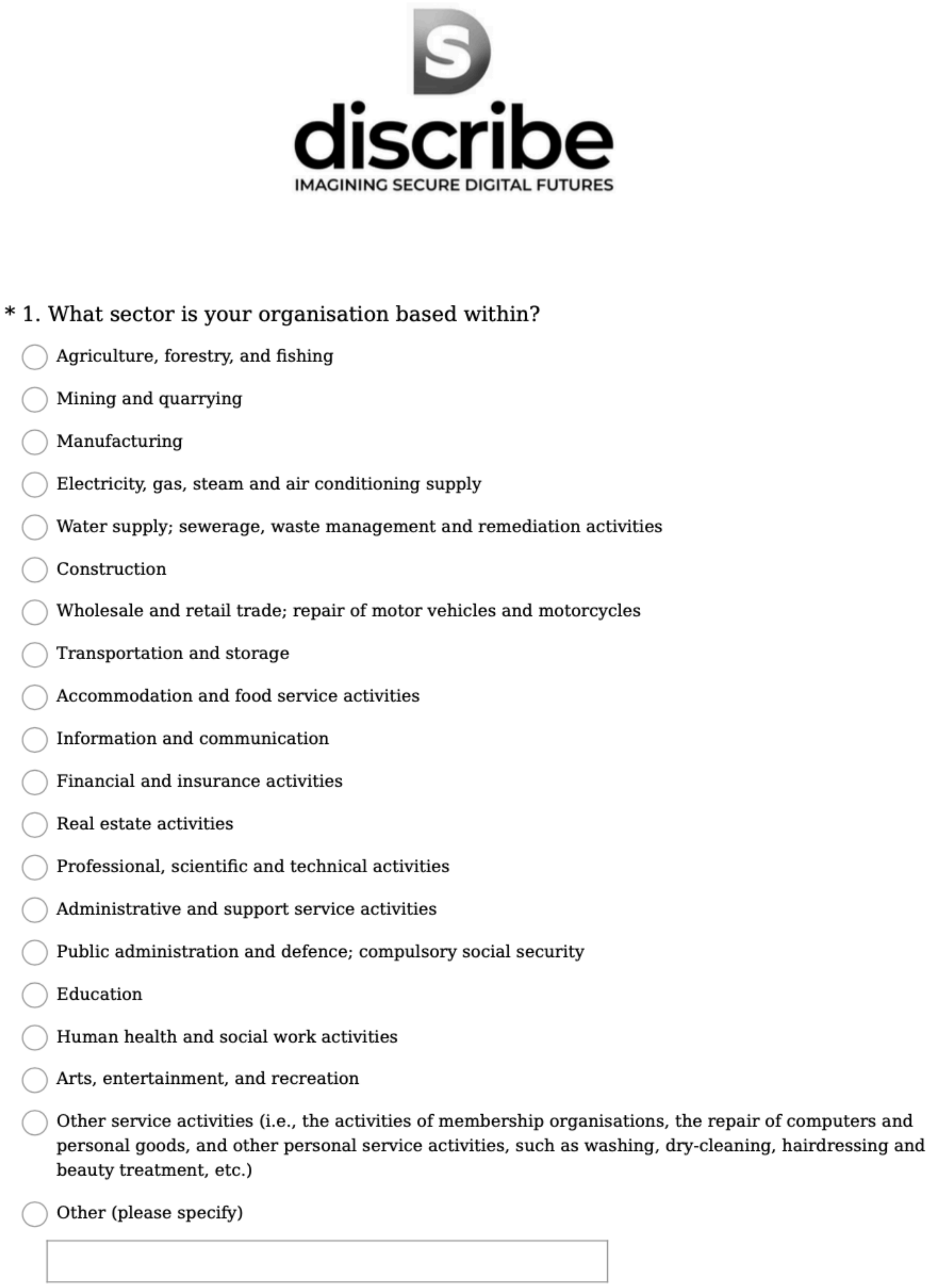
Right to withdraw

You have the right to withdraw at any time during the survey without explanation. However, it will not be possible to delete any data you provide after the questionnaire has been completed as it is anonymous and we cannot track who provided it.

Consent to participate

By proceeding, I consent to participate and confirm the following:

- **I understand the aims and objectives of the research**
- **I understand what taking part in the survey requires me to do**
- **I accept the risks of participation (delete if not applicable)**
- **I understand how the survey data may be used**
- **I understand that I can withdraw at any time without explanation**
- **I agree to participate and my participation is voluntary**



* 1. What sector is your organisation based within?

○ Agriculture, forestry, and fishing

○ Mining and quarrying

○ Manufacturing

○ Electricity, gas, steam and air conditioning supply

○ Water supply; sewerage, waste management and remediation activities

○ Construction

○ Wholesale and retail trade; repair of motor vehicles and motorcycles

○ Transportation and storage

○ Accommodation and food service activities

○ Information and communication

○ Financial and insurance activities

○ Real estate activities

○ Professional, scientific and technical activities

○ Administrative and support service activities

○ Public administration and defence; compulsory social security

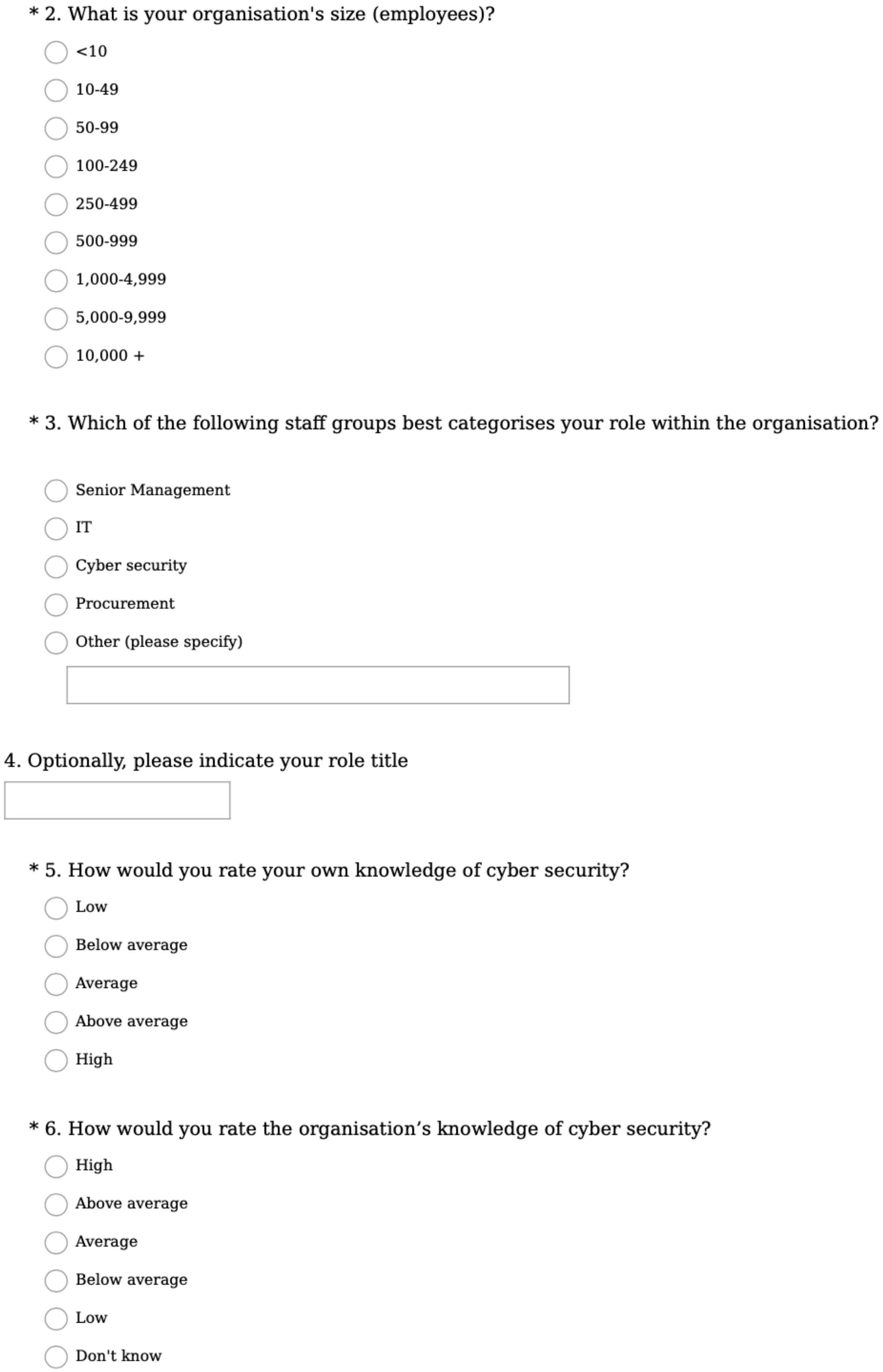
○ Education

○ Human health and social work activities

○ Arts, entertainment, and recreation

○ Other service activities (i.e., the activities of membership organisations, the repair of computers and personal goods, and other personal service activities, such as washing, dry-cleaning, hairdressing and beauty treatment, etc.)

○ Other (please specify)



* 2. What is your organisation's size (employees)?

○ <10

○ 10-49

○ 50-99

○ 100-249

○ 250-499

○ 500-999

○ 1,000-4,999

○ 5,000-9,999

○ 10,000 +

* 3. Which of the following staff groups best categorises your role within the organisation?

○ Senior Management

○ IT

○ Cyber security

○ Procurement

○ Other (please specify)

4. Optionally, please indicate your role title

* 5. How would you rate your own knowledge of cyber security?

○ Low

○ Below average

○ Average

○ Above average

○ High

* 6. How would you rate the organisation’s knowledge of cyber security?

