An Organizational Self-Assessment Tool for Digital Security by Design

Steven Furnell[1], Maria Bada[2], Michal Kukula[1] and Lucija Šmid[3]

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

steven.furnell@nottingham.ac.uk; m.bada@qmul.ac.uk

Abstract

The concept of Digital Security by Design (DSbD) offers a means to improve the security of IT devices by eliminating areas of vulnerability that are often exploited in related attacks. However, the availability of improved technology does not automatically ensure that it will be understood and adopted by potential beneficiaries. Indeed, perceptions and priorities may even vary within the same organization, depending on the role and perspectives of different stakeholders involved in the decision-making. As such, organizations can benefit from a means to assess their environment and the extent of stakeholder alignment in understanding and supporting the security need. Building upon prior work that has assessed organizational DSbD awareness, and then proposed a related assessment methodology, the main focus of this paper is a resulting Self-Assessment Tool that has been designed and developed to support the process. A key focus is the realization of a proof-of-concept prototype, which provides a means of demonstrating how data is collected from stakeholders and then the various ways in which the results can be visualized in order to assist the organization in assessing its positioning over time. The discussion then proceeds to consider the results of related evaluation by a group of senior cyber-related stakeholders, identifying areas of support for the concept as well as a range of issues that can be considered for enhancement.

Introduction

Secure by Design technologies have significant potential to improve the baseline level of security within deployed devices, reducing or removing vulnerabilities that have led to successful cyber attacks in the past. However, it is also recognized that resulting technology adoption is unlikely to be a simple case of 'build it and they will come', raising the question of how potential adopters of the technology can be better supported in recognizing and understanding their own needs. Building upon the foundations of prior papers (Furnell et al. 2023; Furnell et al. 2025), in which we have investigated the current level of organizational awareness of Digital Security by Design (DSbD) and outlined of a self-assessment method to allow organizations to profile their adoption readiness, this paper presents the proof-of-concept implementation of resulting Self-Assessment Tool that enables the collection, collation and analysis of responses from relevant stakeholders within the organization. The resulting approach is intended to provide insights into the awareness, understanding and perception of DSbD amongst relevant potential adopters and beneficiaries. In particular, the approach helps to identify key factors and linkages that potentially make the difference between organizations/environments that are DSbD-ready and those that are not. In broad terms, this provides insights around the level of 'security awareness' an organization needs in order to embrace DSbD. The Self-Assessment Tool is key to the approach, enabling organizations to assess their own DSbD readiness, and particularly to assess the level of alignment between different parties, helping to address the questions of whether the related investment is needed and will work.

The approach and the work that led up to it point has already been addressed in the earlier papers. This paper is therefore focused on the realization of the Self-Assessment Tool prototype and its evaluation by relevant stakeholders. The next section presents some general background on the DSbD concept and a related UK initiative that has supported the work. This leads into an overview of the foundations for them proposed assessment approach, considering the stakeholders that may be involved and the data to be collected form them. From this basis, the main focus of the discussion is to detail the proof-of-concept implementation of a prototype Self-Assessment Tool, which is then exposed to practical evaluation by a series of relevant cyber professionals. The discussion then reflects upon the positives observed from this, as well as various areas for potential enhancement and refinement. The paper concludes by considering the intended role of the SAT and the extent to which the work has addressed this.

Background

In order to provide context for the presentation of the Self-Assessment Tool itself, it is relevant to recap the context in which the work has been conducted. This was presented in more detail in the earlier papers (Furnell et al. 2023; Furnell et al. 2025) and so is treated in abridged form here in order to cover the key points.

In the UK, the UK's Digital Security by Design (DSbD) initiative aims to "radically update the foundation of the insecure digital computing infrastructure by creating a new, more secure hardware and software ecosystem" (DSbD, 2024). Key to the program are the Capability Hardware Enhanced RISC Instructions (CHERI) architecture and the Morello prototype. CHERI extends the CPU instruction and enables memory access using *capabilities* instead of machine-word pointers (Woodruff et al., 2014). Meanwhile, Arm's Morello program (see www.arm.com/architecture/cpu/morello) is a prototype system-on-chip (SoC) and a development board which provides a realization of the CHERI approach. However, simply providing a viable DSbD solution is not sufficient – it needs to find its way through to adoption in practice, and this may be a non-trivial undertaking at several levels, from technology developers and manufacturers (for whom it may call for new mindset and methods), through to end consumers (who need to see the value in upgrading to something new in place of existing technologies that ostensibly 'do the job' already). Recognizing these challenges, the DSbD program included the establishment of the Digital Security by Design Social Science Hub+ (Discribe – see www.discribehub.org) to apply social and economic science to the adoption of new secure technologies.

Most decision-makers are now aware of cyber security and would often claim it as a priority. For example, the 2024 release of the UK Cyber Security Breaches Survey suggests that 75% of businesses consider their directors and other senior managers to regard security as a high priority (DSIT, 2024a). Moreover, this proportion rises significantly as the size of organization increases – with 93% of medium and 98% of large businesses claiming to view security in this way. However, the reality can still be that different stakeholders within the organization will view things differently. For example, a business manager's perception of risk and probability is often based on perceptual quantities that can often be biased (Straub & Welke, 1998; Tversky & Kahneman, 1974). As a result, their view of what is timely and appropriate may differ from that of those leading the technical areas of the organization. As such, even where secure-by-design technologies are available, the resulting security still relies on organizations to take the decision to adopt them rather than favor less secure – but potentially 'easier' (e.g. in terms of cost, effort) alternatives.

While regulation could be used to oblige uptake, this could lead to resistance and in any case would not assist adopters in understanding their need for the new technology. As such, it is arguably preferable to offer a means by which awareness can be raised and later adoption can then be driven by organizations' own increased understanding.

