Assessing Organizational Awareness and Acceptance of Digital Security by Design

Steven Furnell[1], Maria Bada[2] and Joseph Kaberuka[1]

[1] University of Nottingham, Nottingham, UK
[2] Queen Mary University of London, London, UK

{steven.furnell; joseph.kaberuka}@nottingham.ac.uk; m.bada@qmul.ac.uk

Abstract

A significant proportion of attacks on current systems are facilitated by the exploitation of vulnerabilities inherent in the underlying design of the technology concerned or components within it. As such, there is now significant focus on the issue of enabling Security by Design; building in the protection from the outset and avoiding vulnerabilities at source. Related initiatives are now in progress to deliver hardware technologies that would form the foundation for future devices, but questions remain over the understanding and readiness of potential adopters to recognize and implement the resulting approaches. This paper reports upon a survey that was undertaken as part of a funded project to investigate organizational awareness and acceptance of the Digital Security by Design (DSbD) concept. Detailed responses were received from over 70 UK-based organizations, with the respondents themselves largely coming from a security background and in strong general support of the principle of maintaining cyber security. As such, the findings provide a relevant insight into whether an already pro-security group would be willing to go further in terms of their security commitment. The findings reveal that while the generally positive perspective prevails, there is currently relatively limited awareness of DSbD itself, and a variety of challenges that may be faced in promoting the adoption in practice. At the same time, there is general support for more effort to be made to incentivize and to some extent require the use of DSbD-technology once it becomes more widely available.

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.

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 behavior 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 work presented in this paper has been conducted as part of a specific project linked to the first of these points, with the research as a whole seeking to address two elements are considered to merit further attention:

- 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.
- 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).

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. As such, 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.

Investigating organizational 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 organizations':

- 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 organizations, 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.

Table 1: Topic coverage within the awareness and readiness survey

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

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 favorite 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, emails to members of the mailing list for the DSbD community, leaflet-based promotion at two face-to-face security events, social media postings on LinkedIn and Twitter, and Inclusion in the a Cyber Security Newsletter distributed by the responsible department of the UK government (see https://www.gov.uk/government/publications/dcms-cyber-security-newsletter-december-2022/dcms-cyber-security-newsletter-december-2022). 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, 30% 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).

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.

In spite of 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.

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).

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.

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).

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 paper, 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.

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

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%

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). On this basis 54% indicated that they would pay more, 35% did not know, and only 11% explicitly indicated that they would not do so.

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, with customers being the most prominent, cited by 52% and the only group exceeding the 50% threshold (Government and Regulators comes close at 48%, but the third-ranked, Business Partners, is then at 35%). Only 6% felt that no-one would value it.

In terms of steps that would help organizations 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 organization (i.e. consistent with the earlier proportion that felt no-one would value it being adopted).

When asked more specifically about what would further incentivize adoption, regulatory requirement was again the most prominent choice (72%). This compares with 37% for subsidized hardware costs, 33% for a voluntary code of practice, and 22% suggesting allowing things to develop organically via market forces. Notably only 2% felt there was no need for incentivization.

There was strong support for the introduction of legal measures to promote secure approaches, with 78% supporting the need for a legal requirement for providers to *produce* secure technology, and 67% for a requirement to *adopt* it as a technology user.

Discussion

Although the response rate was ultimately lower than the authors 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.

Table 3: Awareness and prioritization of other topical cybersecurity issues

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%

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 'favorable' 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.

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 paper 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.

Acknowledgements

The research described in this paper is supported by the Discribe Hub+ project, which is funded until 2024 by the UK Government's Industrial Strategy Challenge Fund (ISCF) under the Digital Security by Design (DSbD) Programme, to support the DSbD ecosystem. The support of the Economic and Social Research Council (ESRC) is gratefully acknowledged.

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