○ High

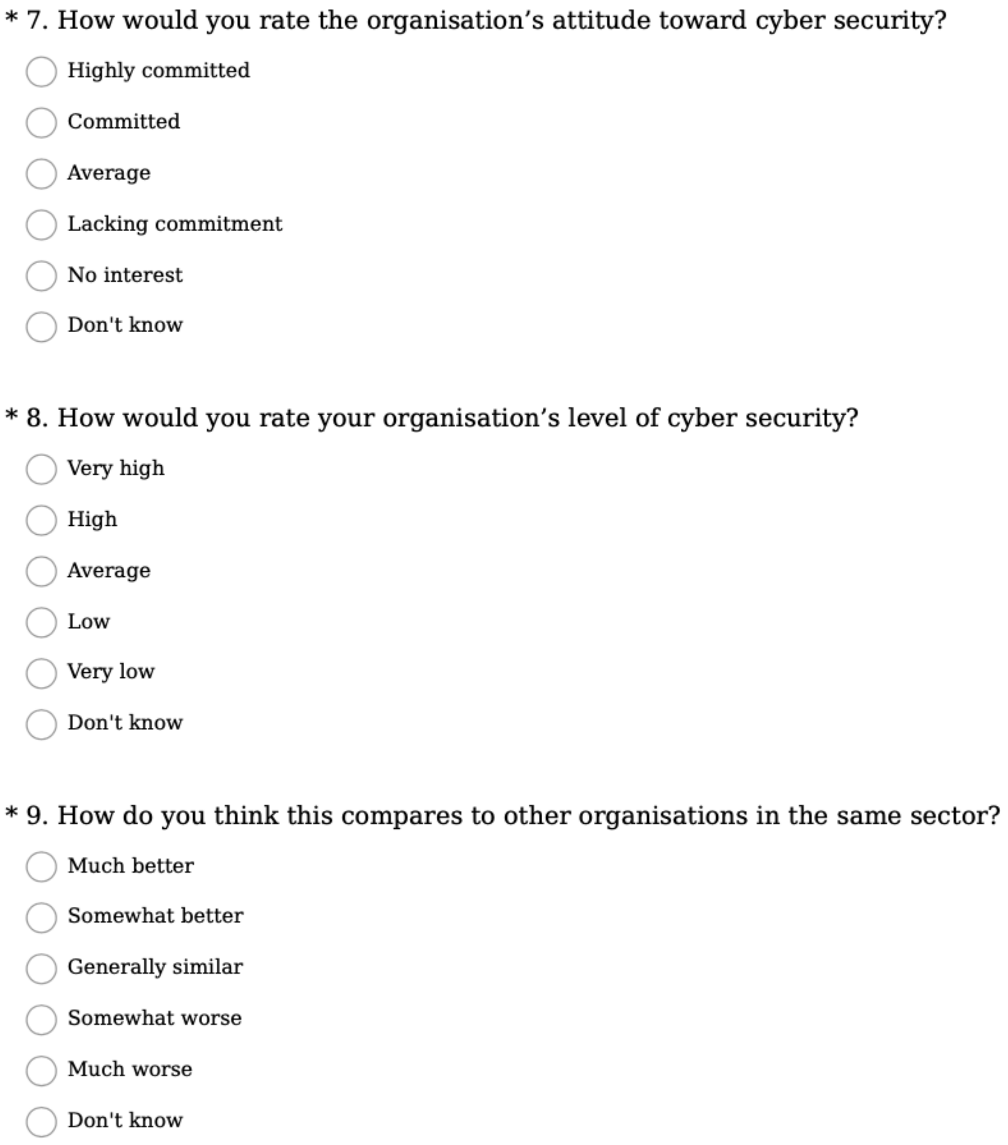
○ Above average

○ Average

○ Below average

○ Low

○ Don't know



* 7. How would you rate the organisation’s attitude toward cyber security?

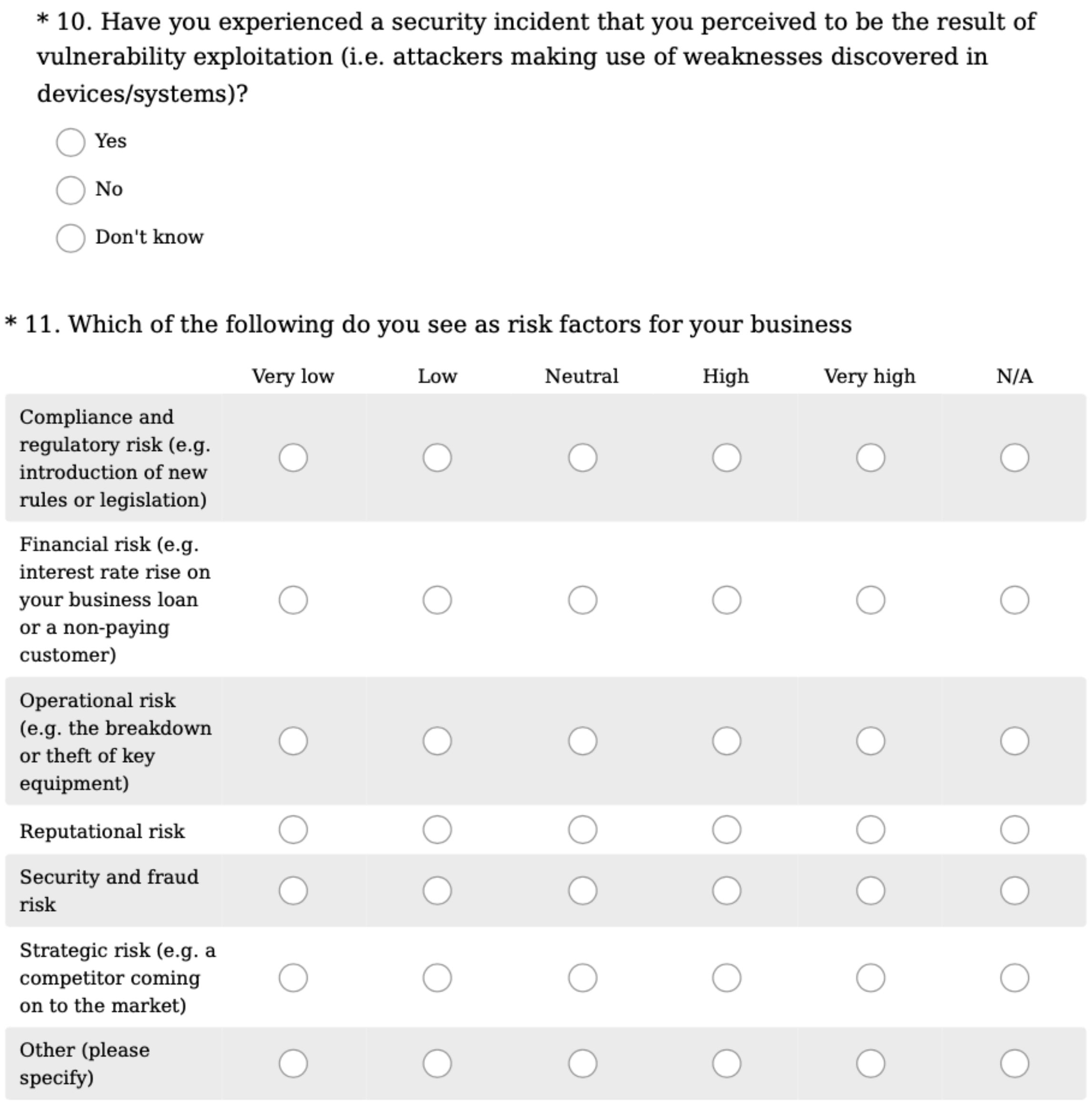
- ○ Highly committed
- ○ Committed
- ○ Average
- ○ Lacking commitment
- ○ No interest
- ○ Don't know

* 8. How would you rate your organisation’s level of cyber security?

- ○ Very high
- ○ High
- ○ Average
- ○ Low
- ○ Very low
- ○ Don't know

* 9. How do you think this compares to other organisations in the same sector?

- ○ Much better
- ○ Somewhat better
- ○ Generally similar
- ○ Somewhat worse
- ○ Much worse
- ○ Don't know



* 10. Have you experienced a security incident that you perceived to be the result of vulnerability exploitation (i.e. attackers making use of weaknesses discovered in devices/systems)?