Unfortunately, it is well recognized that a mismatch between stakeholder opinions within organizational settings can lead to security being the element that is compromised (Vachon, 2024). In some cases, this will be an intentional prioritization of other factors (e.g. revenue, profit, convenience, and inertia being common examples). However, in other scenarios there may be a lack of collective understanding of the related requirements and a lack of ability to capture and reflect upon the differing stakeholder perspectives. As such, there is a need for related consultation with organizational stakeholders, and the next section begins to discuss the design of an approach that enables assessment of DSbD awareness and readiness within their own environments.

Findings from other research within the DSbD program have provided further evidence and justification of the need to increase stakeholder engagement, specifically in relation to the awareness of the CHERI architecture (DSIT, 2024b). The findings indicate that it is typically recognized amongst people in technical, research and cyber security officer roles. Meanwhile, those in senior decision-making positions in large companies are less aware. While this is instinctively not surprising, the question remains about how to address the issue. Two of the notable recommendations in the report are:

- Supporting senior decision-makers in companies to appreciate the increasing hostility of the online environment and the resulting relevance of CHERI adoption;
- Helping CEOs to understand the risks to their businesses from insecure hardware.

These recommendations align well with the objectives of the current work, and the original premise for the Self-Assessment Tool.

Self-Assessment Tool foundations

The tool is based upon a self-assessment methodology previously discussed in Furnell et al. (2025). In order to set the context for understanding the presentation of the prototype, this section outlines the multi-stakeholder data collection that forms the basis of the self-assessment.

Incorporating stakeholder perspectives

A key aspect of the approach and the concept of the resulting tool is to capture related views from different segments of the business. The underlying premise here is that different stakeholders are likely to have different perspectives and perceptions in relation to the security issues and the need to address them, as well as how these needs may compare to other business priorities. While one might argue that the CISO (or equivalent) is most likely to be the stakeholder with the 'correct' perspective, and that other voices may not be as valid in determining what should be done, it may nonetheless be useful to the organization to recognize where disparities and differences of opinion may exist. As such, the act of involving and capturing inputs from other stakeholders can be helpful in promoting a wider understanding of DSbD (and cybersecurity more generally) and supporting related consensus building.

These represent a cross-section of roles that could each have significant impact upon security-related decision making, either directly (because it falls into their domain) or indirectly (based on the fit with other business priorities and perceptions). As can be seen from Table 2, the stakeholders can be broadly categorized as business or technically focused, which may be relevant groups to compare in terms of the responses in various aspects of the assessments.

In practice, the specific stakeholders that an organization elects to include in the self-assessment process could vary, and so the design of the SAT is not tied to using a specific pre-defined set of roles. However, as a basis for illustration, and to demonstrate why different stakeholder perspectives are relevant to capture, consideration can be given to five stakeholder perspectives indicated in Table 1 (which are also more broadly grouped according to whether they are considered have a business or technical focus, which can be useful perspectives to compare when trying to understand where views may differ and work towards consensus). The 'rationale for inclusion' shows how each party could have a role in (or at least an impact upon) security-related decision making. In some cases, these are direct (because it falls into the stakeholder's own domain) or indirect (based on the their role in setting or deciding things in relation to other business priorities).

Table 1: Stakeholder types to involve in data collection

Stakeholder		Description	Rationale for inclusion
Business	CEO	Chief Executive Officer (may also be known as Managing Director) The CEO is the highest-ranking executive in a company. Primary responsibilities include making major corporate decisions, managing operations and	Representing the senior leadership perspective, and likely to be setting the overall tone and priority towards cybersecurity for the organization. Depending upon the organization, the actual role may be Managing Director, or similar.

Stakeholder		Description	Rationale for inclusion
		resources and acting as the main point of communication between the board of directors and corporate operations (Dooley, 2024).	
	CFO	Chief Financial Officer The CFO is a key role across businesses and functions, and is the CEO's strategic partner in maximizing value creation. The CFO helps with shaping portfolio strategies, undertaking major investment and financing decisions, and communicating with key stakeholders—all while leading a multitalented and technologically savvy finance team. Communication is a key part of the role, both with investors and boards (McKinsey & Company, 2023).	Representing the finance perspective, which is significant in ensuring that cyber security receives sufficient resource and prioritization to enable investment to happen.
	CPO	Chief Procurement Officer (may also be known as Chief Acquisitions Officer) The chief procurement officer, or CPO, leads an organization's procurement department and oversees the acquisitions of goods and services made by the organization. The CPO ensures that purchases will meet organizational needs while helping to reduce costs, give higher profit margins or both (Yasar and Pratt, 2022). This role is serving as a wider strategic driver helping firms manage supply chain risk (Lacina, 2023).	Representing the procurement / purchasing perspective, which is relevant when considering the influence on when, where and how new technology investments are realized.
Technical	CIO	Chief Information Officer (may also be known as IT Manager) The CIO oversees the people, processes and technologies within a company's IT organization to ensure they deliver outcomes that support the goals of the business. Also, the CIO plays a key leadership role in the critical strategic, technical and management initiatives — from information security and algorithms to customer experience and leveraging data — that mitigate threats and drive business growth (Gartner, nd).	Representing the overall IT perspective of the organization. In practice the role could also be the Chief Technology Officer, IT manager, Head of IT, or similar.

Stakeholder		Description	Rationale for inclusion
	CISO	Chief Information Security Officer A CISO is, usually, a C-suite executive who oversees an organization's information security, developing and implementing information security policies, from risk management and policy development to compliance and incident response planning (Woollacott, 2024).	Representing the responsibility for cyber security provision and decision making. Depending upon the size of the organization, this stakeholder function may not be distinct from the CTO position.

In practice, organizations may not have distinct representatives for all roles in the table, and so have the ability to customize the names and assignment of roles to suit their local requirements. At the same time, it is expected that for the tool to be relevant and viable to use, there would need to be at least three distinct stakeholders to involve, and for them to collectively span the business and technical perspectives of the business. If too many roles are held by too few people (e.g. as may be the case in smaller organizations, where for example, the CEO, CFO and CPO roles could conceivably all be represented by the same individual), then there is no potential to capture them as distinct stakeholder perspectives.

Self-assessment data

The data collection within the SAT is based upon a series of assessment questions that were established in earlier stages of the work. These are presented in detail as part of the earlier coverage of the assessment methodology (Furnell et al. 2025), but the core themes are summarized in Table 2. These collectively aim to profile how security is viewed, the current security posture of the organization, and the consequent potential for investment and adoption of enhanced technologies.

Table 2: Data collection categories within the self-assessment methodology

Data capture (category and total questions)		Rationale	
Technology and Data Usage (TDU)	6	The need for security based upon what the organization is using the technology for, its dependence upon it, etc.	Informs 'Need' rating
Incidents and Breaches (IAB)	10	Highlights the organization's need for security based upon evidence of exposure, plus suggests the extent to which it already on the agenda.	
Security Priority and Investment (SPI)	10	Attitudes toward security in the organization as a whole.	Informs 'Attitude' rating
Security (in) Technology Adoption (STA)	11	More specific focus upon considerations at the technology investment level (i.e. which is more likely to affect DSbD adoption decisions).	
DSbD-Specific Awareness (DSA)	10	More specifically focused on the CISO/CIO elements of the organization 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.	Informs 'Awareness' rating

The ratings mentioned in the final column of Table 2 are intended as higher-level scorecard-style indicators that would enable an organization to see and track its overall posture. The three measures are defined as follows:

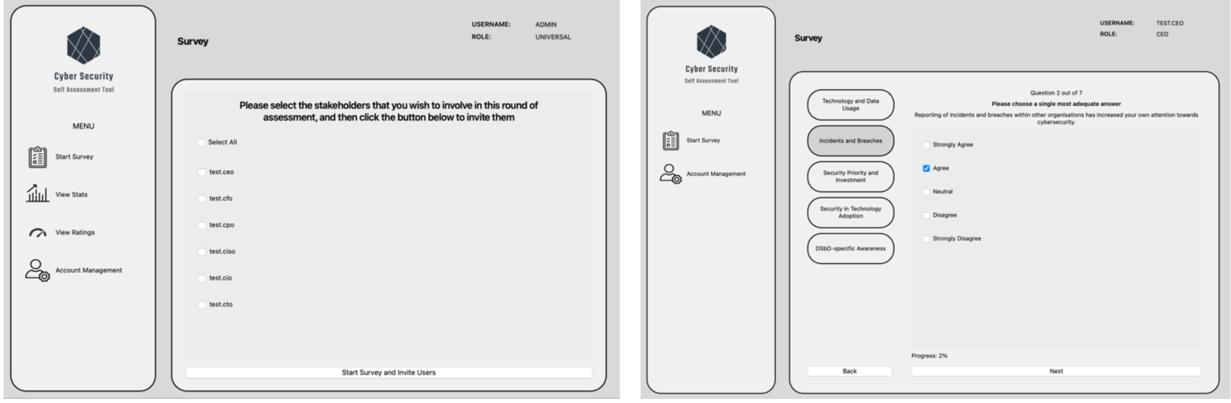
- *Need*: Supports understanding of why security is relevant to the organization. Technical stakeholders may be the most likely source for authoritative / factual responses, but wider stakeholders offer a means to determine whether the perception/understanding is consistent across different business functions.
- *Attitude*: Reflecting what an organization is likely to do in terms of security and related decision-making. While security-focused stakeholders would be expected to exhibit the most positive perspective, it is interesting to compare their stance to that of the other groups in order to assess alignment.
- *Awareness:* Focused on appetite to adopt DSbD-based technologies as future opportunities emerge, where there may again be perceptual differences across the stakeholders.

The full assessment methodology includes 47 questions, but the number that would be encountered in practice depends upon the stakeholders concerned, and the nature of their responses (e.g. some responses can lead to further questions that would otherwise be suppressed). Additionally, certain questions are only asked in cases where the organization is a *producer* of its own products/technologies (i.e. where DSbD could be adopted as part of their own product design and development process).

Self-Assessment Tool Prototype

The prototype realizes the core functionality of the SAT design. It is fully functional in terms of supporting multi-stakeholder data collection based upon the self-assessment question set, and offers an administrator view with resulting data visualization and ratings. As such, it can be considered to represent at least an initial proof-of-concept version of the tool.

The process begins with the registration of the desired stakeholders to be involved in the assessment activities. Once this has been done, the SAT administrator is able to launch assessment runs and nominate which stakeholders are expected to participate (Figure 1a). At this stage, any of the nominated stakeholders logging into the SAT will be presented with a new survey to complete (Figure 1b).



USERNAME: ADMIN
ROLE: UNIVERSAL

Please select the stakeholders that you wish to involve in this round of assessment, and then click the button below to invite them

□ Select All

□ test.ceo

□ test.cfo

□ test.cpo

□ test.ciso

□ test.cio

□ test.cto

USERNAME: TEST.CEO
ROLE: CEO

Question 2 out of 7

Please choose a single most adequate answer

Reporting of incidents and breaches within other organisations has increased your own attention towards cybersecurity.