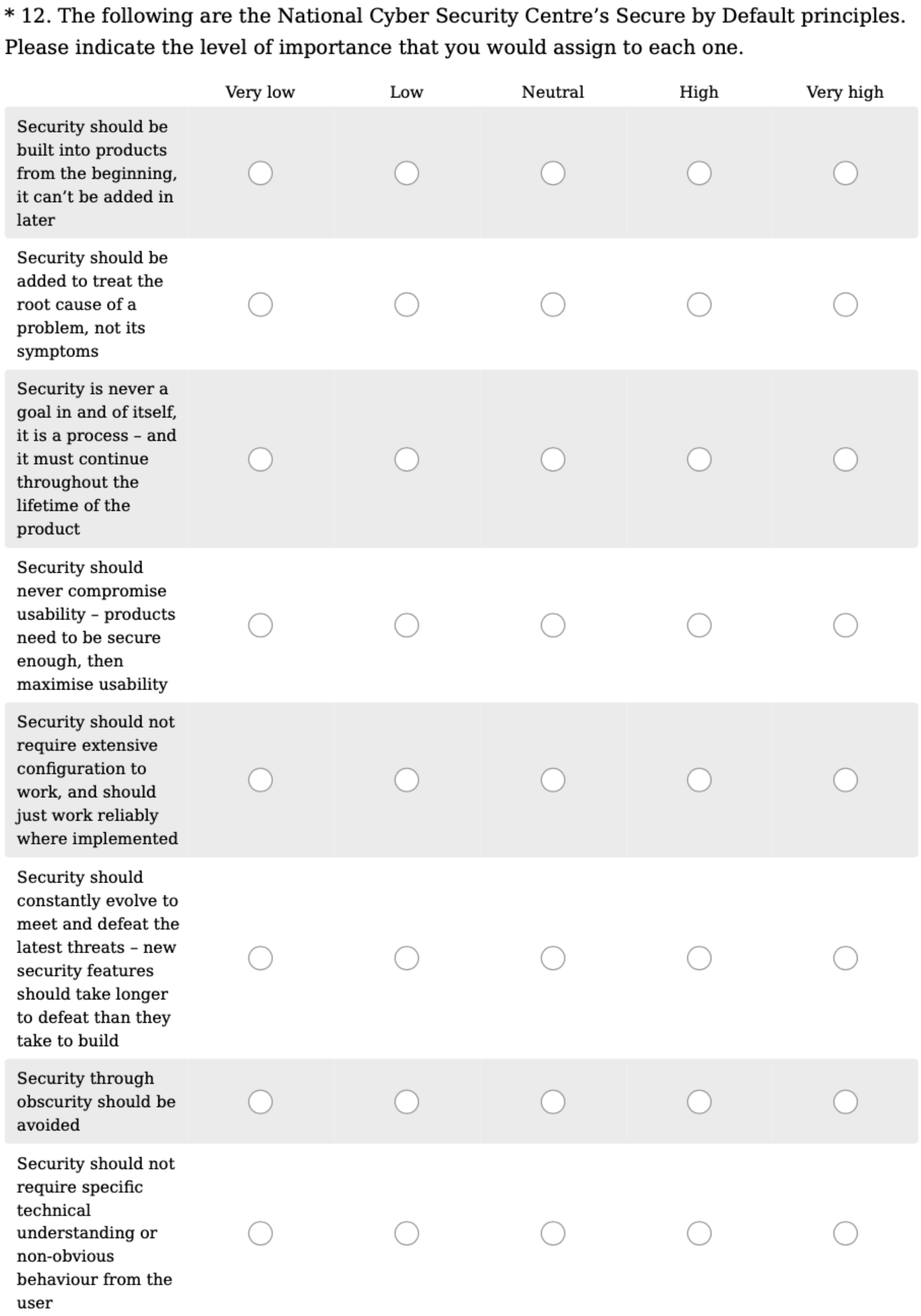
○ Yes

○ No

○ Don't know

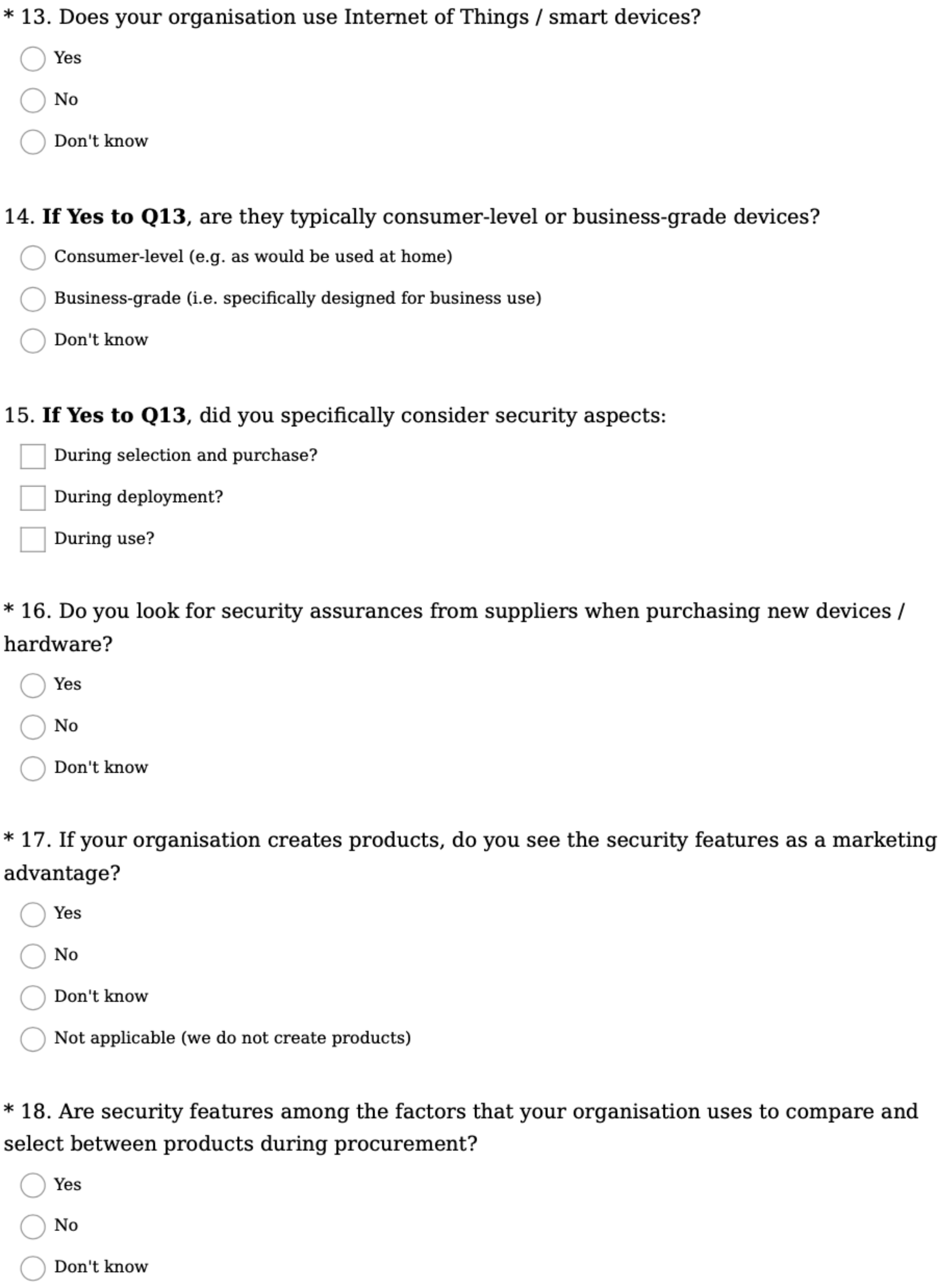
* 11. Which of the following do you see as risk factors for your business

	Very low	Low	Neutral	High	Very high	N/A
Compliance and regulatory risk (e.g. introduction of new rules or legislation)	○	○	○	○	○	○
Financial risk (e.g. interest rate rise on your business loan or a non-paying customer)	○	○	○	○	○	○
Operational risk (e.g. the breakdown or theft of key equipment)	○	○	○	○	○	○
Reputational risk	○	○	○	○	○	○
Security and fraud risk	○	○	○	○	○	○
Strategic risk (e.g. a competitor coming on to the market)	○	○	○	○	○	○
Other (please specify)	○	○	○	○	○	○



* 12. The following are the National Cyber Security Centre's Secure by Default principles. Please indicate the level of importance that you would assign to each one.

	Very low	Low	Neutral	High	Very high
Security should be built into products from the beginning, it can't be added in later	○	○	○	○	○
Security should be added to treat the root cause of a problem, not its symptoms	○	○	○	○	○
Security is never a goal in and of itself, it is a process – and it must continue throughout the lifetime of the product	○	○	○	○	○
Security should never compromise usability – products need to be secure enough, then maximise usability	○	○	○	○	○
Security should not require extensive configuration to work, and should just work reliably where implemented	○	○	○	○	○
Security should constantly evolve to meet and defeat the latest threats – new security features should take longer to defeat than they take to build	○	○	○	○	○
Security through obscurity should be avoided	○	○	○	○	○
Security should not require specific technical understanding or non-obvious behaviour from the user	○	○	○	○	○



* 13. Does your organisation use Internet of Things / smart devices?

○ Yes

○ No

○ Don't know

14. **If Yes to Q13**, are they typically consumer-level or business-grade devices?

○ Consumer-level (e.g. as would be used at home)

○ Business-grade (i.e. specifically designed for business use)

○ Don't know

15. **If Yes to Q13**, did you specifically consider security aspects:

□ During selection and purchase?

□ During deployment?

□ During use?

* 16. Do you look for security assurances from suppliers when purchasing new devices / hardware?

○ Yes

○ No

○ Don't know

* 17. If your organisation creates products, do you see the security features as a marketing advantage?

○ Yes

○ No

○ Don't know

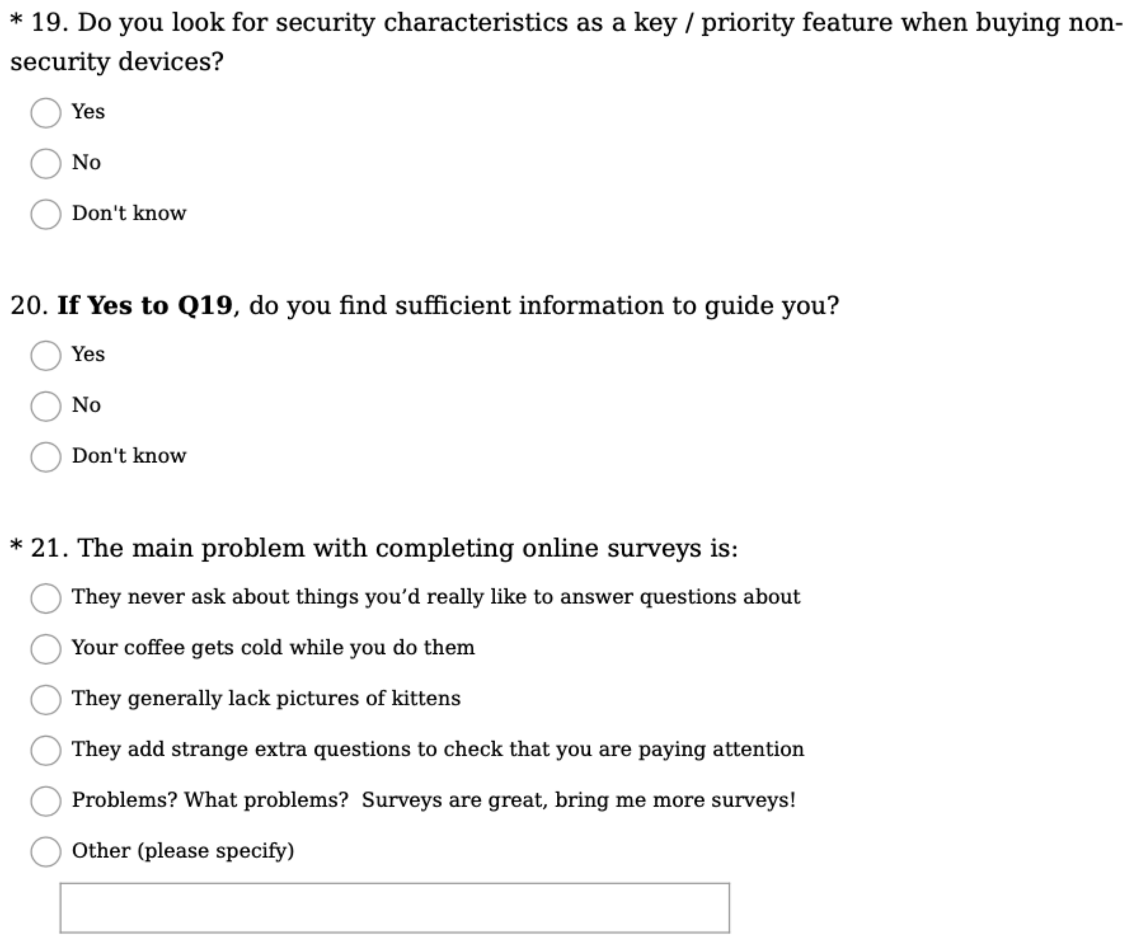
○ Not applicable (we do not create products)

* 18. Are security features among the factors that your organisation uses to compare and select between products during procurement?

○ Yes

○ No

○ Don't know



* 19. Do you look for security characteristics as a key / priority feature when buying non-security devices?

○ Yes

○ No

○ Don't know

20. **If Yes to Q19**, do you find sufficient information to guide you?