□ Strongly Agree

☑ Agree

□ Neutral

□ Disagree

□ Strongly Disagree

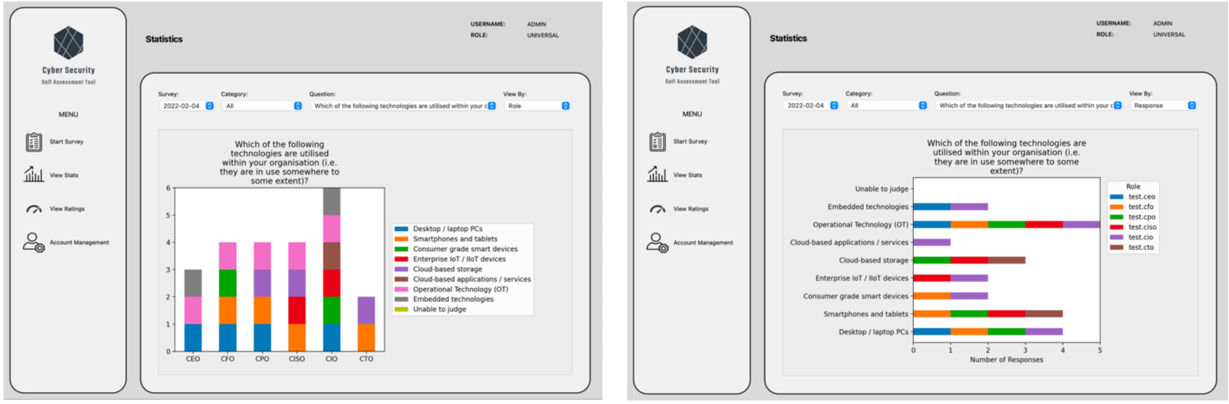
Progress: 2%

(a) (b)

Figure 1: Self-assessment (a) survey initiation and (b) data collection

Once data bas been collected, the main use of the tool comes into focus, allowing it to be used as a means of assessing the alignment of the viewpoints, and providing a potential provocation of interest for the stakeholders. The screenshots presented in Figures 2 to 4 depict a series of data visualizations that are possible for the responses to individual questions, drawn from across the stakeholders that participated in a given assessment run. It should be noted that the charts presented here are based upon dummy data that was used for the purposes of testing, and therefore is not reflective of any real-world organization or actual stakeholder responses.

Figure 2a shows the view by stakeholder role, and gives a clear indication of the degree to which the same response items were selected by different stakeholders. Using the specific chart here as an example, it is possible to immediately observe that the stakeholders appear rather diverse (misaligned) in their overall perceptions, but that there are some specific items over which they agree (e.g. the inclusion of 'cloud-based applications' across five of the six responses). Moreover, it is clear that some stakeholders appear to have a broader sense of the technology usage than others. Changing the 'View by' option to 'Response' (Figure 2b), shows how the same data is visualized when presenting it by response type (i.e. which responses were chosen by which stakeholders). Again, this is considered to enable some fairly quick comparisons and conclusions to be draw. For example, in this case it is clear that the use of Operational Technology is only identified by one stakeholder, which may act as a prompt for a dialogue with them about whether this is actually the case or a misunderstanding on their part.



USERNAME: ADMIN
ROLE: UNIVERSAL

Statistics

Survey: 2022-02-04
Category: All
Question: Which of the following technologies are utilised within your c
View By: Role

Cyber Security
Self Assessment Tool
MENU
Start Survey
View Stats
View Ratings
Account Management
Which of the following technologies are utilised within your organisation (i.e. they are in use somewhere to some extent)?
0
1
2
3
4
5
6
CEO
CFO
CPO
CISO
CIO
CTO
Desktop / laptop PCs
Smartphones and tablets
Consumer grade smart devices
Enterprise IoT / IIoT devices
Cloud-based storage
Cloud-based applications / services
Operational Technology (OT)
Embedded technologies
Unable to judge

USERNAME: ADMIN
ROLE: UNIVERSAL

Statistics

Survey: 2022-02-04
Category: All
Question: Which of the following technologies are utilised within your c
View By: Response

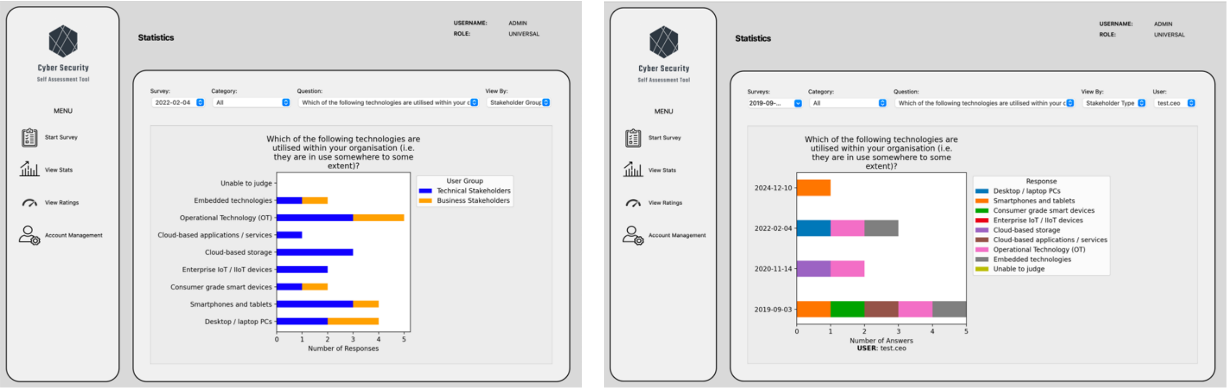
Cyber Security
Self Assessment Tool
MENU
Start Survey
View Stats
View Ratings
Account Management
Which of the following technologies are utilised within your organisation (i.e. they are in use somewhere to some extent)?
Unable to judge
Embedded technologies
Operational Technology (OT)
Cloud-based applications / services
Cloud-based storage
Enterprise IoT / IIoT devices
Consumer grade smart devices
Smartphones and tablets
Desktop / laptop PCs
0
1
2
3
4
5
Number of Responses
Role
test.ceo
test.cfo
test.cpo
test.ciso
test.cio
test.cto

(a)

(b)

Figure 2: Responses viewed by (a) stakeholder role and (b) response type

Recognizing that there will commonly be a disparity between business and technology-oriented stakeholders, a third view is offered by the category of stakeholder. This is intended to enable a broad assessment of the extent to which the two communities are aligned in their thinking or understanding. An example is presented in Figure 3a, and to draw an observation from the (dummy) data on show here, one would highlight that while the use of most technologies appears to have some recognition across both audiences, the use of cloud-based storage is appearing to be unrecognized by any of the business-oriented stakeholders. A final view enables responses from individual stakeholders to be tracked over time. This is shown in practice in Figure 3b with the tool permitting results from up to five prior SAT runs to be selected (by date) and then compared in the resulting chart.



USERNAME: ADMIN
ROLE: UNIVERSAL

Statistics

Survey: 2022-02-04
Category: All
Question: Which of the following technologies are utilised within your c
View By: Stakeholder Grour

USERNAME: ADMIN
ROLE: UNIVERSAL

Statistics

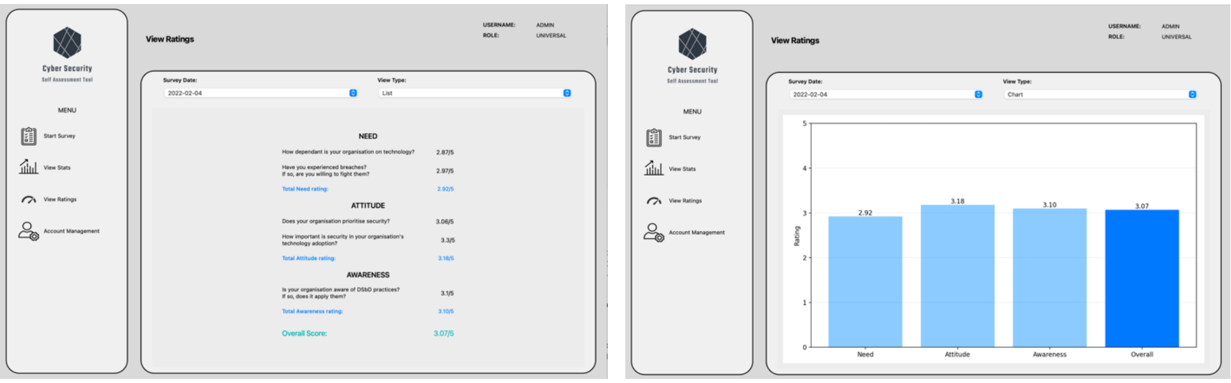
Surveys: 2019-09-...
Category: All
Question: Which of the following technologies are utilised within your c
View By: Stakeholder Type
User: test.ceo

(a)

(b)

Figure 3: Responses viewed by (a) stakeholder category and (b) individual stakeholder over time

A final feature is that the tool incorporated a basic implementation of a 'scorecard' approach for the associated Need, Attitude and Awareness ratings based on responses to related questions within the overall survey. This is presented in Figure 4, depicting the scorecard ratings by value and in chart format respectively.



View Ratings

USERNAME: ADMIN
ROLE: UNIVERSAL

Survey Date: 2022-02-04
View Type: List

NEED	
How dependant is your organisation on technology?	2.87/5
Have you experienced breaches? If so, are you willing to fight them?	2.97/5
Total Need rating:	2.92/5
ATTITUDE	
Does your organisation prioritise security?	3.06/5
How important is security in your organisation's technology adoption?	3.3/5
Total Attitude rating:	3.18/5
AWARENESS	
Is your organisation aware of DSbD practices? If so, does it apply them?	3.1/5
Total Awareness rating:	3.10/5
Overall Score:	3.07/5

Survey Date: 2022-02-04
View Type: Chart

(a) (b)

Figure 4: Scorecard ratings displayed (a) by value and (b) as a chart

While the SAT prototype is considered to offer appropriate core functionality, there are various options for further extension of the tool. These were identified during the design and development activities but were unable to be realized during the development of the current prototype due to the time constraints. One area would be related to expanding the assessment questions database, with the following points having been identified:

- Each question should have an optional 'Description/Rationale' field so that there is a means for users to get a further indication of what the question is asking for and why.
- In addition to the flags to indicate which questions are relevant to pose to which stakeholders, it would be desirable to have the option to provide alternate question wordings (or alternate questions entirely, including associated answer options) to suit different stakeholders. This would – for example – be relevant in the context of capturing incidents and impacts, where it would be relevant to phrase things for the CEO/CFO in terms of business impact, whereas the CIO/CTO may more readily relate to IT impact.
- The current implementation of the Need, Attitude and Awareness ratings is based upon a preset combination of questions and weightings. A more flexible approach would be for each question to have a flag to indicate whether it contributes to Need, Attitude or Awareness ratings, and for Individual responses to questions to then have associated scoring values (which may be positive or negative), so that they can be used in the calculation of overall scores and ratings.
- Questions include a 'P' flag to indicate those that only apply to organizations that Produce their own products/technologies. While the questions are embedded within the related thematic sections (and could influence the scores in these), it may also be relevant to use the P-flagged questions to generate a 'Secure Producer' score or similar.