○ Yes

○ No

○ Don't know

* 21. The main problem with completing online surveys is:

○ They never ask about things you'd really like to answer questions about

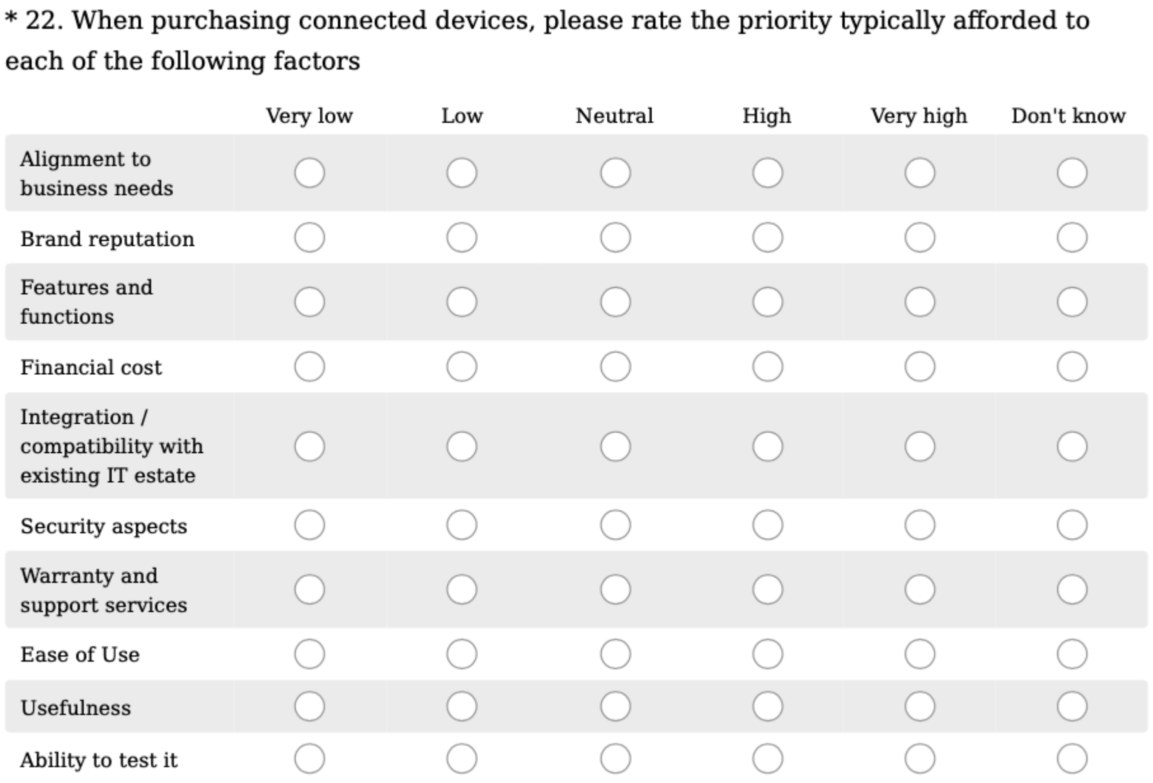
○ Your coffee gets cold while you do them

○ They generally lack pictures of kittens

○ They add strange extra questions to check that you are paying attention

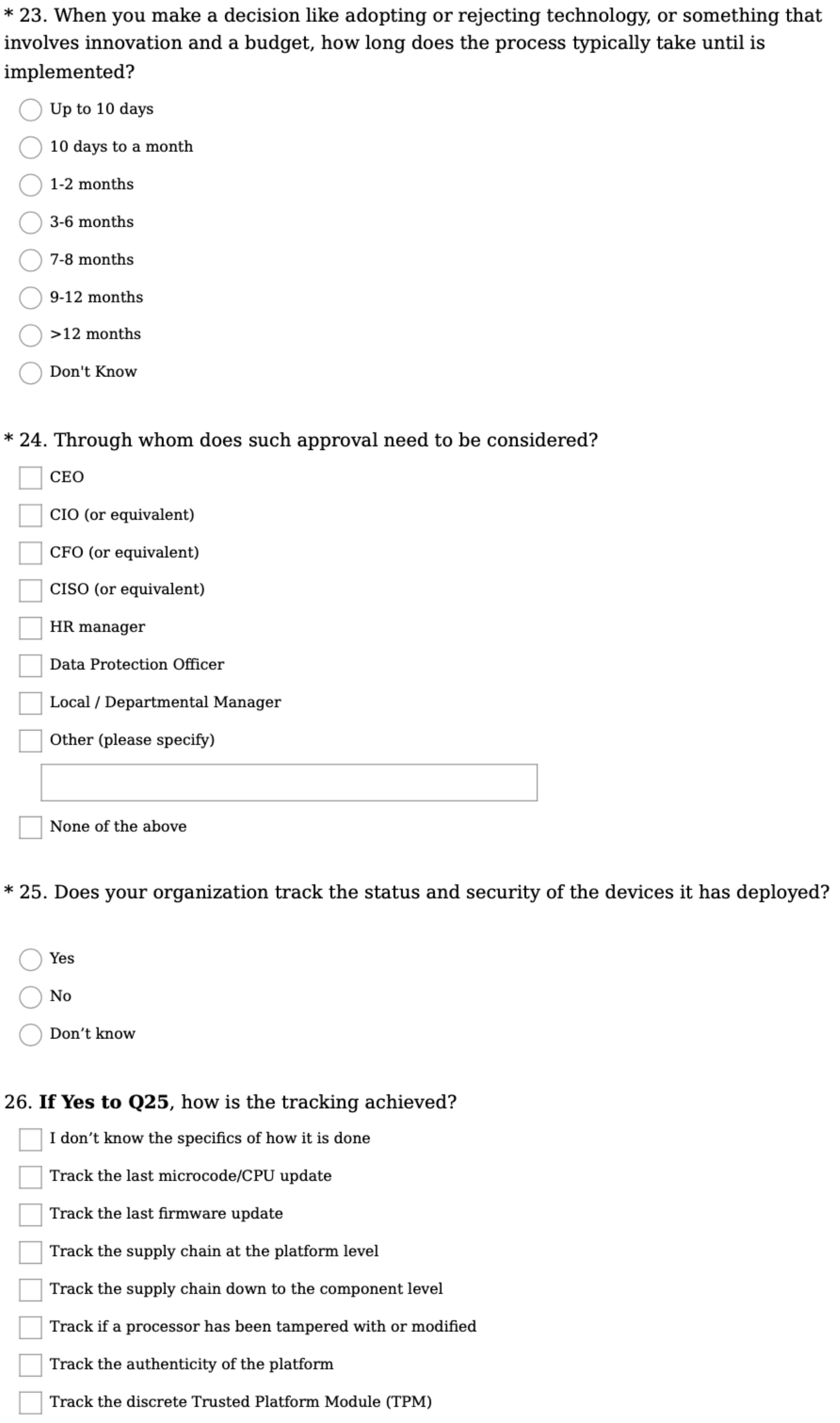
○ Problems? What problems? Surveys are great, bring me more surveys!

○ Other (please specify)



* 22. When purchasing connected devices, please rate the priority typically afforded to each of the following factors

	Very low	Low	Neutral	High	Very high	Don't know
Alignment to business needs	○	○	○	○	○	○
Brand reputation	○	○	○	○	○	○
Features and functions	○	○	○	○	○	○
Financial cost	○	○	○	○	○	○
Integration / compatibility with existing IT estate	○	○	○	○	○	○
Security aspects	○	○	○	○	○	○
Warranty and support services	○	○	○	○	○	○
Ease of Use	○	○	○	○	○	○
Usefulness	○	○	○	○	○	○
Ability to test it	○	○	○	○	○	○



* 23. When you make a decision like adopting or rejecting technology, or something that involves innovation and a budget, how long does the process typically take until is implemented?

○ Up to 10 days

○ 10 days to a month

○ 1-2 months

○ 3-6 months

○ 7-8 months

○ 9-12 months

○ >12 months

○ Don't Know

* 24. Through whom does such approval need to be considered?

□ CEO

□ CIO (or equivalent)

□ CFO (or equivalent)

□ CISO (or equivalent)

□ HR manager

□ Data Protection Officer

□ Local / Departmental Manager

□ Other (please specify)

□ None of the above

* 25. Does your organization track the status and security of the devices it has deployed?

○ Yes

○ No

○ Don’t know

26. **If Yes to Q25**, how is the tracking achieved?

□ I don’t know the specifics of how it is done

□ Track the last microcode/CPU update

□ Track the last firmware update

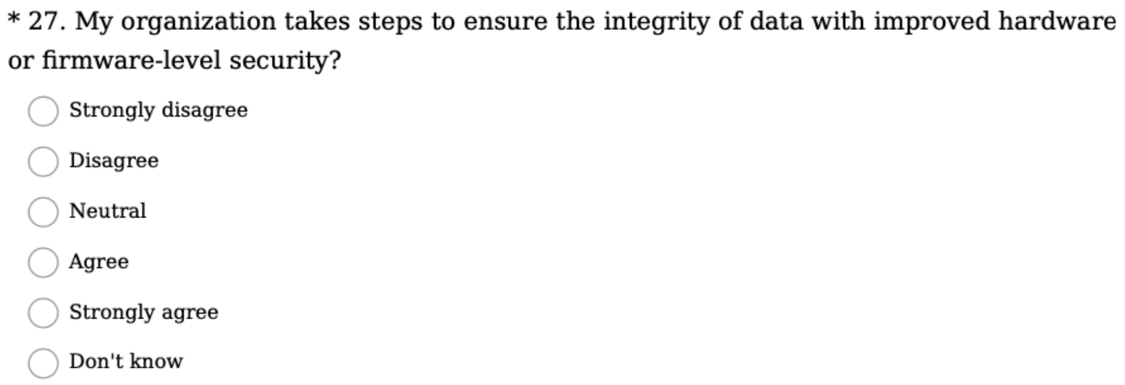
□ Track the supply chain at the platform level

□ Track the supply chain down to the component level

□ Track if a processor has been tampered with or modified

□ Track the authenticity of the platform

□ Track the discrete Trusted Platform Module (TPM)



* 27. My organization takes steps to ensure the integrity of data with improved hardware or firmware-level security?