There are also some enhancements that could usefully be made in relation to collecting and storing stakeholder responses:

- Each *response* should have an optional 'comments' box, and each overall *section* should also have a 'comments 'area.
- A third level of comment / feedback could be offered for the stakeholder response as a whole.

Stakeholder Evaluation

Having achieved the proof-of-concept implementation of the SAT, the final phase of the research was to evaluate it with relevant stakeholders. This was done by means of an online workshop session, in which the tool was demonstrated and then discussed with the participants to obtain their feedback. The workshop was promoted via the DSbD community, including a call for participation as part of a project update video circulated two months ahead of the scheduled workshop. However, this unfortunately yielded no volunteers and so the participants recruited for the workshop were not directly drawn from the DSbD community. Nonetheless, following a series of further invitations, five well-established and highly experienced senior cyber security practitioners were recruited, as listed in Table 1. Given their roles and experience, all were considered to offer valid opinions regarding the tool and the premise behind it. Having said this it would also be fair to observe that some of their responses is evaluating the role of the SAT appear to come from the perspective of cyber security in general rather than thinking about enabling DSbD specifically. All participants were offering their input from an individual perspective rather than offering the views of their parent organizations, and as such organization names are omitted in order to preserve anonymity. Participants are referred by number where appropriate in the upcoming analysis and discussion of the results.

Table 1 : Participants in the SAT evaluation workshop

Participant	Gender	Role
1	Male	Head of Cloud Security and Compliance
2	Male	Chief Information Security Officer
3	Male	Senior Technical Advisor
4	Male	Director of Information & Cyber Security
5	Female	CEO

The session was conducted on Microsoft Teams in November 2024, and was approved by the University of Nottingham School of Computer Science Research Ethics Committee (CS REC), application ID CS-2022-R29. Participants had consented to be involved based upon an email invitation, and further verbal consent was also obtained to record the session for transcription and analysis purposes.

The lead researcher shared their PowerPoint presentation with the participants for the first part of the workshop, to give an insight of the SAT conceptualization and its part in the larger project. Then, one of the students shared their screen and performed a short demonstration of the tool in its current form. Finally, the lead researcher opened a feedback session, where the participants were asked to share their thoughts on the tool and its potential application within the industry.

Thematic analysis was used to analyze the data collected in the session. This is a common method to understand and analyze participants' thoughts and opinions. As per Braun and Clarke's stages of thematic analysis (Braun and Clarke, 2006), the researchers familiarized themselves with the content of the transcripts by (re)reading, generated initial codes, searched and structured the themes, reviewed, named and defined them, and finally, produced the results. Throughout the process, researchers debriefed and discussed the analysis progress.

Four main themes (and associated sub-themes) were identified after applying thematic analysis across the data:

- Digital Security by Design knowledge gap in real-world applications
    - Lack of awareness of DSbD concept within organizations
    - A need to improve the selling point of the tool
- Evaluating the unique contribution of the tool

    - Competitive value compared to established tools and frameworks
    - Evaluation of purpose and measures
- Alternative settings that may be more suitable for application
- Feedback regarding the structure of the tool

Each theme and subtheme are described in the subsections that follow, each with supporting quotes from participants during the feedback part of the workshop. Reflecting upon the comments received is then presented in the later Discussion section.

Digital Security by Design knowledge gap in real-world applications

This is a crucial theme that subtly guided the feedback session and therefore reoccurs in many other themes within the analysis. It highlights that the concept of DSbD is generally unknown to non-technical professionals. Participants hypothesized that the lack of awareness of the DSbD concept would introduce limitations to implementing the SAT in the industry. They shared their thoughts on how the SAT and its presentation could be rephrased to showcase its relevance and explained how they would present it to their own management colleagues if they were required to use it.

Participants highlighted the lack of awareness of DSbD of most employees within their respective organizations. Several observed that the tool uses high-level technical knowledge, which their superiors and co-workers would not relate to:

> "*It seems a bit too far disconnected from what the CFO and CEO and that think about. It's very, /…/ technology led /…/ when you look at it in the context of being secured by design, asking a CEO: "would you be prepared to buy, you know, secure by design technology?" the response I'd probably get from people I deal with is like: "well, you're telling me it's not secure already? Why isn't it already secure? What are you telling me?"* (Participant 4)

However, participants themselves were supportive of the DSbD efforts and believe it is important to strive for improvement in that direction:

> *"*(Hypothetically*) Am I going to buy a building management system because it's been built secured by design? Yes. Possibly. Because I think there's a real uncertainty as to how we manage the security of all of those embedded Internet things /…/ So I absolutely support the secure by design drive. I think /…/ as a nation, as a profession, we need to work at how we drive that."* (Participant 2)

Participants also suggested that, in its current form, the SAT would not be applied successfully to real-world settings. However, most participants recognized the tool's potential. Two suggested the selling point of the tool's significance can be improved by talking about risk to the business. One of the participants stated the following:

> *"I'd also say the word that's missing, probably, for me, is risk. They* (the superiors) *will understand that - risk. They won't know why it's a risk, they won't have the details of technology, but ultimately the CEO of something or hopefully the CFO understands risk at a high level and actually linking the use of consumer grade OT for example in a business, that's a risk (where) you might make that stretch. But ultimately they will know the impact if you break it down to like an impact /…/ They may not know how likely it is - that's maybe the technical way, but if the risk to the business or risk to the organization hopefully is something they might know about"* (Participant 1)

Evaluating the unique contribution of the tool

Extensive discussion was held around the unique contribution of the SAT. Participants commented on its competition with other tools and frameworks in the field, as well as questioning the tool's purpose and what it intends to measure. The discussion is reflected in the following example quote:

> *"If I think about how I would go about having the conversation across my various businesses as to their attitude towards cyber and how much cyber is enough /…/ we would typically take our internal risk framework and our definitions of how we measure risk and we'd have a conversation with a business unit as to what do you see the points of risk in your particular organization /…/ So I think, would I use this in preference to using my own company's corporate risk frameworks? Having the conversation, no, I'd go with the latter…"* (Participant 2)

Participants suggested ways to improve the efficiency of the tool, in terms of the questions it poses and what it can measure as a result:

> *"I think that absolutely essential to this tool is getting the right balance of questions and at the moment they're obviously very, very high level and I think you're going to get motherhood and apple pie back from people because they're all going to say "yes, I believe in this"… But you're going to get back maybe not terribly honest answers with people, because everybody in essence will say that they support security and that, you know, something should be done."* (Participant 5)

> *"There are a lot of different ways that the attitude of the organization can be measured, so we've got benchmarking, which is always a sort of in my experience the preferred way of assessing your security and how much the organization ultimately wants to spend on security. We've got existing control frameworks which we can assess the organization against. To some extent is attitude and behavior surveys that you can look at across your organization."* (Participant 2)

Alternative settings that may be more suitable for application

Here the participants offered insights into settings in which they believe the SAT would perform well, that had not been previously considered. The views are included below:

> *"I think if you're in a large organization, you've got a lot of discrete business units all potentially managing their own entities. So in some ways, this could be a good barometer to actually see the behaviors against different business units and certainly when there's potential for reorganizing an organization structure in terms of leadership and etcetera. Then you could see over time whether those attitudes are changing within those business units. So I think there's some mileage in terms of giving you some sort of consistent view or at least looking for some out of kilter trends."* (Participant 3)

> *"I think that this approach could be useful if you've got organizations that are going through mergers and acquisitions so that you can start understanding what is important to different areas of the business and whether they align with your perceptions of the core business. And now it's expanded, does that still stand with the new people that are joining? So there's some interesting things from that. /../ But I think also the thing is the elapsed time. I think maybe this should be used more on a project basis, so that when you're going into something you should be looking at it from a project which it's almost defining, you know: "What are your requirements out of this? Do you really care about this? Are you prepared to invest in it?" And often the drivers that we have for doing things are external like audit points. And legislation where it's you've just got to do it. So I think there's a lot of good stuff in there, but it needs to have a rethink about how you go about it."* (Participant 5)

At the same time, doubts were raised around whether collection from multiple stakeholders would capture differing views, since few would be familiar with the concepts the tool enquires about:

> *"I think from a large organization, it would potentially come from one point, you know, like the chief architect or you know the architecture team. So, I don't think you'd get a lot of disparate views in terms of that because they would set the policy or they would set the course in terms of cyber then that's a totally different answer."* (Participant 3)

Feedback regarding the structure of the tool

The final theme is focused on feedback from one participant, who gave great thought to restructuring how the tool intends to obtain data and how stakeholders can offer their feedback:

> *"I think that if it was anonymized, and this is completely counter to what you're trying to do, you might get more honest answers from people rather than people fessing up and saying, "well, I know I'm the CFO, but I don't actually really want to invest in this"* (Participant 5)
>
> *"I find that often you get more out of questionnaires if you've got some free form text opportunities for people that they can actually feed in something that you probably might not have thought of asking."* (Participant 5)

By the end of the session, the participants suggested that an unstructured approach and discussion might be more successful in gathering in-depth information from within organizations:

> *"I was just wondering if a lot of the data that you get would be better coming from conversations. Because a lot of the time it's about winning the hearts and minds of people and I'm not sure that if you're asking just standard questions, that you get anything amazing back. I think that it's really more you want to sort of try and open up a discussion somehow. So I think what would be useful is almost to take a psychological approach to it somehow, so that the questions that people answer are not black and white, but it sort of tries to home into what their perception of risk is and what their appetite is, but in slightly more subtle ways…"* (Participant 5)

Discussion

Reflecting upon the workshop findings, the feedback was mixed, with some comments representing feedback on the SAT *concept* and others that could be more specifically linked to the form and function of the prototype *implementation*. One of the key criticisms of the prototype was that seemed "*disconnected from what the CFO and CEO and that think about*" and the related later observation that it would be appropriate for some stakeholders if the focus was framed more clearly around risk. It would be fair to say that some of these concerns have the potential to be addressed by incorporating alternate wording for different stakeholders so that questions are posed in more relatable language.

Another issue in relation to the question set was the observation around getting the balance right and the concern that if they are too high level then it becomes too easy for stakeholders to agree with. This is a potentially valid concern, although the hope would be that capturing of inputs from multiple stakeholders would still provide an opportunity to highlight significant divergences of opinion should they exist. Again, ensuring appropriate framing of the questions per stakeholder group would also be anticipated to help here.

Regarding the concern that the SAT would potentially be competing with existing approaches already in use, this is a fair point but from the context of the research the SAT had to be realized as a separate/standalone tool, as it was not possible to assume that an organization had a particular pre-existing approach in place. At the same time, however, considering how the assessment approach could be integrated within existing approaches would clearly be relevant to avoid it being seen as a further overhead.

A final point worth drawing out from the concerns was the suggestion that responses would be coming from one point in the organization (e.g. the chief architect or the architecture team) rather than capturing a more disparate set of view. While technical respondents may drive certain aspects of the response, part of the rationale for the SAT is to capture the wider views in order to assess whether the organization as a whole is on the same page.