○ Strongly disagree

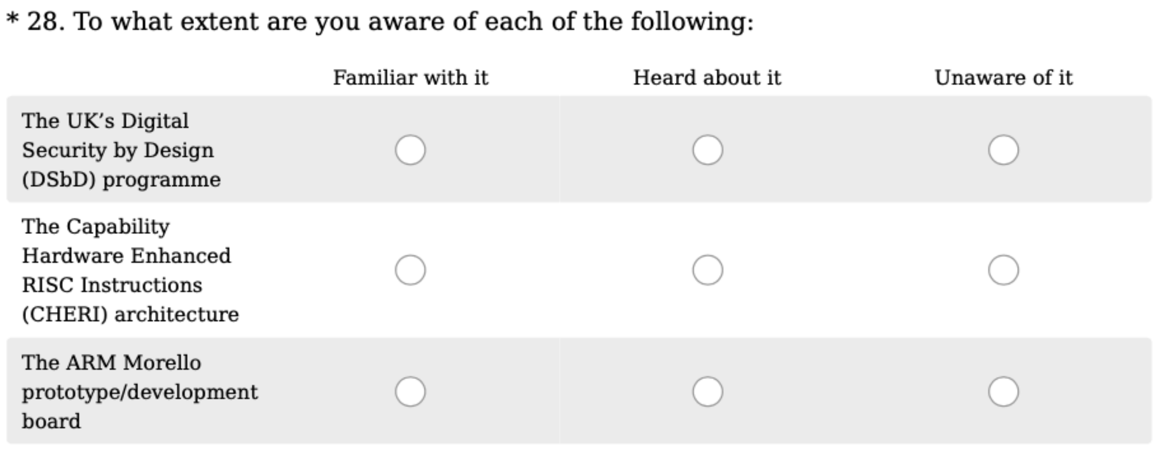
○ Disagree

○ Neutral

○ Agree

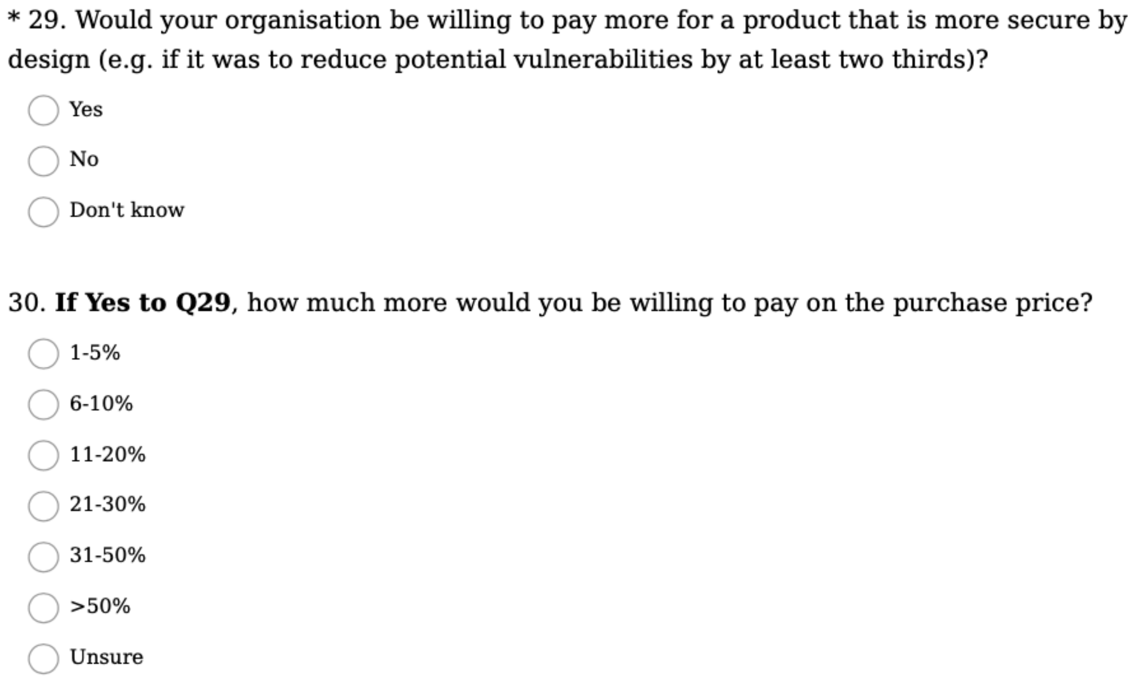
○ Strongly agree

○ Don't know



* 28. To what extent are you aware of each of the following:

	Familiar with it	Heard about it	Unaware of it
The UK's Digital Security by Design (DSbD) programme	○	○	○
The Capability Hardware Enhanced RISC Instructions (CHERI) architecture	○	○	○
The ARM Morello prototype/development board	○	○	○



* 29. Would your organisation be willing to pay more for a product that is more secure by design (e.g. if it was to reduce potential vulnerabilities by at least two thirds)?

○ Yes

○ No

○ Don't know

30. **If Yes to Q29**, how much more would you be willing to pay on the purchase price?

○ 1-5%

○ 6-10%

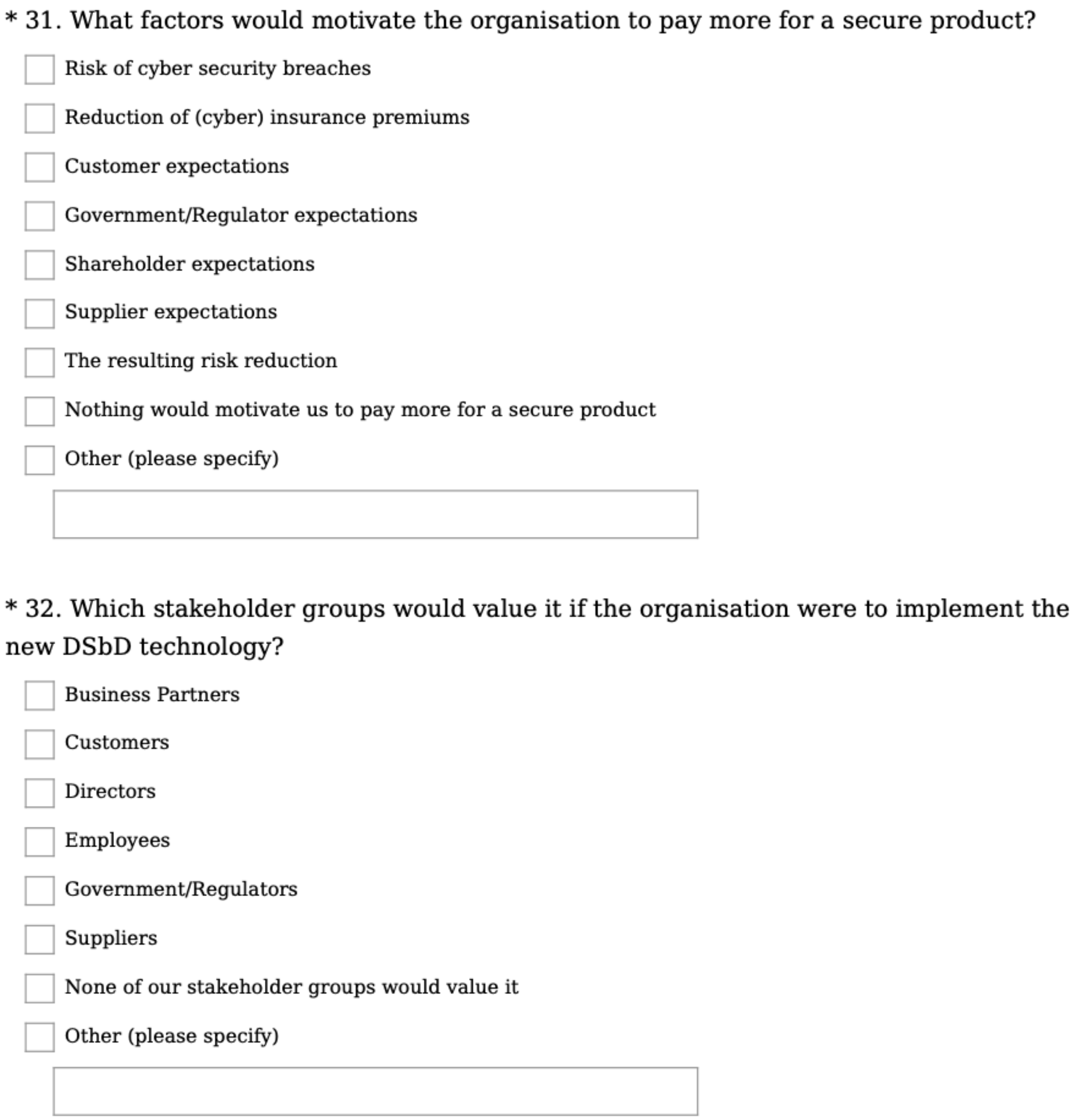
○ 11-20%

○ 21-30%

○ 31-50%

○ >50%

○ Unsure



* 31. What factors would motivate the organisation to pay more for a secure product?

□ Risk of cyber security breaches

□ Reduction of (cyber) insurance premiums

□ Customer expectations

□ Government/Regulator expectations

□ Shareholder expectations

□ Supplier expectations

□ The resulting risk reduction

□ Nothing would motivate us to pay more for a secure product

□ Other (please specify)

* 32. Which stakeholder groups would value it if the organisation were to implement the new DSbD technology?

□ Business Partners

□ Customers

□ Directors

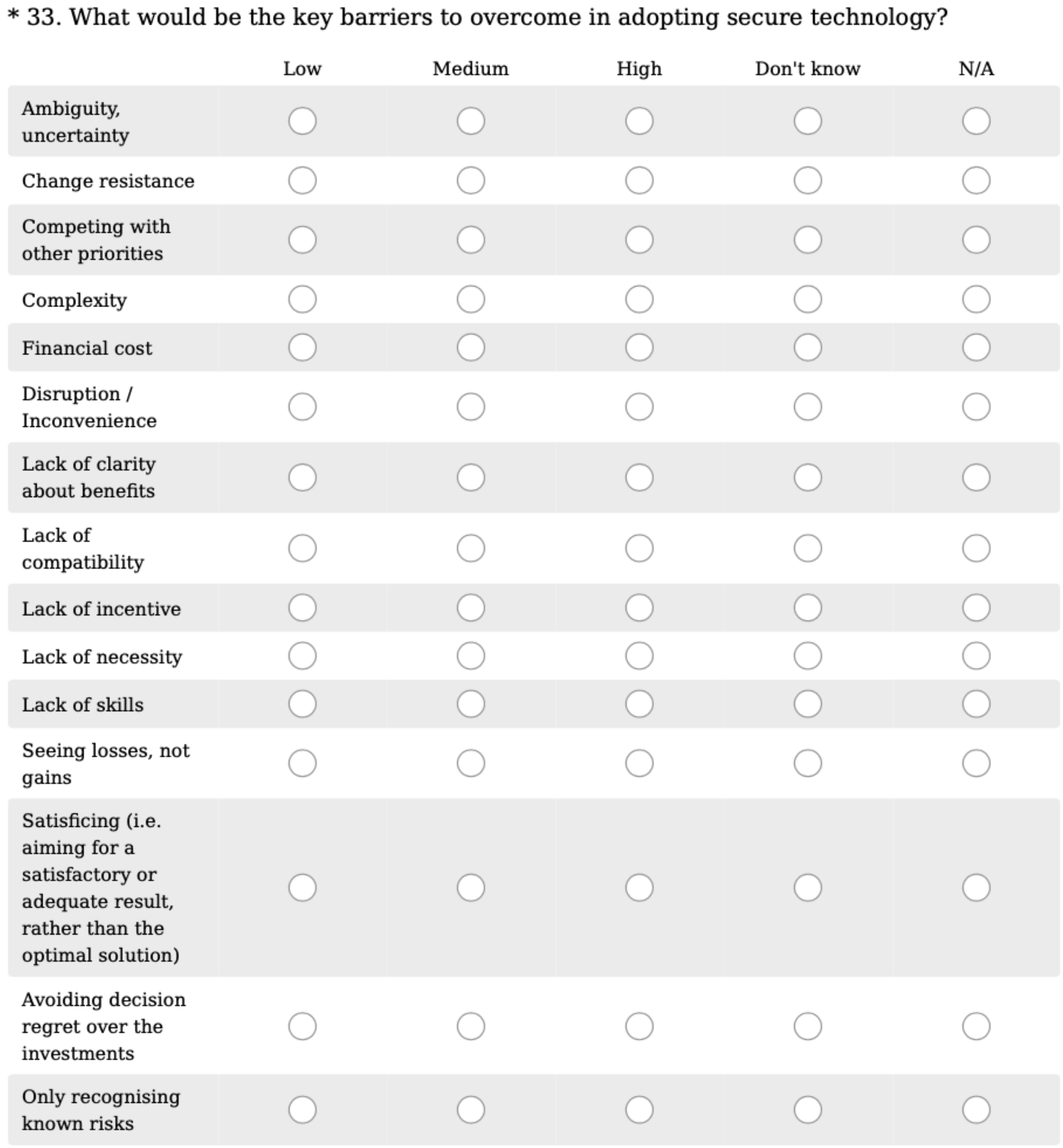
□ Employees

□ Government/Regulators

□ Suppliers

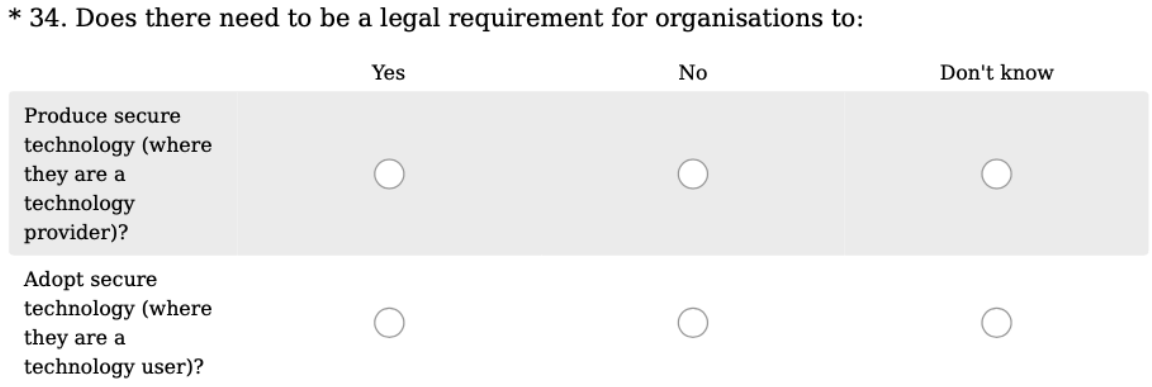
□ None of our stakeholder groups would value it

□ Other (please specify)



* 33. What would be the key barriers to overcome in adopting secure technology?

	Low	Medium	High	Don't know	N/A
Ambiguity, uncertainty	○	○	○	○	○
Change resistance	○	○	○	○	○
Competing with other priorities	○	○	○	○	○
Complexity	○	○	○	○	○
Financial cost	○	○	○	○	○
Disruption / Inconvenience	○	○	○	○	○
Lack of clarity about benefits	○	○	○	○	○
Lack of compatibility	○	○	○	○	○
Lack of incentive	○	○	○	○	○
Lack of necessity	○	○	○	○	○
Lack of skills	○	○	○	○	○
Seeing losses, not gains	○	○	○	○	○
Satisficing (i.e. aiming for a satisfactory or adequate result, rather than the optimal solution)	○	○	○	○	○
Avoiding decision regret over the investments	○	○	○	○	○
Only recognising known risks	○	○	○	○	○



* 34. Does there need to be a legal requirement for organisations to:

	Yes	No	Don't know
Produce secure technology (where they are a technology provider)?	○	○	○
Adopt secure technology (where they are a technology user)?	○	○	○

* 35. What do you believe would help your organisation to adopt devices based on secure-by-design hardware?

□ Pricing them competitively

□ A clear requirement or directive that pushes towards adoption

□ Access to expertise/advice to help understand what to look for and choose

□ We do not need help as we are already doing it

□ Nothing, as I do not perceive a need for such devices in our organisation

□ Other (please specify)

* 36. How should the adoption of secure-by-design hardware be further incentivised?

□ Subsidised hardware costs

□ Voluntary code of good practice

□ Regulatory requirements

□ Organically, via market forces

□ There is no need to incentivise the adoption

* 37. Which of these kittens is your favourite?

(Source: https://commons.wikimedia.org/wiki/File:Funny_Kitten.jpg)

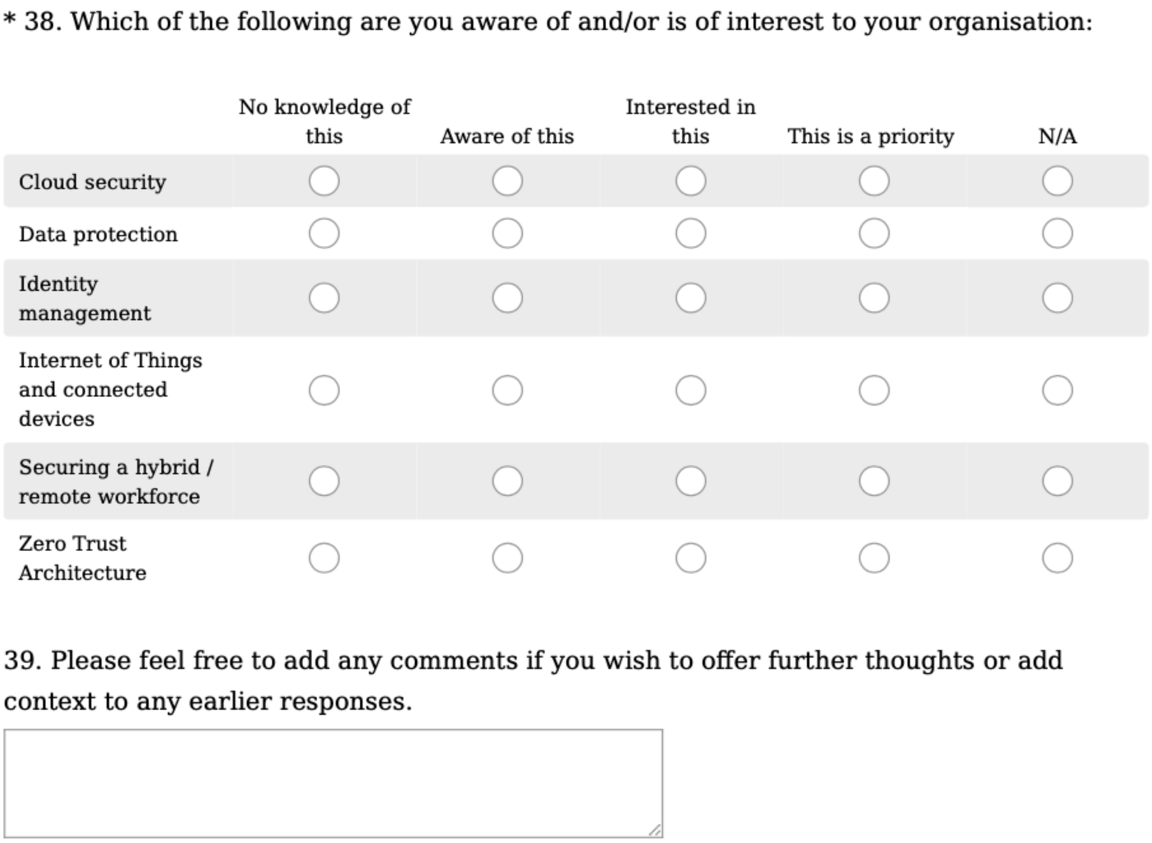
○ Left kitten

○ Middle kitten

○ Right kitten

○ I prefer puppies

○ None of the above



* 38. Which of the following are you aware of and/or is of interest to your organisation:

	No knowledge of this	Aware of this	Interested in this	This is a priority	N/A
Cloud security	○	○	○	○	○
Data protection	○	○	○	○	○
Identity management	○	○	○	○	○
Internet of Things and connected devices	○	○	○	○	○
Securing a hybrid / remote workforce	○	○	○	○	○
Zero Trust Architecture	○	○	○	○	○

39. Please feel free to add any comments if you wish to offer further thoughts or add context to any earlier responses.

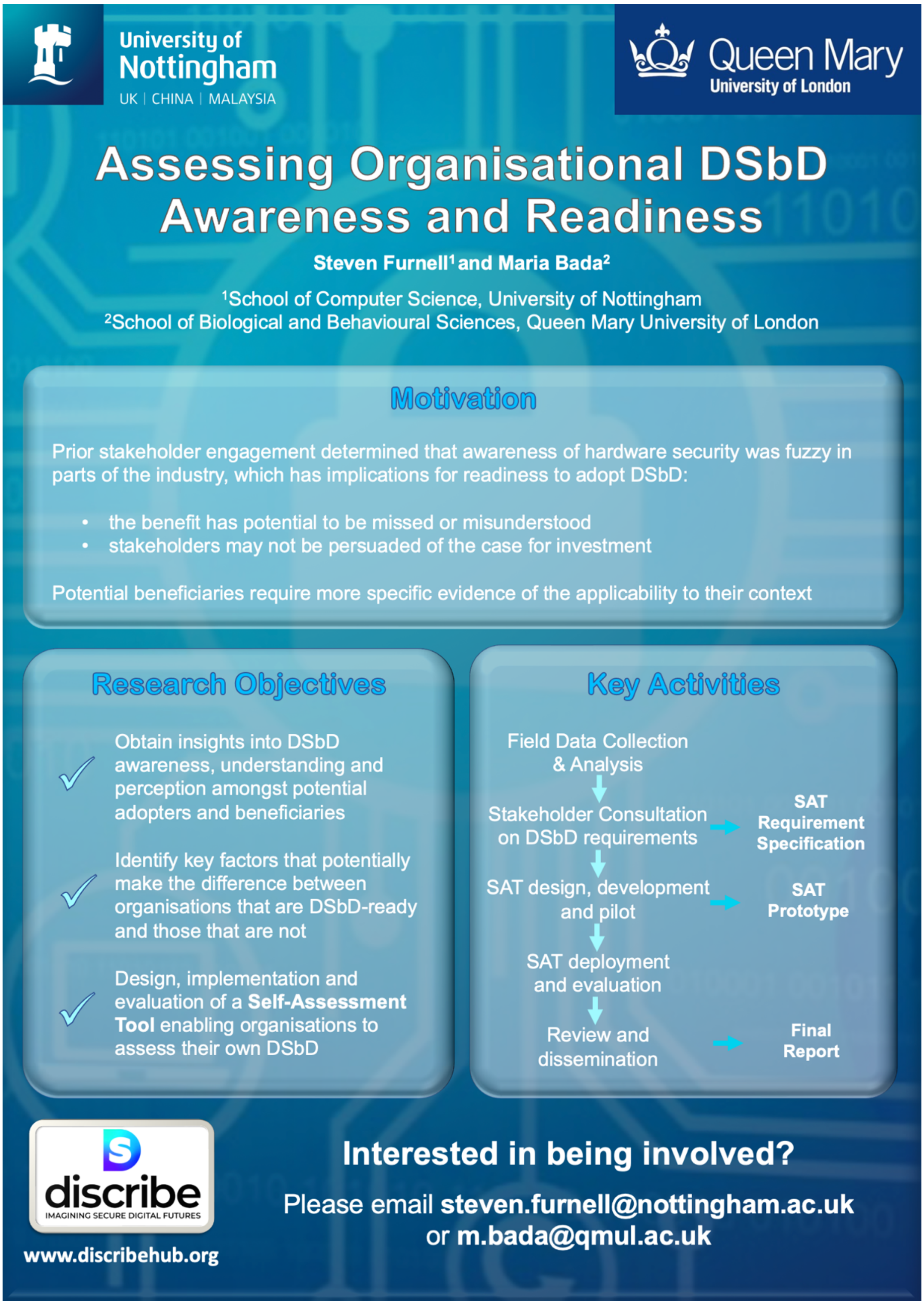
Appendix B – All-Hands Meeting Materials

This section presents materials used to promote the project activities and findings to date at a series of DSbD All-Hands Meetings.