There were also some clear examples of the SAT approach being recognized as having the potential to add value. For instance, the suggestion of its potential to be used as a barometer to compare business units, and as a potential means of gauging organizational posture during acquisitions are good examples and demonstrate recognition of the concept even if some specifics are considered to need refinement. Meanwhile the points made about the desirability of capturing open comments and the greater value that could be gained through conversations are both points that are already recognized (and agreed) in the wider approach. Indeed, the point about opening up a discussion highlights what one of the main benefits of the

SAT is intended to be - as a provocation of interest and a basis from which to initiate a discussion, should it be needed within the organization (or between particular stakeholders).

Considering the findings more broadly, it should be recognized that the SAT is not going to guarantee that security issues are solved, or to directly help to promote that that DSbD technologies are accepted and adopted. Instead, the role of the SAT is more subtle, and the objective is to act as a trigger and provide a basis for stakeholder dialogue. While it could be argued that organizations could perform a risk analysis or vulnerability scans as a basis for initiating a dialogue, this is likely to become a more control-centric approach, and focused on specific weaknesses requiring attention rather than evidencing the wider context in which the technology is being used and the potentially differing perspectives of those involved in the process. The advantage of the SAT is that it helps to reveal elements around attitudes and awareness of those taking decisions, and provides an opportunity to work towards a harmonized, collective approach.

The SAT results are expected to prompt a process of stakeholder dialogue and discussions. In this sense the results themselves are potentially not as important as *using* them as the opportunity to initiate a discussion in which all stakeholders already feel that they've contributed into. This in turn highlights another key point - the stakeholders are not just stakeholders in the organization. By engaging as participants in the SAT they become stakeholders in the assessment and the resulting security posture.

Conclusions

As the importance of cybersecurity continues to escalate in our rapidly evolving digital environment, the adoption of proactive assessment methodologies becomes imperative for safeguarding organizational assets and effectively countering cyber threats. The paper has presented the work undertaken to realize and evaluate a prototype self-assessment assessment tool. While the evaluation revealed a mixed reception for some of the specific aspects of the prototype in its current form, there was a recognition that an appropriately targeted tool could have value within an organizational setting if engaging the right stakeholders over the right aspects (i.e. reflecting that the data collection needs to be framed in a manner that each group can relate to and engage with).

Ultimately, finding a means to enable the wider stakeholder engagement is potentially key to the future adoption of DSbD-based approaches. Organizations need a means of collectively understanding the rationale and benefits of further investment when existing technologies may otherwise be perceived as functional and sufficient to support core business. The SAT aims to act as an enabling method. It not seeking to prove or demonstrate what the organization needs through security economics. It instead aims to provide a provocation of interest through which stakeholders can become directly engaged in the process.

Acknowledgements

The research described in this paper is supported by the Discribe Hub+ project, which is funded 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. The authors would also like to acknowledge the contribution of Dr Joseph Kaberuka, who helped to design the self-assessment question set upon which the SAT prototype is based.

References

Braun, V. and Clarke, V. (2006). 'Using thematic analysis in psychology', *Qualitative Research in Psychology*, 3(2), pp. 77–101. doi: 10.1191/1478088706qp063oa.

Dooley, R. (2024). "What Is A Chief Executive Officer? CEO Role Explained", Forbes, 21 April 2024. https://www.forbes.com/sites/rogerdooley/article/chief-executive-officer-ceo/

DSbD (2024), 'About Digital Security by Design', Digital Security by Design. *www.dsbd.tech/about/*, accessed 25 February 2024.

DSIT. (2024a). Cyber security breaches survey 2024 - Official Statistics. Department for Science, Innovation & Technology. 9 April 2024. https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2024/cyber-security-breaches-survey-2024

Furnell, S., Bada, M. and Kaberuka, J. (2023), "Assessing Organizational Awareness and Acceptance of Digital Security by Design," *Journal of Information Systems Security*, 19 (1): 3-19.

Furnell, S., Bada, M. and Kaberuka, J. (2025), "A Self-Assessment Method for Organizational Awareness of Digital Security by Design," *Journal of Information Systems Security*, 21 (2).

Gartner. (nd). "Chief Information Officer (CIO)". https://www.gartner.com/en/information-technology/glossary/cio-chief-information-officer

Lacina, L. (2023). "Chief Procurement Officers: What they do and why they're 'unsung heroes' for tackling big global challenges", World Economic Forum, 19 December 2023. https://www.weforum.org/stories/2023/12/chief-procurement-officers-what-they-do-why-important/

McKinsey & Company. (2023). "What are the roles and responsibilities of a CFO?", 29 November 2023. https://www.mckinsey.com/featured-insights/mckinsey-explainers/what-are-the-roles-and-responsibilities-of-a-cfo

Straub, D.W. and Welke. R.J. (1998), "Coping with systems risk: Security planning models for management decision making," MIS Quarterly, 22: 441-469.

Tversky, A. and Kahneman, D. (1974), "Judgment under Uncertainty: Heuristics and Biases," *Science*, 185: 1124- 1131.

Vachon, P. (2024), "Security Mismatch," *Communications of the ACM*, 67 (2): 40-41.

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', *www.cl.cam.ac.uk/research/security/ctsrd/pdfs/201406-isca2014-cheri.pdf*

Woollacott, E. (2024). "What Is A Chief Information Security Officer? CISO Explained", Forbes, 19 March 2024. https://www.forbes.com/sites/technology/article/chief-information-security-officer-ciso

Yasar, K. and Pratt, M.K. (2022). "Definition - chief procurement officer (CPO)", TechTarget. https://www.techtarget.com/searchcio/definition/Chief-Procurement-Officer-CPO