Specifically, the materials presented over the following pages are:

- Project overview poster (April 2022)
- Survey promotional flyer (October 2022)
- Survey results poster (April 2023)
- Workshop promotional flyer (April 2023)

Project overview poster (April 2022)



University of Nottingham
UK | CHINA | MALAYSIA
Queen Mary
University of London

Assessing Organisational DSbD Awareness and Readiness

Steven Furnell[1] and Maria Bada[2]

[1]School of Computer Science, University of Nottingham
[2]School of Biological and Behavioural Sciences, Queen Mary University of London

Motivation

Prior stakeholder engagement determined that awareness of hardware security was fuzzy in parts of the industry, which has implications for readiness to adopt DSbD:

- the benefit has potential to be missed or misunderstood
- stakeholders may not be persuaded of the case for investment

Potential beneficiaries require more specific evidence of the applicability to their context

Research Objectives

✓ Obtain insights into DSbD awareness, understanding and perception amongst potential adopters and beneficiaries

✓ Identify key factors that potentially make the difference between organisations that are DSbD-ready and those that are not

✓ Design, implementation and evaluation of a **Self-Assessment Tool** enabling organisations to assess their own DSbD

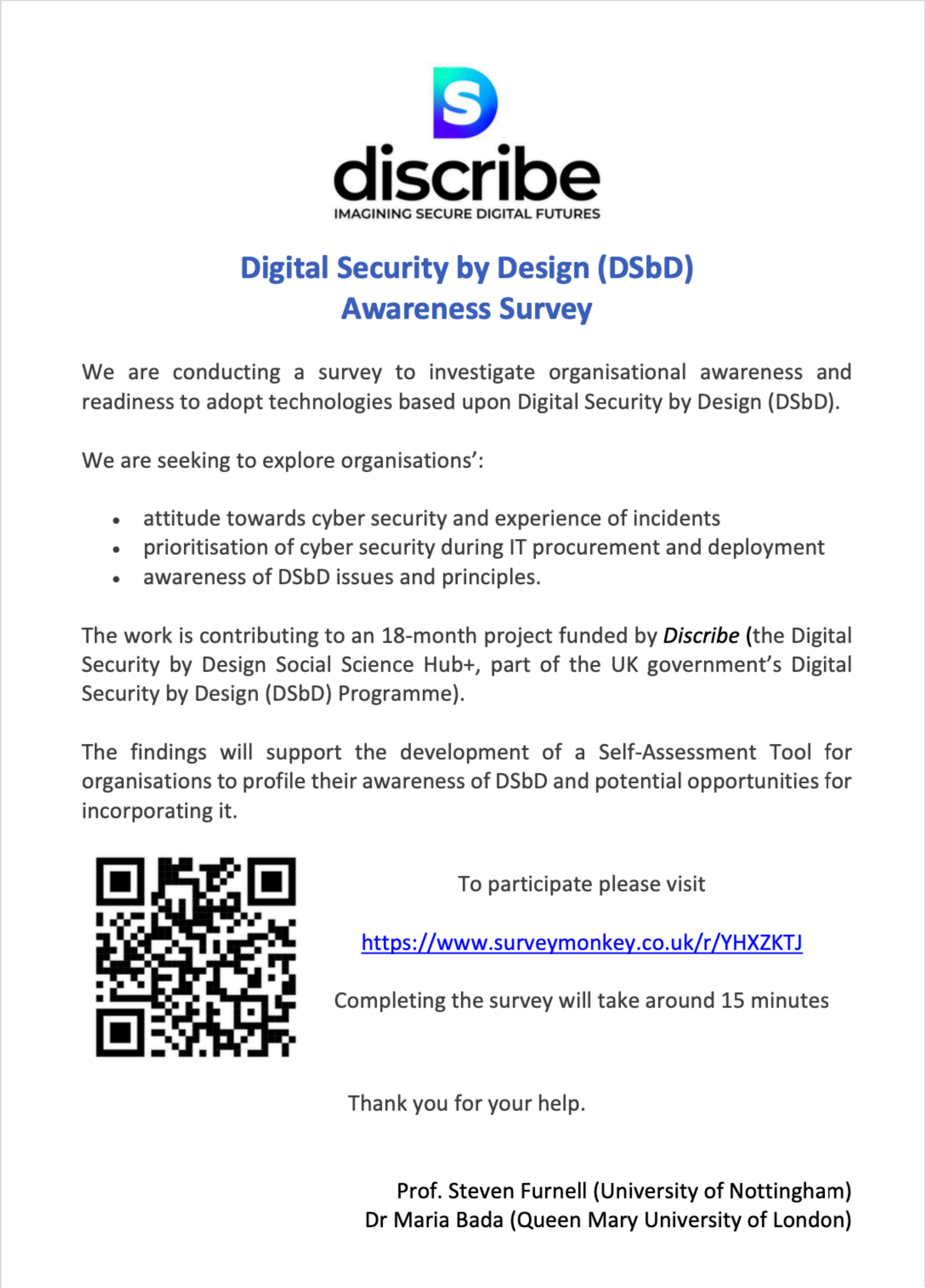
Key Activities

Field Data Collection & Analysis
↓
Stakeholder Consultation on DSbD requirements → **SAT Requirement Specification**
↓
SAT design, development and pilot → **SAT Prototype**
↓
SAT deployment and evaluation
↓
Review and dissemination → **Final Report**

Interested in being involved?

Please email **steven.furnell@nottingham.ac.uk** or **m.bada@qmul.ac.uk**

Survey promotional flyer (October 2022)



discribe
IMAGINING SECURE DIGITAL FUTURES

Digital Security by Design (DSbD)
Awareness Survey

We are conducting a survey to investigate organisational awareness and readiness to adopt technologies based upon Digital Security by Design (DSbD).

We are seeking to explore organisations':

- attitude towards cyber security and experience of incidents
- prioritisation of cyber security during IT procurement and deployment
- awareness of DSbD issues and principles.

The work is contributing to an 18-month project funded by ***Discribe*** (the Digital Security by Design Social Science Hub+, part of the UK government's Digital Security by Design (DSbD) Programme).

The findings will support the development of a Self-Assessment Tool for organisations to profile their awareness of DSbD and potential opportunities for incorporating it.

To participate please visit

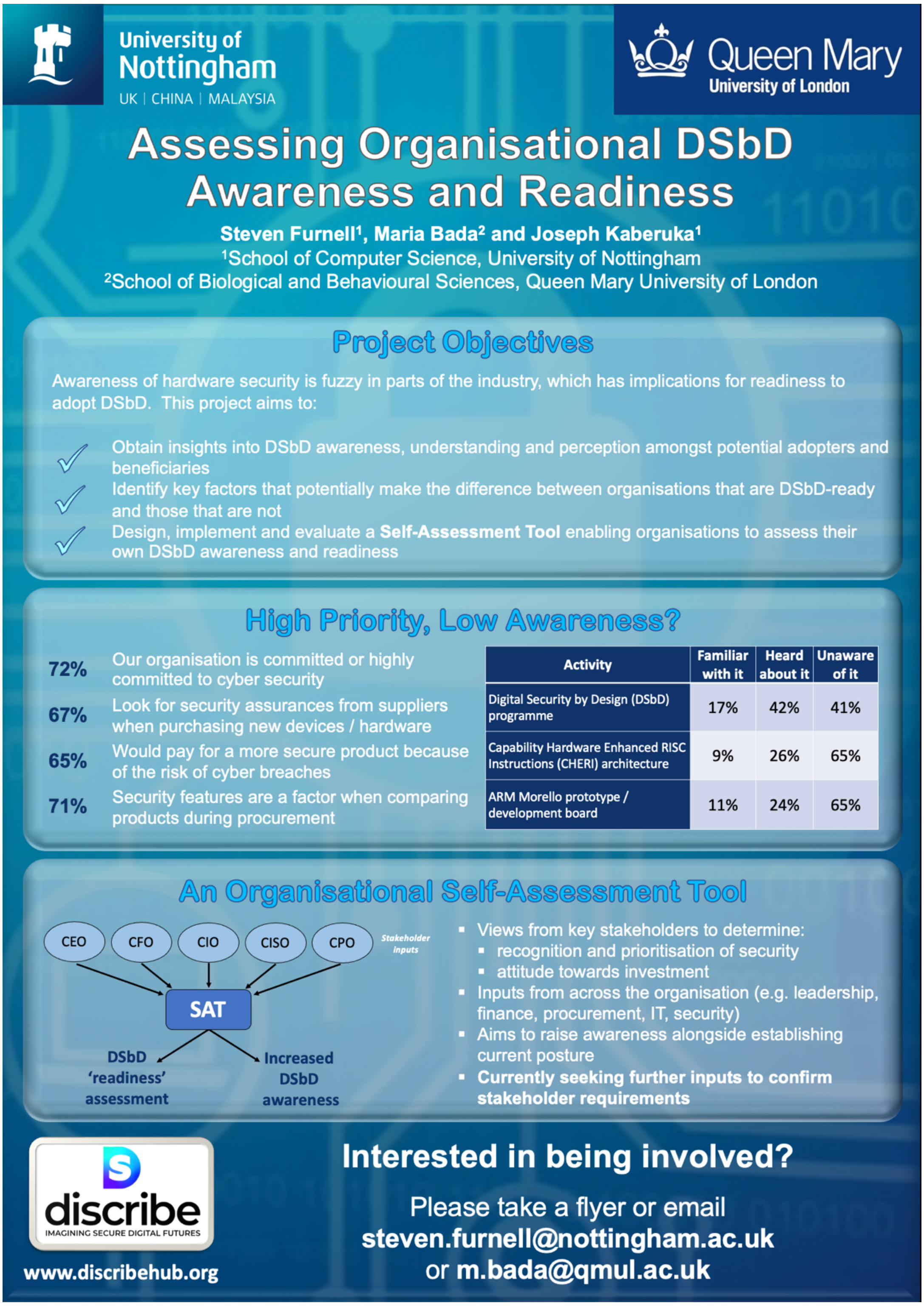
https://www.surveymonkey.co.uk/r/YHXZKTJ

Completing the survey will take around 15 minutes

Thank you for your help.

Prof. Steven Furnell (University of Nottingham)
Dr Maria Bada (Queen Mary University of London)

Survey results poster (April 2023)



University of Nottingham
UK | CHINA | MALAYSIA

Queen Mary
University of London

Assessing Organisational DSbD Awareness and Readiness

Steven Furnell[1], Maria Bada[2] and Joseph Kaberuka[1]
[1]School of Computer Science, University of Nottingham
[2]School of Biological and Behavioural Sciences, Queen Mary University of London

Project Objectives

Awareness of hardware security is fuzzy in parts of the industry, which has implications for readiness to adopt DSbD. This project aims to:

- ✓ Obtain insights into DSbD awareness, understanding and perception amongst potential adopters and beneficiaries
- ✓ Identify key factors that potentially make the difference between organisations that are DSbD-ready and those that are not
- ✓ Design, implement and evaluate a **Self-Assessment Tool** enabling organisations to assess their own DSbD awareness and readiness

High Priority, Low Awareness?

72%	Our organisation is committed or highly committed to cyber security
67%	Look for security assurances from suppliers when purchasing new devices / hardware
65%	Would pay for a more secure product because of the risk of cyber breaches
71%	Security features are a factor when comparing products during procurement

Activity	Familiar with it	Heard about it	Unaware of it
Digital Security by Design (DSbD) programme	17%	42%	41%
Capability Hardware Enhanced RISC Instructions (CHERI) architecture	9%	26%	65%
ARM Morello prototype / development board	11%	24%	65%

An Organisational Self-Assessment Tool

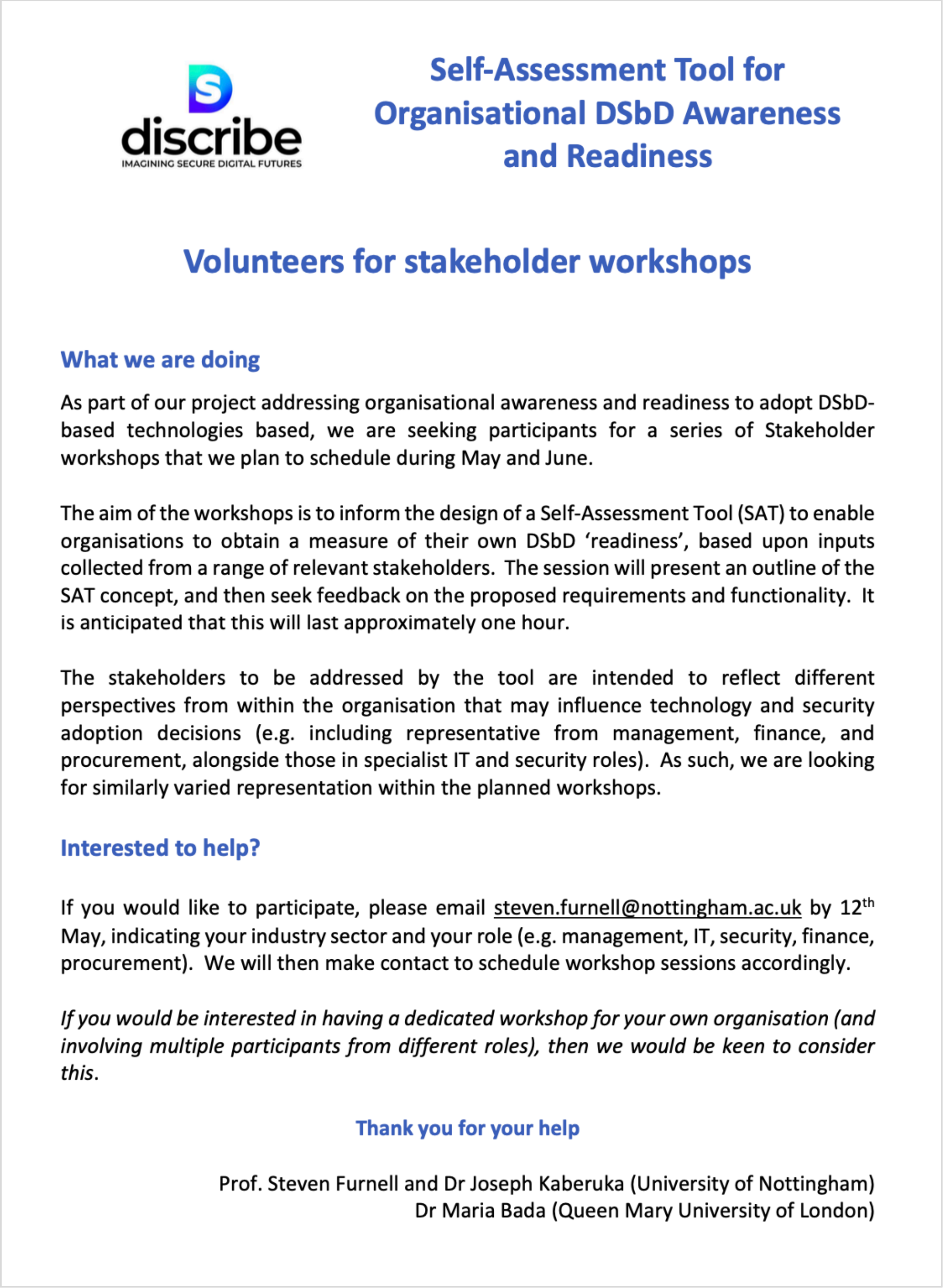
- Views from key stakeholders to determine:
  - recognition and prioritisation of security
  - attitude towards investment
- Inputs from across the organisation (e.g. leadership, finance, procurement, IT, security)
- Aims to raise awareness alongside establishing current posture
- **Currently seeking further inputs to confirm stakeholder requirements**

discribe
IMAGINING SECURE DIGITAL FUTURES
www.discribehub.org

Interested in being involved?

Please take a flyer or email
steven.furnell@nottingham.ac.uk
or **m.bada@qmul.ac.uk**

Workshop promotional flyer (April 2023)



discribe
IMAGINING SECURE DIGITAL FUTURES

Self-Assessment Tool for Organisational DSbD Awareness and Readiness

Volunteers for stakeholder workshops

What we are doing

As part of our project addressing organisational awareness and readiness to adopt DSbD-based technologies based, we are seeking participants for a series of Stakeholder workshops that we plan to schedule during May and June.

The aim of the workshops is to inform the design of a Self-Assessment Tool (SAT) to enable organisations to obtain a measure of their own DSbD 'readiness', based upon inputs collected from a range of relevant stakeholders. The session will present an outline of the SAT concept, and then seek feedback on the proposed requirements and functionality. It is anticipated that this will last approximately one hour.

The stakeholders to be addressed by the tool are intended to reflect different perspectives from within the organisation that may influence technology and security adoption decisions (e.g. including representative from management, finance, and procurement, alongside those in specialist IT and security roles). As such, we are looking for similarly varied representation within the planned workshops.

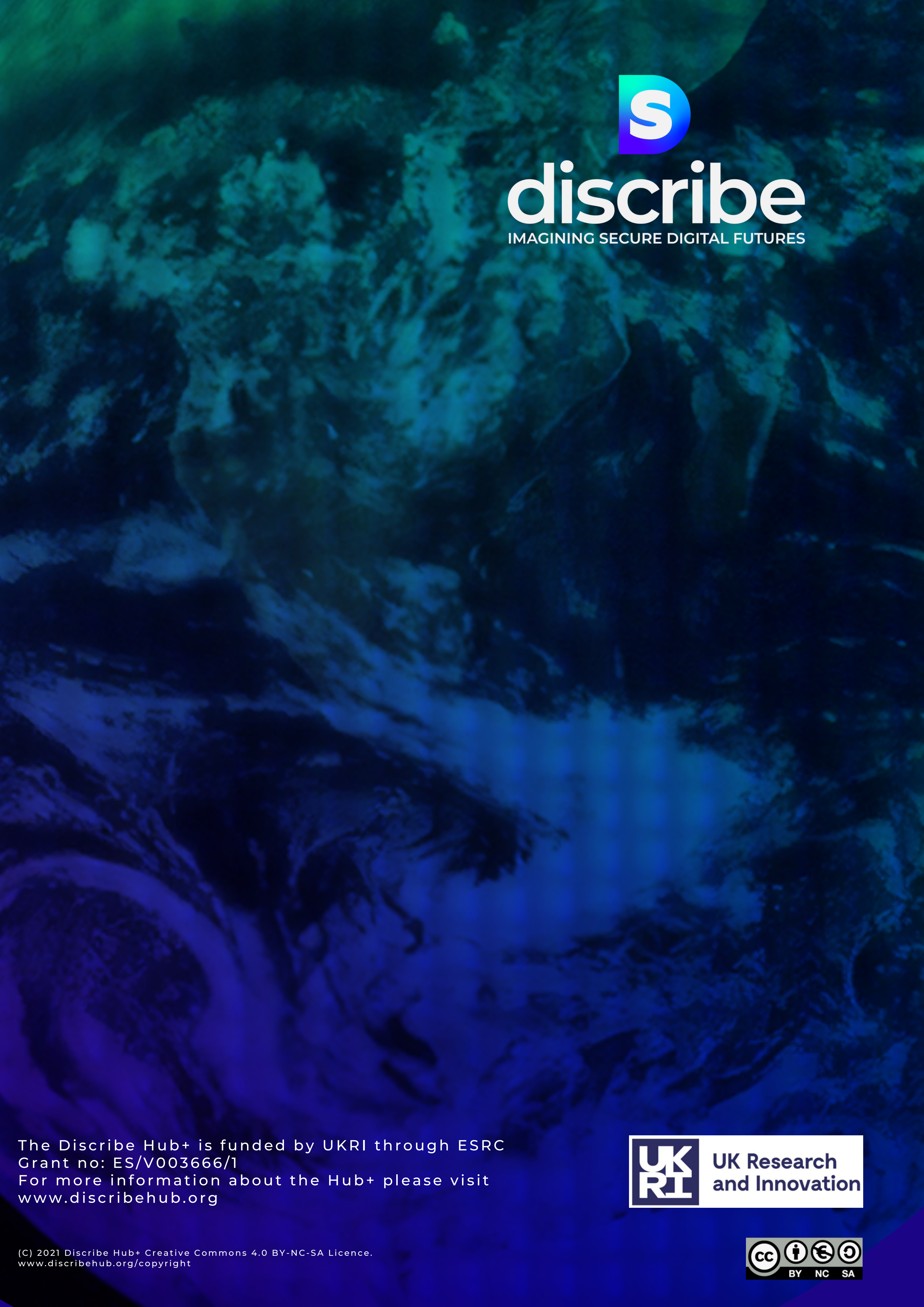
Interested to help?

If you would like to participate, please email steven.furnell@nottingham.ac.uk by 12th May, indicating your industry sector and your role (e.g. management, IT, security, finance, procurement). We will then make contact to schedule workshop sessions accordingly.

If you would be interested in having a dedicated workshop for your own organisation (and involving multiple participants from different roles), then we would be keen to consider this.

Thank you for your help

Prof. Steven Furnell and Dr Joseph Kaberuka (University of Nottingham)
Dr Maria Bada (Queen Mary University of London)



discribe

IMAGINING SECURE DIGITAL FUTURES

The Discribe Hub+ is funded by UKRI through ESRC
Grant no: ES/V003666/1
For more information about the Hub+ please visit
www.discribehub.org

UK Research and Innovation